UNIVERSITE SORBONNE PARIS CITE
UNIVERSITÉ PARIS.DIDEROT

École Doctorale: 386, Sciences Mathématiques de Paris Centre
Laboratoire: Institut de Recherche en Informatique Fondamentale

DOCTORAT

Discipline : Informatique

presentée par

Arthur MILCHIOR

Logique du premier ordre, relations d'entiers et automates dans une base fixe

---

Thèse dirigée par Alexis BÈS et Olivier CARTON

Soutenue le 22 juin 2016 :

JURY

M. Alexis Bès	Universite Paris-Est Créteil	directeur
M. Olivier Carton	Universite Paris Diderot	directeur
M. Christian Choffrut	Universite Paris Diderot	
M. Arnaud Durand	Universite Paris Diderot	
M. Jérôme Leroux	Université de Bordeaux	rapporteur
M. Christian Michaux	Universite de Mons	rapporteur
M. Serge Grigorieff	Universite Paris Diderot	

Institut de Recherche en Informatique Fondamentale
Université Paris-Diderot – Paris 7
75 252 Paris cedex 05

École doctorale Sciences Mathématiques de Paris centre
8 place Aurélie Nemours,
75 013 Paris

Remerciements

Étant naturellement très bavard, je vais profiter de cette section non scientifique pour remercier tout plein de gens, plus ou moins liés à ma thèse ou à mes années de thèses. Les remerciements seront par ordre chronologique pour m'éviter de me demander qui je mets en premier.

Je commence donc par remercier mes parents pour tout. "Pour tout" car je serai bien incapable de faire la liste depuis la naissance, mais, vu qu'on est dans une thèse, je les remercie de m'avoir permis de faire des longues études.

Ensuite, je remercie mes professeures de mathématiques de 6ème au Lycée Molière, dont j'ai malheureusement oublié le nom, celle de 5ème à l'Institut de la tour, Mme Michaux, ainsi que celle du lycée, Mme Praquin. Ces professeurs en particulier car je sais qu'elles m'ont prêté des livres de mathématiques ou des exercices plus avancés que le niveau de ma classe, que j'ai trouvés très intéressants et qui m'ont donné envie de faire des mathématiques après le bac. De même, je remercie ma professeure de technologie, il me semble qu'elle se nommait Madame De La Roche Saint-André, qui en 3ème nous avait fait découvrir le HTML, et de fil en aiguille m'a donné goût à la programmation, et qui m'a permis de rester après les cours discuter de ce sujet avec elle. Je finirai avec le lycée en remerciant les prépas, qui m'ont unanimement refusé, ce qui fut probablement le meilleur choix pour moi.

À l'université, je remercie particulièrement M. Chailloux, responsable de la licence informatique, qui m'a permis de suivre des cours de L3 d'informatique en deuxième année en plus du cursus de L2, puis m'a proposé de faire un échange avec l'Université de Montréal. D'où le remerciement suivant: Pierre McKenzie, professeur du cours d'introduction à l'informatique théorique, qui m'a donné envie de faire de la recherche dans ce domaine. Je pense en particulier au fait qu'il posait des "questions bonus", que j'étais parfois le seul à faire, et qui consistaient quelque part en une mini introduction à la recherche. Je remercie aussi le remplaçant de son chargé de TD, Michaël Cadilhac. Un chargé de TD des plus horripilants qu'il m'ait été donné d'avoir, avec qui je suis resté en contact et m'a parfois conseillé durant la thèse.

Je remercie ensuite l'École normale supérieure de la rue d'Ulm de m'avoir accepté dans le département d'informatique. D'abord Isabelle Delais, la secrétaire pédagogique, qui a toujours été d'une grande gentillesse et d'une grande aide. Je suis reconnaissant envers le responsable pédagogique de mathématique, M. Paulin, de m'avoir autorisé à m'inscrire en math-info, même s'il me le déconseillait, et de m'avoir permis de découvrir par moi même que le niveau mathématique était effectivement trop élevé pour que je le suive en même temps que leur licence d'informatique. Au moins j'ai pu tenter.

Parmi les professeurs à Ulm, je remercie mon professeur de "langage formel, calculabilité et complexité", Olivier Carton, mais j'y reviendrai plus tard, mon professeur d'"Informatique scientifique par la pratique", David Naccache, grâce à qui j'ai co-publié mon premier papier avec deux élèves de mon année: Jacques-Henri , Stéphane. Je remercie aussi Jean-Christophe Filliatre, professeur de compilation, et surtout mon maître de stage de fin de L3, qui m'a permis de travailler sur mon premier gros projet de programmation: "Alt-Ergo". Concernant mes professeurs du MPRI, je tiens à remercier Luc Ségoufin, professeur du cours de Complexité, qui m'a mis en relation avec David A. Mix Barrington, mon maître de stage de M1, puis Alexis Bès, mon maître de stage de M2, devenu depuis mon directeur de thèse.

Je fais une pause dans le côté études pour passer aux gens que je tiens à remercier en dehors. D'abord des gens d'Ulm. Subbak avec qui j'ai partagé la promo 08 de l'ENS, puis 3 ans au LIAFA. Ensuite a3_nm, une personne dont je suis vraiment fan, et si ce n'était pour ses nouvelles de SF, ça pourrait être pour avoir fondé le club inutile. Puis Yap, qui a été mon co-auteur durant 6 mois, et qui a toute mon admiration, ne serait-ce que pour les 2 sketchs qu'on a eu le temps de jouer sur scène, et qui ont parfois eu un beau succès (et parfois pas)[1].

Ensuite, merci pour ces bons moments de répétitions (et jamais assez de représentation) aux membres des Cons Comptes de Fée Fêlées, avec qui j'ai joué le Lapin Blanc d'Alice au pays des Scones, Frère Tuck dans une version localement correcte de Robin des Bois, et Archibald de Mystérieux Meutre Mortel, une enquête d'Hercule Patate. Donc, je remercie Rachel, notre auteur, Denise notre costumière, Irène, notre metteuse en scène, Bibi notre régisseur. Puis Adeline, Clément, Marie Christophe, Jérôme, Fathi, Jérôme, Marie, Manon, Marie, Nathanaël, Séverine et Ismael. De même je remercie les cirqueux de l'Ens pour tous ces enseignement et les spectacles qu'on a passés ensemble. Sans eux, je ne saurais pas tenir les pieds en haut ni faire passer trois massues d'une main à l'autre avant de recommencer[2], ce qui en soit n'est pas bien grave, mais c'est marrant à faire. Je ne nommerai que ceux que j'ai souvent vu *et* qui ne sont pas dans la liste précédente, histoire de faire court. Noé et Annette qui ont été responsables du club à ma suite. Rémi, Chloé, à qui mon omoplate droite est encore reconnaissante, Auréliane, Jean-Baptiste, Alice, Émilia, Averell, Ilia, Paul, Théo et Truc.

Quittons un peu l'ENS, je tiens à remercier le Petit Théâtre du Bonheur et le Théâtre Popul'air du Reinitas et le Ze Artist, qui ont accepté que j'y joue mon one-man-show, les organisateurs de scènes ouvertes et de plateaux d'humoristes, entre autre le FIEALD, le Pranzo, le chinchman, mais aussi Christian, Ronan, Yacine et Franck, les 4 programmateurs de plateau qui sont venu me proposer de jouer chez eux. C'est des endroits où j'ai passé une bonne partie de mes soirées durant trois ans, et puis l'équipe d'On n'demande qu'à en rire, où j'ai eu la chance de faire quelques passages, ce qui m'a permis de belles rencontres, de la publicité pour le one-man, et paradoxalement les meilleures notes de mon parcours universitaires. Forcément, je remercie mes spectateurs, que je ne peux pas lister. Je n'énumérerai pas non plus les humoristes, il y en a trop que j'apprécie, humainement et artistiquement, et aurait peur d'en oublier.

Je remercie aussi la sagasphère, i.e. le monde de la saga MP3, c'est à dire des histoires audio. Où j'ai passé trois très bonnes années, à écouter, à jouer pour d'autres, et même à créer un peu. Je ne peux pas remercier la totalité de ceux avec qui j'ai travaillé, de ceux qui m'ont apporté conseil et/ou soutien. Mais je me dois de remercier en particulier, Selkio et Ryku, auteurs de Jencyo Rêva, a qui je dois le meilleur rôle de ma carrière et surtout l'expérience d'enregistrement la plus intense, Ian et A.J.K. qui ont pris de leur temps pour mixer des textes que j'ai écrits et aussi Xuè et Corinne, qui m'ont accordé plusieurs heures pour enregistrer les rôles principaux de mes sagas MP3s.

Enfin, je remercie le MAG Jeunes LGBT, avec qui j'ai passé 5 ans à intervenir dans des lycées et collèges un peu partout en Île-de-France, pour parler d'homophobie, de biphobie, de transphobie et de sexisme. Histoire d'avoir bonne conscience en faisant un peu de bénévolat, et aussi d'avoir des anecdotes intéressantes à raconter. Encore une fois, je ne ferai pas un itemize exhaustif des intervenants, mais je remercie au moins Gary pour tout son travail pour la commission intervention, qui a considérablement amélioré ce que j'ai pu faire en intervention, puis Marine, Léa/Erwan et Lucie/Lucas qui ont pris sa suite. Je remercie de même SOS Homophobie qui m'a récupéré quand j'étais trop vieux pour le MAG. Merci aussi à SOS homophobie, grâce à qui j'ai pu découvrir ce que ça fait de parler de ces sujets aux adultes.

[1] Je l'admire aussi pour avoir fini sa thèse en moins de 3 ans, être directement rentré au CNRS, et avoir fait des remerciements hilarants dans sa thèse.

[2] mais pas en même temps

Revenons enfin sur les études, c'est-à-dire sur le doctorat. Je remercie d'abord Alexis Bès. Mon maître de stage de M2, puis mon directeur de thèse. Tout d'abord, merci d'avoir réussi à me proposer comme sujet de stage une question qui a été effectivement résoluble en 6 mois, et m'a valu de pouvoir parler à Computability in Europe, donc d'avoir visité Milan. Merci d'avoir su me guider, par exemple en me conseillant des documents qui m'ont permis d'avancer dans ces questions de recherche. Le reste des remerciements concernent la thèse et non le stage, ils vont donc aussi à Olivier Carton, mon autre directeur de thèse.

Merci à vous deux de m'avoir laissé beaucoup de liberté. D'abord au niveau horaire. J'apprécie beaucoup d'avoir pu faire des interventions en semaines, comme mentionné plus haut. De toute façon je n'ai jamais réfléchi aussi bien aux démonstrations qui me bloquaient que quand j'étais allongé dans mon lit. Niveau liberté, merci aussi de m'avoir laissé suivre des idées qui me sont venues seuls, en particulier voir comment adapter le résultat de Jérôme Leroux à la logique sur laquelle je travaille. Ce problème a été le plus long de ceux que j'ai traités durant la thèse, étant passé par énormément d'étapes distinctes, et par des algorithmes très différents, avant d'avoir une version à peu près définitive mathématiquement, et qui a pu être codé en 2 mois. Avant d'être entièrement réécrit un grand nombre de fois de manière à en améliorer la lisibilité. D'ailleurs, merci pour les textes que vous avez $(\text{re})^+$lu. Quand je vois ce que j'ai écrit durant le master, j'admire l'effort qu'a du faire Alexis. Je sais que je me suis amélioré en rédaction, j'ai juste peur du chemin qu'il peut encore rester à faire.

Faisons un peu le tour du laboratoire, je ne peux remercier tout le monde, mais j'ai au moins une pensée pour les secrétaires Noëlle et Nathalie. Et bien sûr, merci à Frec-junior: Sam, Lorjn, Laure, Luc, Nathanaël, Denis et Charles. Ce dernier en particulier, car je dois à une de ses questions toute la partie qui traite de logique à deux variable de ce manuscrit. Merci aussi à Huu Vu, Bin, Thibault, Jehanne et Timo qui ont été mes co-bureau récents - ainsi qu'à tous mes anciens co-bureau que j'ai pu oublier. Merci à Victor, qui a considérablement amélioré ma compréhension des automates lisant des entiers. Merci à Florian (alias Dieu) pour... Un merci aussi à Michele, Christina, Pierre, Jean-Michel, Ines et Christian pour qui j'ai donné des TDs et TPs.

Ce n'est pas classique, mais j'aimerais vraiment remercier des gens que je cite dans mes papiers. Je ne les connais pas personnellement, ou très peu, mais sans eux et sans les articles qu'ils ont écrit, mon travail aurait été impossible ou en tout cas très différent de ce qu'il est. Sans remonter jusqu'à Alan Turing ou Mojżesz Presburger, voire jusqu'à Euclide, j'aimerais remercier Jérôme Leroux, qui a inspiré un des principaux résultats de cette thèse et s'est toujours montré intéressé envers mon travail. Christian Michaux et Roger Villemaire, ainsi que Andrei Muchnik, dont des articles ont inspiré une autre partie importante de ma thèse. Dans tous ces cas il s'agissait d'avoir un théorème similaire au leur, mais sur une autre logique. Je remercie Howard Straubing et Neil Immerman, dont les livres m'ont donné envie de travailler dans ce domaine, et qui ont toujours été très aimables quand je les ai rencontrés. Je suis aussi très reconnaissant à Victor Marsault et Jacques Sakarovitch, dont un article de 2013 a réussi à débloquer un point qui m'a longtemps posé problème.

Je tiens aussi à remercier mes étudiants. En particulier ceux de L2 Math-info que j'ai eu en 2014, parce que ça fait très plaisir pour un enseignant de voir dans son cours certains qui se plaignent que les questions soient trop simple, qui vont d'eux-même regarder les questions posées pour ce même cours à l'Ens, qui restent discuter de maths après le cours; et qui me remercient d'avoir pensé à eux en faisant une fiche de TD hors programme bien plus complexe[3]. Non seulement ils tentaient effectivement de répondre à ces questions, mais j'ai pu vérifier qu'ils comprenaient suffisamment pour remarquer et corriger les fautes que j'ai faites dans le sujet. Il y a quelques années, c'était moi qui restait discuter avec le professeur de mathématique après le cours, j'ai été ravi de pouvoir avoir le rôle inverse.

[3]Je ne suis pas non plus méchant, ils étaient au courant que j'avais caché une question ouverte.

Chronologiquement, les derniers à intervenir dans ce processus de thèse sont les membres du jury. Merci à Jérôme Leroux et Christian Michaux d'avoir accepté de rapporter ce long manuscrit, et merci à Christian Choffrut, Arnaud Durand et Serge Grigorieff d'avoir accepté de faire parti du jury.

Enfin, un merci tout particulier à Épiphanie, Hélène, Axel, Anthony, Nathanaël(le), Thomas, Annalí, et Nicolas.

Contents

1 Introduction **7**

2 Definitions and standard results **19**

I Logic **37**

3 Characterizations of first-order definable relations **39**

4 Spectra of logics with successor and a unary function **69**

5 Undecidability of satisfiability of some logics **95**

II Logic and automata **97**

6 Introduction **105**

7 From Formula to Automaton **107**

8 The Minimal Automaton $\mathcal{A}_{\phi,\mathbb{N}}$ **155**

9 The algorithm *EQF*$(\mathcal{V}_t^{\mathbb{N}})$ **195**

10 The algorithm *CEF'*$(\mathcal{V}_t^{\mathbb{N}})$ **247**

11 Conclusion **267**

Chapter 1

Introduction

Logic is a fundamental subject of both mathematics and computer science. Mathematical logic was first introduced in order to give a precise foundation to mathematics. One of the first results of logic is the formalization of the notion of proof: that is, logic could be considered to be an abstraction of mathematics. More recently, computers are used to check formal proofs, and to automatically check some mathematical statements. In particular, those statements deal with programs, considered as a function from a memory state to another memory state. Logic thus became an important tool of program verification: logical formulas are used as annotation of code. Those formulas specify the meaning and the expected effect of the code. Proof assistant and automated deduction tools are then used to assert that the effect of the code and the specification coincide.

Many kinds of logics are used for different types of specification. In this manuscript, we mainly consider first and second order logic over integers. In particular, we consider so-called Presburger arithmetic, i.e. the first-order logic of addition over integers, which is denoted by $\mathsf{FO}[\mathbb{N}, +]$. This logic is often used in program specification because it admits two important properties: it is decidable and it is expressive enough to state an important part of the notions used in specification of programs(see [Lat05]). Presburger arithmetic is named after Mojżesz Presburger, who proved in [Pre27] that this logic is decidable. This logic has then been extensively studied during this past century. It has been shown that the sets definable in Presburger arithmetic admit some nice characterizations. For example, the sets definable in Presburger arithmetic are also the semilinear sets. A semilinear set is a finite union of linear sets, also known as generalized arithmetic progressions. This equivalence implies that a $\mathsf{FO}[\mathbb{N}, +]$-definable set can naturally be decomposed into simpler sets.

My guideline

The main idea defended in this manuscript is that the class of sets definable in the fragment $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}]$ – where mod denotes the set of modular predicates – of Presburger arithmetic – which is called the class of regular sets – is very similar to the class of semilinear sets. My guideline during this PhD is: if a theorem T deals with semilinear sets, then there exists a theorem T', similar to T, which deals with regular sets.

The class of regular sets is a strict subset of the class of semilinear sets. The class of regular sets has not been as thoroughly studied as Presburger arithmetic, but a few characterizations of the logic $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}]$ shows that it is nonetheless an interesting fragment. By [Bü60], the languages definable in first-order logic with regular predicates are regular. For example the formula:

$$\exists x, y. x < y \wedge P_a(x) \wedge P_b(y),$$

defines the set of words which contain a letter a which occurs before a letter b. This language is regular.

Peladeau proved in [Pél92] that the class of regular sets is the greatest class of sets whose first-order logic only defines regular languages(Not to be confused with regular sets.). This theorem is a first justification for considering the fragment $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$. By [Bü60] the regular language are exactly the languages which are defined by an existential monadic second-order with regular sets, denoted by $\exists\mathsf{MSO}[\mathbb{N},<,\mathrm{mod},(P_a)_{a\in A}]$. The equivalence between the logic $\exists\mathsf{MSO}[\mathbb{N},<,\mathrm{mod},(P_a)_{a\in A}]$ and the regular language is effective, which implies that the logic $\exists\mathsf{MSO}[\mathbb{N},<,\mathrm{mod},(P_a)_{a\in A}]$, and hence the logic $\exists\mathsf{MSO}[\mathbb{N},<,\mathrm{mod}]$, are decidable.

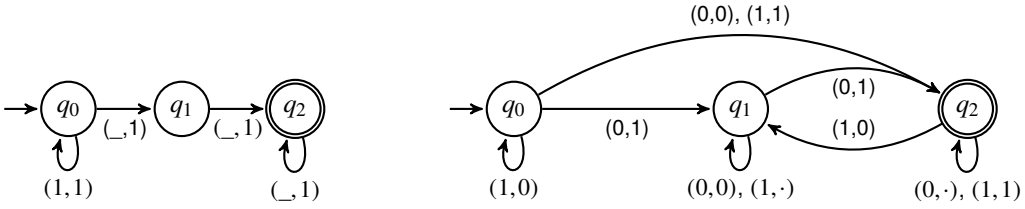
Automata

The first application of the guideline deals with automata. By [Sem77] (see also [BHMV94]), a set $R \subseteq \mathbb{N}^d$ is semilinear if and only if it is accepted by an automaton in base b for all $b \geq 2$. Similarly, by [Str91] (see [Str94, Chapter 3]) a set $R \subseteq \mathbb{N}^d$ is regular if and only if it is accepted by an automaton in base 1, which justifies the name "regular".

Automata theory is a central tool in theoretical computer science. Many problems are more easily solved with automata than with formulas. In fact, it is usual to reduce logical problems to automata problems. For example, automata admits a computable canonical form: the minimal deterministic automata. This canonicity of minimal automata allows to test the equality of two languages by testing whether, up to isomorphism, two automata are equal.

Automata provide natural encodings of sets of tuples of integers. The notion of automata is, after logic, the main concept studied in this manuscript. An automaton reads words, hence, numbers must first be encoded as words. A number n can naturally be encoded as the word of the form $1\ldots1$ of length n, called the base 1 expansion of n. A number is also usually represented as its base b expansion (for some integer $b \geq 2$). For example 11111 and 12 are the base 1 and base 3 expansion of 5. An automaton in base b (for some $b \geq 1$) reads the base b expansion of each number.

Let us now give examples of automata in base 1 and 2 which accepts the set R of pairs (n,m) such that $n+1<m$. The set R is accepted by the automata in base 1 and 2 pictured in Figure 1.1a and Figure 1.1b respectively. Those automata read pairs of digits in order to read a pair of integers. In the first automaton, the number of 1 read in the first position is n and the number of 1 in second position is m. In the second automaton, the concatenation of the digit read in the first position is the binary expansion of n and the concatenation of the digit read in the second position is the binary expansion of m. Note that no words accepted by the first automaton contains the substring "_1" in any of the positions. That is, the _ are only used on the right-side of a word in order to pad the smaller words. It is then said that an automaton



(a) In base 1

(b) In base 2

Figure 1.1: Automata accepting $n+1<m$.

accepts a tuple of integers if the automaton accepts its base-b expansion.

Note that, by [BHMV94], the sets accepted by an automaton in base b, called the b-recognizable sets, are exactly the sets definable in the logic $\mathsf{FO}[+,<,V_b]$ (where $V_b(n)$ is the greatest power of b which divides n). By [Sem77] a set $R \subseteq \mathbb{N}^d$ is b- and b'-recognizable, for b and b' multiplicatively independent

(b and b' are said to be multiplicatively independent if $\frac{\log(b)}{\log(b')}$ is irrational) if and only if R is semilinear. The same result for $d = 1$ was already proven in [Cob69]. Those papers also prove that R is semilinear if and only if it is b-recognizable for all $b \geq 2$.

We must emphasize that a b-recognizable set R is not a recognizable subset of the monoid $(\mathbb{N}, +)$. It is the set of base b expansions of tuples of integers of R which is recognizable in the monoid $(\{0, \ldots, b-1\}^d, \cdot)$ where $\cdot$ is the concatenation of words. Note that a subset of the monoid $(\mathbb{N}^d, +)$ is rational if and only if it is $\mathsf{FO}[\mathbb{N}, +]$-definable.

Quantifier elimination

Another intuition behind the guideline comes from the notion of quantifier elimination. Presburger proved in [Pre27] that the logic $\mathsf{FO}[\mathbb{N}, +, <, \mathrm{mod}]$ admits quantifier elimination. Each $\mathsf{FO}[\mathbb{N}, +, <, \mathrm{mod}]$-formula is equivalent to a $\Sigma_0[\mathbb{N}, +, <, \mathrm{mod}]$-formula, that is to a quantifier-free formulas with addition, order and modular predicates. Quantifier elimination is an important tool when studying logic because studying formulas without quantifier is easier than studying a formula with quantifiers. For example, deciding whether a sentence - that is, a formula without variable - holds, consists in checking some arithmetic (in)equalities. Checking the satisfiability of a formula is reduced to checking whether a sentence holds by existentially quantifying the variables and then applying the quantifier elimination.

The two following results would seem hard to prove directly, and become trivial when only quantifier-free formulas are considered. The set of integers definable in Presburger arithmetic and the spectra of Presburger arithmetic are the ultimately periodic sets. The spectrum of a formula is the set of cardinalities of finite models of this formula. For example, the spectrum of:

$$\exists \,\mathrm{last}\,.\neg\exists y.\ \mathrm{last} + 1 = y \wedge \exists\,\mathrm{middle}\,.\ \mathrm{middle} + \mathrm{middle} = \mathrm{last}$$

is $2\mathbb{N} + 1$. Indeed the universe $[n]$ of cardinality $n + 1$ is a model of this formula only when n is even. When n is even, last must be interpreted by n and middle by $n/2$.

The paper [Coo72] gives an algorithm of quantifier elimination for $\mathsf{FO}[\mathbb{N}, +, <, \mathrm{mod}]$ which is more efficient than the algorithm of [Pre27]. We remark (Proposition 2.2.21) that the algorithm of [Coo72] also eliminates the quantifiers of logics such as $\mathsf{FO}[\mathbb{N}, <, +\mathbb{N}, \mathrm{mod}]$ - where $+\mathbb{N}$ is the set of additions of constant - $\mathsf{FO}[\mathbb{N}, +\mathbb{N}, \mathrm{mod}]$, $\mathsf{FO}[\mathbb{N}, <, +\mathbb{N}]$ and $\mathsf{FO}[\mathbb{N}, +\mathbb{N}]$.

Muchnik's theorem

We already stated the important result, proved in [Cob69, Sem77] that a set $R \subseteq \mathbb{N}^d$ is b- and b'-recognizable, for b and b' multiplicatively independent if and only if R is semilinear. Another proof of this result was given as [Muc03, Theorem 5]. This proof uses the impressive characterization of [Muc03, Theorem 2], which states that a set $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[\mathbb{N}, +]$-definable if and only if R satisfies two properties. The first property is: all sections of R are also $\mathsf{FO}[\mathbb{N}, +]$-definable. A section of R being R with a component fixed, it is a set of dimension $d - 1$. The second property is: each bounded set, far enough from 0, admits a periodicity, and furthermore, there is a finite number of periodicities. Muchnik's result allows to reduce the study of $\mathsf{FO}[\mathbb{N}, +]$-definable to the study of sets of smaller dimension and of bounded sets. As stated above, this characterization allows to prove more easily Cobham-Semevov's theorem.

The exact characterization of [Muc03, Theorem 1] is recalled in Theorem 3.2.9; it is a bit technical, but admits two important corollaries. The first corollary, the so-called "definable criterion for definability in Presburger arithmetic" [Muc03, Theorem 2], states that there exists a $\mathsf{FO}[\mathbb{N}, +, R]$-formula which holds if and only if R is $\mathsf{FO}[\mathbb{N}, +]$-definable. This result is quite impressive because it is uncommon that a model is expressive enough to characterize itself. Usually, statements about a logic must be expressed in a more expressive logic. Muchnik's result also admits another corollary, [Muc03, Theorem 3]: it is decidable whether an automaton in base b accepts a $\mathsf{FO}[\mathbb{N}, +]$-definable set. Equivalently, by [BHMV94],

it is decidable whether a $\mathsf{FO}[\mathbb{N},+,V_b]$-formula is equivalent to a $\mathsf{FO}[\mathbb{N},+]$-formula. Note that, in the case of set of integers, i.e. sets of dimension 1, this result was already proven in [Hon86].

Considering the theorems of [Muc03], our guideline led to the following results. We found a characterization of the $\mathsf{FO}[<,\mathrm{mod}\,m]$-definable sets ($\mathsf{FO}[<,\mathrm{mod}\,m]$ is the restriction of $\mathsf{FO}[<,\mathrm{mod}]$ where the modulus is fixed to m). A set $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[<,\mathrm{mod}\,m]$-definable if all sections and diagonals of R are $\mathsf{FO}[<,\mathrm{mod}\,m]$-definable, and apart from a finite number of sections, R is equal to:

$$\{(x_0+m,\dots,x_{d-1}+m) \mid (x_0,\dots,x_{d-1}) \in R\},$$

that is, R translated by m in all directions. Furthermore, this characterization is $\mathsf{FO}[\mathbb{N},<,R]$-expressible. Note that, when $m=1$, this logic is $\mathsf{FO}[\mathbb{N},<]$ hence this result also concerns $\mathsf{FO}[\mathbb{N},<]$.

This characterization naturally leads to a characterization of $\mathsf{FO}[\mathbb{N},<,\ \mathrm{mod}\ ]$: "there exists m such that the characterization of $\mathsf{FO}[<,\mathrm{mod}\,m]$ holds". Similarly to [Muc03, Theorem 3], the fact that the characterization of the $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-definable set is $\mathsf{FO}[\mathbb{N},+]$-expressible implies that it is decidable whether an automaton in base b accepts a $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-definable set. By [Str94], it is equivalent to state that it is decidable whether an automaton in base $b \geq 2$ accepts a set accepted by an automaton in base 1. Note that the proof is new, but not the result. Indeed, Choffrut proved in [Cho08] that it is decidable whether a $\mathsf{FO}[\mathbb{N},+]$-formula accepts a set which is definable in weaker logics such as $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$.

Michaux-Villemaire's theorem

Muchnik's results lead to another impressive characterization of $\mathsf{FO}[\mathbb{N},+]$-definable set, [MV96, Theorem 5.1]: A set $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[\mathbb{N},+]$-definable if and only if all $\mathsf{FO}[\mathbb{N},+,R]$-definable sets of integers are $\mathsf{FO}[\mathbb{N},+]$-definable - that is, are ultimately periodic. The importance of this theorem entirely comes from one side of the equivalence: for all sets R of dimension d which are not semilinear, there exists a witness, a set of integers, which is $\mathsf{FO}[\mathbb{N},R,+]$-definable and not semilinear. A careful study of the proof of this theorem allowed us to prove that the formula which defines this witness can be chosen independently of R (Theorem 3.2.12).

A little twist with respect to the guideline is required when dealing with those results. Indeed, + is not regular, but all sets of integers which are $\mathsf{FO}[\mathbb{N},+,<,\mathrm{mod}]$-definable are ultimately periodic, hence regular. It is proven in this manuscript that a semilinear set R is regular if and only if all $\mathsf{FO}[\mathbb{N},<,R]$-definable unary functions are regular (Theorem 3.3.8). More precisely, given a set R which is semilinear and which is not regular, there exists a unary function f which is $\mathsf{FO}[\mathbb{N},<,R]$-definable, and has the form $f(n) = rn + h(n)$ with $r \in \mathbb{Q}$, $r > 1$ and $h : \mathbb{N} \to \mathbb{Z}$ bounded. It should be noted that unary functions are one of the easiest data structures strictly more complex than sets of dimension 1, hence it seems hard to imagine how to improve this result and to exhibit a simpler witness.

A second theorem similar to [MV96, Theorem 5.1] is given. In this second theorem, the witness is a set of integers, but the logic studied is restricted to the fragment $\mathsf{FO}[<,\mathrm{mod}\,m]$. A set R is $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}\,m]$-definable if and only if all $\mathsf{FO}[\mathbb{N},<,R]$-definable sets of integers are $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}\,m]$-definable - that is are ultimately m-periodic.

From automata to formulas

The algorithms of Honkala and Muchnik are inefficient, and so is our algorithm which decides whether an automaton accepts a regular sets using our characterization of regular set. More precisely, their worst time complexity is not even exponentially bounded. More recently, Leroux gave a polynomial time algorithm [Ler06], which takes as input an automaton in base $b \geq 2$, and returns a $\mathsf{FO}[\mathbb{N},+]$-formula which defines the set accepted by the automaton if such a formula exists, and rejects otherwise. In the

case of dimension 1, Marsault and Sakarovitch gave a simpler algorithm [MS13] which runs in quasi-linear time.

Our guideline led to a polynomial time algorithm which takes as input an automaton in base b and outputs a $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-formula which defines the set accepted by an automaton in base b if such a formula exists (Part II). This algorithm returns in time $O\left(n^3\log(n)\right)$. Furthermore, the algorithm can return in linear time a Boolean stating whether the formula exists when the automaton is minimal. When our algorithm is applied to an automaton of dimension 1, it is similar to the algorithm of [MS13]. More precisely, [MS13] was an important inspiration for the part of our algorithm which considers the modular predicates.

Satisfiability

We did not try to follow our guideline when dealing with satisfiability results: as stated above, the satisfiability of logic with regular sets over words is known to be decidable, whereas by [Lan04, Lemma 6.3], the satisfiability of first-order logic with semilinear sets over words is undecidable. Those results naturally leads to the following question: what is the biggest class C of sets, between the class of regular sets and the class of semilinear sets, such that first order logic with C over words is decidable ? We prove (Theorem 5.2.4) that this biggest class is exactly the class of regular sets. This result is another proof that $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$ is a logic worth studying.

A natural example of relation which is semilinear and not regular is the multiplication by 2. Hence our result implies that $\mathsf{FO}[\mathbb{N},<,\times 2,\mathrm{mod},(P_a)_{a\in A}]$ is undecidable. Recall that we stated above that if R is semilinear and not regular, then there exists a function g which is $\mathsf{FO}[\mathbb{N},<,R]$-definable of the form $rn + h(n)$ with $r > 1$ and $h(n)$ bounded. More generally, the study of $\mathsf{FO}[\mathbb{N},<,R,(P_a)_{a\in A}]$ leads to the study of the logics $\mathsf{FO}[\mathbb{N},<,g]$ where $g : \mathbb{N} \to \mathbb{N}$ is an increasing function which is not bounded by any function of the form $n \mapsto c + n$. We prove (Theorem 5.2.1) that, for any such function g, the satisfiability of $\mathsf{FO}[\mathbb{N},+1,g,(P_a)_{a\in A}]$ is undecidable. Hence, for example, the satisfiability of $\mathsf{FO}[\mathbb{N},+1,n\mapsto n!,(P_a)_{a\in A}]$ and $\mathsf{FO}\left[\mathbb{N},+1,n\mapsto n^2,(P_a)_{a\in A}\right]$ are undecidable.

Note that while the class of regular sets is the maximal class below Presburger arithmetic whose first-order satisfiability over words is decidable, it is not the maximal logic whose satisfiability is decidable. Indeed, the satisfiability of $\mathsf{FO}[\mathbb{N},<,\mathrm{mod},R,(P_a)_{a\in A}]$ is decidable when R denotes the set of factorials or the set of powers of two (this is a direct consequence of Elgot-Rabin's result that satisfiability of $\mathsf{MSO}[<,R]$ is decidable in this case [ER66]).

Spectra

We mentioned logics such as $\mathsf{FO}[\mathbb{N},+1,\times 2,(P_a)_{a\in A}]$, $\mathsf{FO}[\mathbb{N},+1,n\mapsto n!]$ and $\mathsf{FO}\left[\mathbb{N},+1,n\mapsto n^2\right]$. They seem harder to characterize than the other logics considered above. Since no direct characterizations were found, we simplified the problem by considering the spectra of those formulas. In this case, we show that the spectra of those logics contains the encoding of the set of halting times of non-deterministic 2-counter automata (Theorem 4.2.10). 2-counter automata are a Turing-complete model ([Min60]), which, intuitively, implies that the set of halting times of the non-deterministic version of those automata are complex sets. This result shows that the spectra of those logics can express complex sets.

The complexity of $\mathsf{FO}[\mathbb{N},+1,\times b,(P_a)_{a\in A}]$, with $b \geq 2$, is also shown by the fact that all b-recognizable sets of integers are $\mathsf{FO}[\mathbb{N},+1,\times b,(P_a)_{a\in A}]$-spectra (Theorem 4.2.1). Those two results surprised us, as the $\mathsf{FO}[\mathbb{N},+1]$-spectra are the finite and co-finite sets, and it was not expected that adding a predicate such as the multiplication by a constant adds so much expressivity.

Logic with an uninterpreted function

Note that in the logics $\mathsf{FO}[\mathbb{N},+,<,V_b]$, $\mathsf{FO}[\mathbb{N},+,<]$, $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$ and $\mathsf{FO}[\mathbb{N},+1]$, all symbols have a precise meaning. The proofs of the above-mentioned statements led us to the study of another kind of logics: logics with uninterpreted function. Let us first give an example of a formula with an uninterpreted function f. The formula:

$$f(0) = 0 \wedge \forall n > 0. f(n+1) = f(n) + 2 \wedge f(x) = y$$

holds only if $f(n) = 2n$ for all n, hence only if $2x = y$.

The study of the logic $\mathsf{FO}[\mathbb{N},+1,\times b,(P_a)_{a\in A}]$ led us to the study of $\mathsf{FO}[\mathbb{N},+1,f]$, with f uninterpreted. While those two logics may seem unrelated, we prove that all $\mathsf{FO}[\mathbb{N},+1,\times b,(P_a)_{a\in A}]$-spectra admit an encoding as $\mathsf{FO}[\mathbb{N},+1,f]$-spectra. This comes from the fact that letters, multiplication by a constant and modular predicates can be encoded in $\mathsf{FO}[\mathbb{N},+1,f]$.

This result was also surprising to us, because by [Ehr59], $\mathsf{FO}[\mathbb{N},f]$ is decidable, and by [DFL98], the spectra of the $\mathsf{FO}[\mathbb{N},f(x)]$-formulas are exactly the ultimately periodic sets (by [GS03], the same holds for $\mathsf{MSO}[f(x)]$.). The least logic above $\mathsf{FO}[\mathbb{N},+1,f]$ which is known to be undecidable being $\mathsf{MSO}[+1,f(x)]$, by [Tho75]. It was not expected to us that mixing the two logics $\mathsf{FO}[\mathbb{N},+1]$ and $\mathsf{FO}[\mathbb{N},f]$, which only defines simple sets, lead us to sets as complicated as the encoding of the set of halting times of 2-counter automata.

Contributions

We now state the results proven in this manuscript. There are two kinds of results. In Part I, characterizations of logics are given in terms of definable sets and of spectra. Furthermore some undecidability results are given. Part II considers automata which accept sets which are $\mathsf{FO}[\mathbb{N},<,-,\mathrm{mod}]$-, $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-, or $\mathsf{FO}[\mathbb{N},+1,\mathrm{mod}]$-definable. Here, $-$ is the unary minus function.

Quantifier elimination

Our first result is a fine analysis of [Coo72]'s algorithm, which shows that some fragments of $\mathsf{FO}[\mathbb{N},+]$, such as $\mathsf{FO}[\mathbb{N},<,+\mathbb{N},\mathrm{mod}]$, admit quantifier elimination (Proposition 2.2.19 and Proposition 2.2.21).

Characterizations

In this manuscript (Chapter 3), we give many characterizations of classes of sets of tuples of integers.

- We prove (Theorem 3.2.12) that for all $d \in \mathbb{N}^{>0}$, there exists a $\mathsf{FO}[\mathbb{N},+,R]$-formula ϕ_d, such that when R is interpreted by a set of dimension d which is not semilinear, ϕ_d defines a set of integers which is not semilinear. This construction allows to give a slightly shorter proof of [MV96, Theorem 5.1].

- We prove that a set $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}\, m]$-definable if and only if all sets of integers which are $\mathsf{FO}[\mathbb{N},<,R]$-definable are $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}\, m]$-definable, (Theorem 3.3.11).

- We prove (Theorem 3.4.1), that a $\mathsf{FO}[\mathbb{N},+]$-definable set $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-definable if and only if all unary functions which are $\mathsf{FO}[\mathbb{N},<,R]$-definable are $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-definable.

- We prove (Theorem 3.3.1) that a set $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}\, m]$-definable if and only if:

– Every section of R (i.e. every subset of $\mathbb{N}^{d-1}$ obtained from R by fixing a component) is $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}\, m]$-definable and

– apart from a finite number of sections, R is equal to

$$\{(x_0 + m, \ldots, x_{d-1} + m) \mid (x_0, \ldots, x_{d-1}) \in R\},$$

that is, R translated by m in all directions.

- The preceding result is then used to prove that the fact that R is $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}\, m]$-definable is $\mathsf{FO}[\mathbb{N}, <, R]$-definable.
- The preceding result is used to show that is decidable whether a b-recognizable set is $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}\, m]$- or $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}]$-definable (Corollary 3.3.9).
- It is also decidable whether a $\mathsf{FO}[\mathbb{N}, +, V_b]$-formula accepts a $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}]$-definable set (Corollary 3.3.10).

The results mentioned in this section are summarized in Figure 1.2. In the figure, the symbol R represents a $\mathsf{FO}[\mathbb{N}, +]$-definable set which is not $\mathsf{FO}[\mathbb{N}, <, \mathrm{mod}]$-definable. The function $g(x)$ is not bounded by any function of the form $n \mapsto n + c$. The function $f(x)$ and $f'(x)$ are uninterpreted. The number b is greater than 1.

The spectra

We now summarize the results concerning spectra which are proven in this manuscript (Chapter 4). In this section, let g be a function which is not bounded by any function of the form $n \mapsto n + c$ for $c \in \mathbb{N}$, and let f be an uninterpreted function. The results about spectra are independent of the results about characterizations.

- We prove (Theorem 4.2.1) that each b-recognizable set of integers is a $\exists\mathsf{MSO}\Pi_2^2[+1, \times b]$-spectrum.

  Here Π_2 means that the universal quantifiers appear before the existential one, and the 2 in exponent means that only two first-order variables can be quantified.
- Similarly, we prove (Theorem 4.3.1) that a Boolean combination of b-recognizable sets, for different values of b, is a $\Pi_2[+1, f]$-spectrum.
- Finally, we prove (Theorems 4.2.10 and 4.3.12) that the set of accepting computations of any non-deterministic two-counter automaton can be encoded as an $\exists\mathsf{MSO}\Pi_2^2[+1, g]$-spectrum and as a $\Pi_2[+1, f]$-spectrum.

The results mentioned in this section are summarized in Figure 1.3.

Satisfiability

We now summarize the results about satisfiability proven in this manuscript (Chapter 5). Those results use both our results about spectra and the characterizations of class of sets given above.

- Using the encoding of 2-counter automata introduced in Section 1, it is shown (Corollaries 5.2.1 and 5.2.3) that the satisfiability problem for $\exists\mathsf{MSO}\Pi_2^2[+1, g]$ and $\Pi_2[+1, f]$ are undecidable. As above, the first result is equivalently stated as: the satisfiability problem for $\Pi_2^2[+1, g, (P_a)_{a \in A}]$ over words is undecidable.

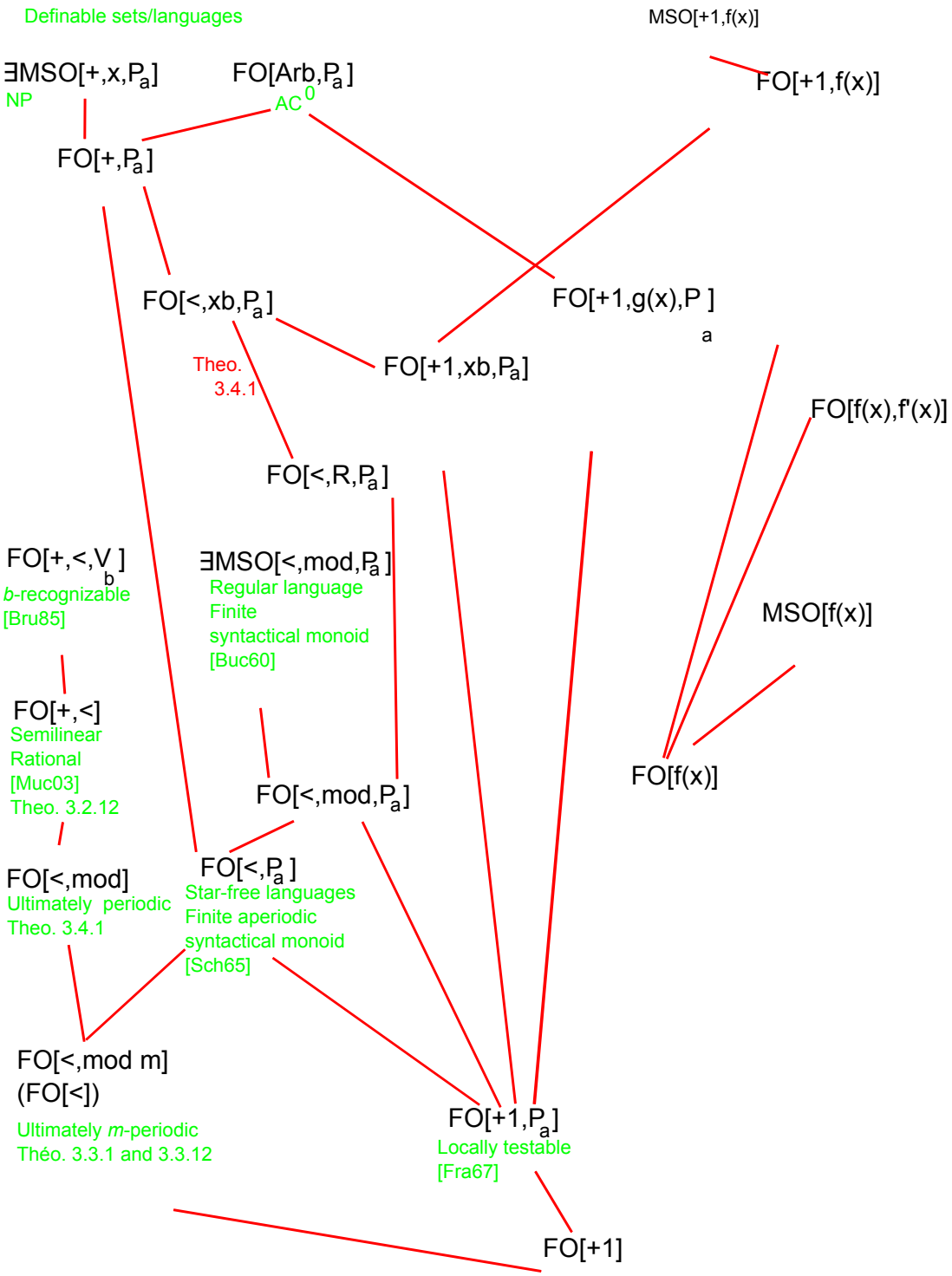


Figure 1.2: Summary of the results about the characterizations.

- The characterization stated in Section 1 allows to prove (Theorem 5.2.4) that the satisfiability of $\exists\mathsf{MSO}\Pi_3[<,+1,R]$ is undecidable, when $R \subseteq \mathbb{N}^d$ is $\mathsf{FO}[\mathbb{N},+]$-definable and is not $\mathsf{FO}[\mathbb{N},+,<]$-definable. The satisfiability of $\Pi_3[<,+1,R,(P_a)_{a\in A}]$ over words is also undecidable.

  When the number of alternations of quantifiers is ignored, it means that the satisfiability of the fragment $\mathsf{FO}[<,R,(P_a)_{a\in A}]$ is undecidable.

  As stated above, the satisfiability of $\mathsf{FO}[<,\mathrm{mod},(P_a)_{a\in A}]$ is decidable. This result shows that the maximal fragment of $\mathsf{FO}[+,(P_a)_{a\in A}]$ which contains the order relation and whose satisfiability is decidable is $\mathsf{FO}[<,\mathrm{mod},(P_a)_{a\in A}]$.

The results mentioned in this section are summarized in Figure 1.4. The union of results given in Part I are summarized in Figure 1.5

From automata to formula

Finally, we consider in Part II the automata in base $b \geq 2$ which encode $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-definable sets. The results in this part are independent of all previously mentioned results, apart from the quantifier elimination results.

In this part, it is shown how to decide whether a set $R \subseteq \mathbb{Z}^d$, given as a minimal automaton is definable in the logics $\mathsf{FO}[\mathbb{Z},<,-,\mathrm{mod}]$, $\mathsf{FO}[\mathbb{Z},<,\mathrm{mod}]$ or $\mathsf{FO}[\mathbb{Z},+1,\mathrm{mod}]$. When the automaton accepts non-negative numbers, the existence of a formula can be decided in time $O(n)$ where n is the number of states of the automaton. When the automaton accepts subsets of $\mathbb{Z}^d$, the complexity time is $O(n\log(n))$ (because some automata must then be minimized).

When the set R is definable in one of those logics, there exists an existential formula which defines the set accepted by the automaton and which can be computed in time $O\left(n^3\log(n)\right)$. More precise bounds on the computation time are given in terms of the basis b of the automaton and the dimension d of the set. A proof of concept of this algorithm in OCaml is available at: `https://github.com/Arthur-Milchior/RegAut`[1].

[1]It is not an exact implementation of this algorithm. Indeed, since the code has been written, the algorithm has been simplified. Those simplifications has not yet been implemented in the code.

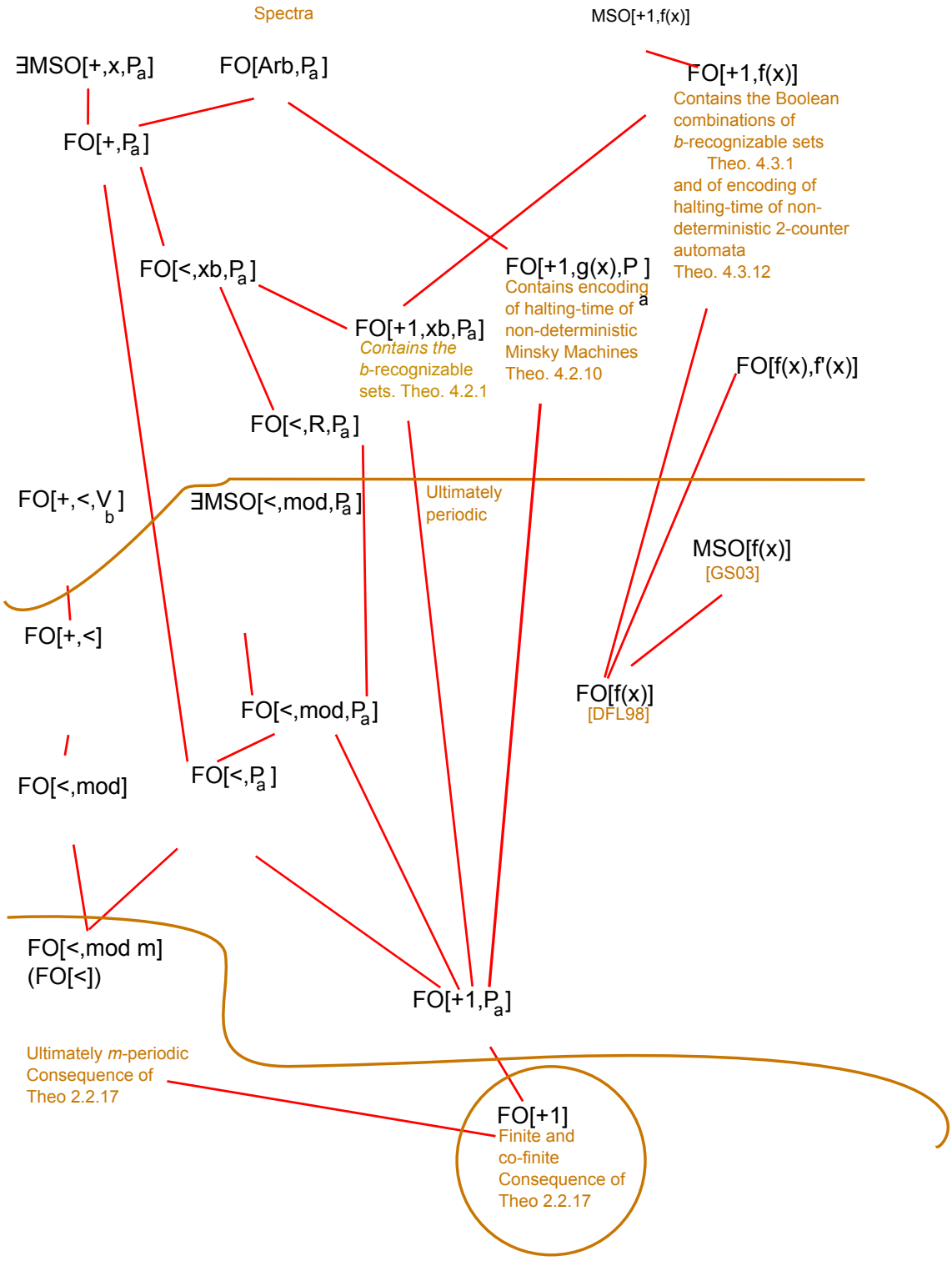


Figure 1.3: Summary of the results about the spectra.

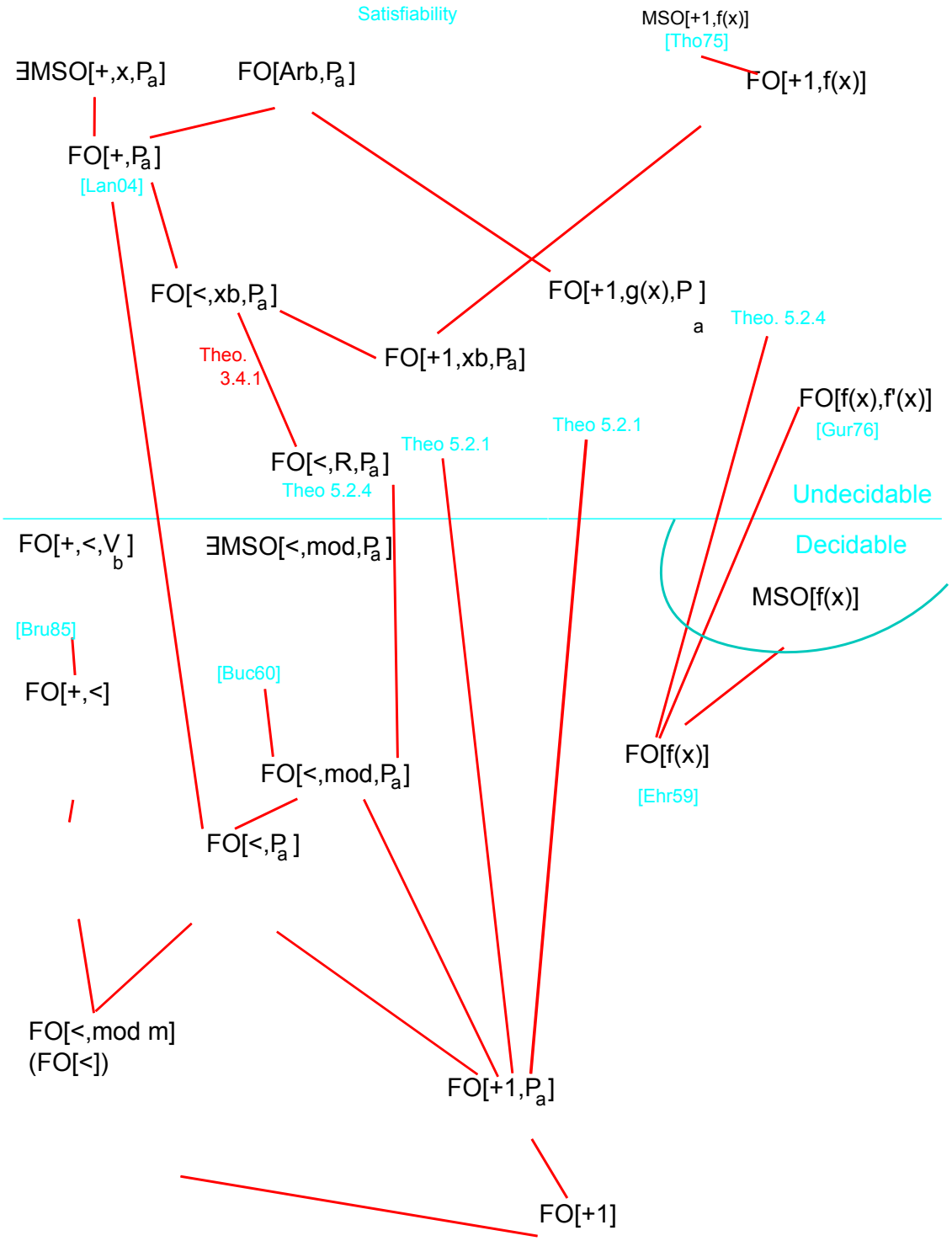


Figure 1.4: Summary of the results about undecidability.

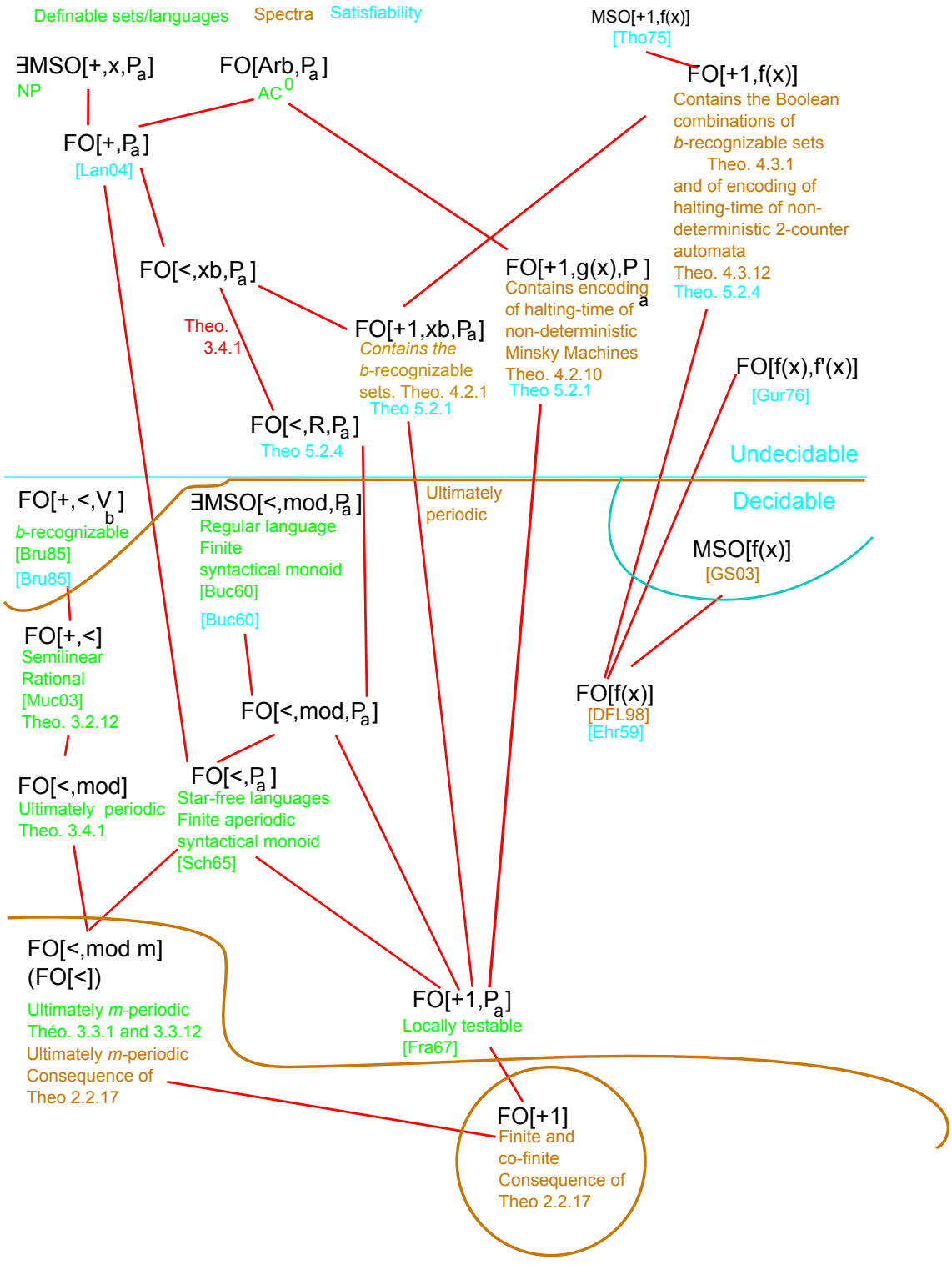


Figure 1.5: Summary of the results of Part I.

Chapter 2

Definitions and standard results

In this section, the main definitions used in this manuscript are introduced. A variable of type TYPE is, in general, denoted by t, except when another letter is more standard. The symbols t_i for i an integer are used when a sequence of values of the same type T is used. For $d \in \mathbb{N}$, bold letters are used to denote d-tuples of variables, such as $\boldsymbol{x} \in \mathbb{N}^d$, which is an abbreviation for $(x_0, \cdots, x_{d-1})$.

Contents

2.1 Standard Notations 19
2.2 Logics 21
2.2.1 Syntax and semantic 21
2.2.1.1 Semantic 23
2.2.1.2 Explicitly writing some formulas 24
2.2.2 Quantifier elimination for fragments of FO[+] 26
2.2.3 Sections, diagonals and subsets 30
2.2.4 Logic over $\mathbb{N}$ and over finite models. 31
2.3 Automaton, words and monoid 31
2.3.1 Monoid, semigroup and actions 31
2.3.2 Words and Languages 32
2.3.3 Integers in Base b 33
2.3.4 Deterministic automata 34
2.3.4.1 Automata reading tuples of integers 35

2.1 Standard Notations

In this section, standard mathematical notations are given. Those notations concern sets and numbers.

Numbers

- Let $\mathbb{N}$ denote the set of non-negative integers.
- Let $\mathbb{Z}$ denote the set of integers.
- Let $\mathbb{Q}$ denote the set of rational numbers.

- Let $\mathbb{R}$ denote the set of real numbers.
- For $S \subseteq \mathbb{R}$, let $S^{\geq 0}$ (respectively, $S^{>0}$) be the set of non-negative (respectively positive) numbers belonging to S.
- For $n \in \mathbb{N}$, the set $\{i \in \mathbb{N} \mid i \leq n\} = \{0, \cdots, n\}$ is denoted by $[n]$.

Sets

- For F a finite set, its cardinality is denoted by $|F|$.
- For S a set:
  - let $\mathbb{P}(S)$ denote the set of subsets of S.
  - Let $\mathbb{S}_S$ be the set of permutations of S. That is, the set of bijective functions $\sigma : S \mapsto S$. For $S = [n-1]$ this set is denoted by $\mathbb{S}_n$.
  - for $d \in \mathbb{N}$, let S^d be the set of d-tuples of S. In particular, S^0 contains exactly one element, denoted by () and S^{d+1} is isomorphic to $S \times S^d$.
- For a pair of sets (S_0, S_1), let $S_0 \times S_1$ be the Cartesian product of S_0 and S_1, that is the set of pairs (s_0, s_1) with $s_i \in S_i$.
- Let $f : S_0 \to S_1$ be a function from S_0 to S_1,
  - For $F \subseteq S_0$, let $f(F)$ denotes the set $\{f(x) \mid x \in F\}$.
  - for $F \subseteq S$, let $f_{|F}$ denotes the function f whose domain is restricted to F.
  - For $F \subseteq S_1$, let $f^{-1}(F)$ denotes the set of $\{x \in S_0 \mid f(x) \in F\}$.
  - For $\boldsymbol{x} \in S^d$, let $f(\boldsymbol{x})$ denote $(f(x_0), \ldots, f(x_{d-1}))$.
- Similarly, for $\mathcal{R}$ a binary relation on $S_0 \times S_1$, for $\boldsymbol{x} \in S_0^d$, $\boldsymbol{y} \in S_1^d$, let $\boldsymbol{x}\mathcal{R}\boldsymbol{y}$ denote $x_i \mathcal{R} y_i$ for all $i \in [d-1]$.

Real numbers

- For r a real number:
  - $\lfloor r \rfloor$ is the greatest integer less than or equal to r.
  - $\lceil r \rceil$ is the least integer greater than or equal to r.
  - $|r|$ is the absolute value of r, that is, $|r|$ is r if $r \geq 0$, and is $-r$ otherwise.

Tuples

- Let $\boldsymbol{r} = (r_0, \ldots, r_{d-1})$ be a d-tuple of real numbers:
  - $\min(\boldsymbol{r})$ is the smallest of the r_i.
  - $\max(\boldsymbol{r})$ is the greatest of the r_i.
  - $\| \boldsymbol{r} \|$ denote $\sum_{i=0}^{d-1} |r_i|$.
- $\mathbf{0}$ denotes the d-tuple $(0, \cdots, 0)$, where the value of d is implicit.

2.2 Logics

In this section, general notions about logics are given.

A logical fragment can be characterized by:

- its number of alternation of quantifiers, or the absence of quantifiers,
- the order of its quantifiers: first order, second order, higher-order,
- its kind of quantifiers: existential quantifiers, universal quantifiers, modular quantifiers, threshold quantifiers, ...
- the number of variables (0, 2 or any),
- its vocabulary: interpreted or uninterpreted symbols, with or without function symbol,
- its universe: finite or infinite,
- its structure: integers, words.

Different kinds of logics are studied in this manuscript.

2.2.1 Syntax and semantic

Definition 2.2.1 (Universe)**.** A *universe* $\mathcal{U}$ is a nonempty set. In this manuscript, the universes $\mathcal{U}$ which are considered are of the form $\mathbb{N}$ or $\mathbb{Z}$ or $[n]$ for $n \in \mathbb{N}$.

Definition 2.2.2 (Vocabulary)**.** A *vocabulary* is a set of the form:

$$\mathcal{V} = \left\{(R_i/d_i)_{i<n}, (f_i/d'_i)_{i<p}, (c_i)_{i<q}\right\},$$

where n, p and q are either integers or ω (the cardinality of the set of integers).

For $i < n$, the R_i's are the *relation* symbols and their arity is d_i. For $i < q$, the c_i's are the *constant* symbols.

In general, arity are clear in the context and, for the sake of readability, are omitted. Hence vocabularies are usually considered as a set of symbols. Curly brackets are avoided when there is no ambiguity.

Vocabularies are mostly composed of the following symbols, which always occur in this order:

- Equality with a constant $c \in \mathbb{Z}$: "$\doteq c$". The set of equalities with a constant belonging to a set $R \subseteq \mathbb{Z}$: "$\doteq R$".
- The addition : "+".
- The multiplication : "$\times$".
- The equality "$\doteq$ ".

  Note that, in order to avoid ambiguity between the equality symbol and the formal equality of formulas, the symbol "=" is not used in logical formulas. For example, it is written "the formula ϕ, which is equal to $x \doteq y$, holds on a model A if $x^{\mathcal{A}} = y^{\mathcal{A}}$."
- The order relation : "$<$".

- Adding the constant 1 : "+1". Adding a constant $c \in \mathbb{Z}$: "$+c$". The set of functions $+c$ for $c \in R$ $R \subseteq \mathbb{Z}$: "$+R$".
- The unary minus function : "$-$" and more generally the unary functions "$c-$" which send x to $c-x$. The set of functions $c-$ for $c \in R$, $R \subseteq \mathbb{Z}$: "$R-$".
- The set of negative numbers : "$0>$". The set of integers less than a constant $c \in \mathbb{Z}$, "$c>$". The set of sets $c>$ for $c \in R$, $R \subseteq \mathbb{Z}$.
- The modular predicates : "$\mathrm{mod}\, m$" for a fixed integer $m \in \mathbb{N}$. The set "$\mathrm{mod}\, R$" of predicates "$\mathrm{mod}\, m$" for $m \in R$ and $R \subseteq \mathbb{N}^{>0}$.
- The floor function : "$\lfloor \cdot \rfloor$".
- The multiplication by a constant $c \in \mathbb{Z}$, the set "$\times R$" of functions "$\times c$" for $c \in R$ and $R \subseteq \mathbb{Z}$.
- A relation symbol : "R".
- A function symbol : "f".

Definition 2.2.3 (Structure)**.** Let $\mathcal{V}$ be a vocabulary. A $\mathcal{V}$*-structure* $\mathcal{S}$ over the universe $\mathcal{U}$ is a tuple

$$(\mathcal{U}, (R_i^{\mathcal{S}})_{i<n}, (f_i^{\mathcal{S}})_{i<p}, (c_i^{\mathcal{S}})_{i<q})$$

where $R_i^{\mathcal{S}} \subseteq \mathcal{U}^{d_i}$ for $i<n$, $f_i^{\mathcal{S}} : \mathcal{U}^{d_i} \to \mathcal{U}$ for $i<n$, and $c_i^{\mathcal{S}} \in \mathcal{U}$ for $i<q$.

For ς a relational symbol with arity d and $\iota \subseteq \mathcal{U}^{[d-1]}$, let $\mathcal{S}[\varsigma/\iota]$ denote the $(\mathcal{V} \cup \{\varsigma\})$-structure of universe $\mathcal{U}$ where $\varsigma^{\mathcal{S}[\varsigma/\iota]} = \iota$ and $\tau^{\mathcal{S}[\varsigma/\iota]} = \tau^{\mathcal{S}}$ for every symbol $\tau \in \mathcal{V} \setminus \{\varsigma\}$. The same definition is used for ς a constant symbol and $i \in \mathcal{U}$.

Let $\mathcal{Z}$ and $\mathcal{N}$ be the standard structure over integers and over non-negative integers respectively.

Definition 2.2.4 (Finite structure $\mathcal{S}_{|n}$)**.** Let $n \in \mathbb{N}$, let $\mathcal{V}$ be a vocabulary and let $\mathcal{S}$ be a $\mathcal{V}$-structure of cardinality at least n. Then $\mathcal{S}_{|n}$ is the $\mathcal{V}$-structure over the universe $[n-1]$ such that $c_i^{\mathcal{S}_{|n}} = \min\left(c_i^{\mathcal{S}}, n-1\right)$ and $R_i^{\mathcal{S}_{|n}} = R_i^{\mathcal{S}} \cap [n-1]^{d_i}$.

Note that for vocabularies $\mathcal{V} \subseteq \mathcal{W}$, each $\mathcal{W}$-structure is a $\mathcal{V}$-structure over the same universe.

The set of $\mathcal{V}$-terms is now defined.

Definition 2.2.5 (Terms)**.** Let $\mathcal{V}$ be a vocabulary. The set of $\mathcal{V}$*-terms* is defined by the grammar:

$$t(\mathcal{V}) ::= c_i \mid f_i(t_0, \ldots, t_{d_i'-1})$$

where c_i is a constant of $\mathcal{V}$, f_i is a function of $\mathcal{V}$ and the t_j's are $\mathcal{V}$-terms.

The *fragments* of first- and second-order logic used in this manuscript are now defined.

Definition 2.2.6 ($\mathcal{V}$-Formulas)**.** Let $\mathcal{V}$ be a vocabulary. The set of quantifier-free $\mathcal{V}$-formulas, denoted by $\Sigma_0[\mathcal{V}]$ and $\Pi_0[\mathcal{V}]$, is defined by the grammar:

$$\Sigma_0[\mathcal{V}] ::= \neg\phi_0 \mid \phi_0 \wedge \phi_1 \mid \phi_0 \vee \phi_1 \mid R_i(t_0, \ldots, t_{d_i-1}) \mid t_0 \doteq t_1$$

where the t_i's are $\mathcal{V}$-terms and the ϕ_i's are $\Sigma_0[\mathcal{V}]$-formulas.

The sets $\Sigma_i[\mathcal{V}]$, $\Pi_i[\mathcal{V}]$ and $D_i[\mathcal{V}]$ are defined by mutual induction on i. For $i \in \mathbb{N}$ let $D_i[\mathcal{V}]$ be defined by the grammar:

$$D_i[\mathcal{V}] ::= \neg\phi_0 \mid \phi_0 \wedge \phi_1 \mid \phi_0 \vee \phi_1 \mid \psi$$

where ϕ_i belongs to $D_i[\mathcal{V}]$ and ψ belongs to $\Sigma_i[\mathcal{V}]$ or to $\Pi_i[\mathcal{V}]$.

For $i \in \mathbb{N}^{\geq 0}$, let $\Sigma_i[\mathcal{V}]$ be defined by the grammar :

$$\Sigma_i[\mathcal{V}] ::= \exists x.\psi \mid \phi_0 \wedge \phi_1 \mid \phi_0 \vee \phi_1 \mid \neg\chi \mid \xi$$

where $\psi \in \Sigma_i[\mathcal{V}, x]$ the ϕ_i's are $\Sigma_i[\mathcal{V}]$-formulas, χ is a $\Pi_i[\mathcal{V}]$-formula and ξ is a $D_{i-1}[\mathcal{V}]$-formula.

Similarly, let $\Pi_i[\mathcal{V}]$ be defined by the grammar:

$$\Pi_i[\mathcal{V}] ::= \forall x.\psi \mid \phi_0 \wedge \phi_1 \mid \phi_0 \vee \phi_1 \mid \neg\chi \mid \xi$$

where $\psi \in \Pi_i[\mathcal{V}, x]$, the ϕ_i's are $\Pi_i[\mathcal{V}]$-formulas, χ is a $\Sigma_i[\mathcal{V}]$-formula and ξ is a $D_{i-1}[\mathcal{V}]$-formula.

Let $\mathsf{FO}[\mathcal{V}]$ be the union of the fragments $\Pi_i[\mathcal{V}]$ for $i \in \mathbb{N}$.

For a logical fragment $\mathcal{L}[\mathcal{V}]$, let $\exists\mathsf{MSO}\mathcal{L}[\mathcal{V}]$ denote the set of formulas of the form $\exists R_0, \ldots, R_n.\psi$ where ψ is a $\mathcal{L}[\mathcal{V}, R_0, \ldots, R_n]$-formula and where the arity of the R_i's is 1.

Let us assume that the vocabulary $\mathcal{V}$ contains at most two constant symbols x and y. The set of two-variable $\mathcal{L}[\mathcal{V}]$-formulas, denoted by $\mathcal{L}^2[\mathcal{V}]$, is the set of formulas where the only quantified first-order variables are x and y.

A formula is said to be in prenex normal-form if it begins by a sequence of quantifiers and that those quantifiers are followed by a quantifier-free formula.

Our definition differs from the standard definition of $\Sigma_i[\mathcal{V}]$ and of $\Pi_i[\mathcal{V}]$ which only considers formulas in prenex normal form. The standard definition is equivalent to our definition over the set of formulas in prenex normal form. Furthermore, it is easy to prove that that there is an inductive algorithm which transforms each $\Sigma_i[\mathcal{V}]$-formula into an equivalent $\Sigma_i[\mathcal{V}]$-formula in prenex normal form, hence there is no loss of generality in accepting our definition. Using Definition 2.2.6 allows us write more easily the formulas in this manuscript. Furthermore, Definition 2.2.6 allows us to give a precise sens to $\Pi_2^2[\mathcal{V}]$, the set of formulas with two-variables and only one alternation of quantifiers.

2.2.1.1 Semantic

The notion of semantic of a formula is now introduced.

Definition 2.2.7 (Interpretation and Model)**.** Let $\mathcal{V}$ be a vocabulary, $\mathcal{S}$ be a $\mathcal{V}$-structure over an universe $\mathcal{U}$ as in Definition 2.2.1. That is, $\mathcal{U}$ is either $\mathbb{N}$ or $[n]$ for some $n \in \mathbb{N}$.

Let ϕ be a $\mathcal{V}$-formula. We define the satisfaction relation $\mathcal{S} \models \phi$ by induction over ϕ as follows:

- $\mathcal{S} \models c \doteq c'$ if and only if $c^{\mathcal{S}} = c'^{\mathcal{S}}$,
- $\mathcal{S} \models R(t)$ if and only if $t^{\mathcal{S}} \in R^{\mathcal{S}}$,
- $\mathcal{S} \models \psi_0 \vee \psi_1$ if and only if $\mathcal{S} \models \psi_0$ or $\mathcal{S} \models \psi_1$,
- $\mathcal{S} \models \psi_0 \wedge \psi_1$ if and only if $\mathcal{S} \models \psi_0$ and $\mathcal{S} \models \psi_1$,
- $\mathcal{S} \models \neg\psi$ if and only if $\mathcal{S} \not\models \psi$,
- $\mathcal{S} \models \exists x.\psi$ if and only if there exists $n \in \mathcal{U}$ such that $\mathcal{S}[x/n] \models \psi$,

- $\mathcal{S} \models \forall x.\psi$ if and only if for all $n \in \mathcal{U}$, $\mathcal{S}[x/n] \models \psi$,
- $\mathcal{S} \models \exists R.\psi$ if and only if there exists $N \subseteq \mathcal{U}$ such that $\mathcal{S}[R/N] \models \psi$,
- $\mathcal{S} \models \forall R.\psi$ if and only if for all $N \subseteq \mathcal{U}$, $\mathcal{S}[R/N] \models \psi$.

A $\mathcal{V}$-structure $\mathcal{S}$ is said to be a model of ϕ if $\mathcal{S} \models \phi$.

For a vocabulary $\mathcal{V}$, and a logical fragment $\mathcal{L}$, the $\mathcal{L}[\mathcal{V} \cup \{x_0, \cdots, x_{d-1}\}]$-formulas are said to be $\mathcal{L}[\mathcal{V}]$-formulas with arities d. The x_i's for $i \in [d]$, are called the free variables and do not belong to $\mathcal{V}$. Given some $\mathcal{V}$-structure $\mathcal{S}$, the semantics of a formula is defined recursively as usual.

Definition 2.2.8 (Definability)**.** Let $d \in \mathbb{N}$ and $\phi(x_0, \cdots, x_{d-1})$ be a formula with d free variables in a logic $\mathcal{L}[\mathcal{V}]$. For a $\mathcal{V}$-structure $\mathcal{S}$, the formula ϕ defines in $\mathcal{S}$ the d-ary set $\phi(\boldsymbol{x})^{\mathcal{S}} = \left\{\boldsymbol{x} \in \mathcal{U}^d \mid \mathcal{S} \models \phi(\boldsymbol{x})\right\}$.

A set $R \subseteq \mathcal{U}^d$ is said to be $\mathcal{L}[\mathcal{V}]$-definable in $\mathcal{S}$ if there exists $\phi(x_0, \cdots, x_{d-1}) \in \mathcal{L}[\mathcal{V}]$ such that $R = \phi(x_0, \cdots, x_{d-1})^{\mathcal{S}}$. Furthermore, if f is a function from $\mathcal{U}^d$ to $\mathcal{U}$, then f is $\mathcal{L}[\mathcal{V}]$-definable if its graph is $\mathcal{L}[\mathcal{V}]$-definable.

2.2.1.2 Explicitly writing some formulas

In this manuscript, it is often needed to write explicitly some formulas. In order to do this, some abbreviations are now introduced.

Let $\phi_0 \Longrightarrow \phi_1$ be an abbreviation for $(\neg\phi_0) \vee \phi_1$ and let $\phi_0 \Longleftrightarrow \phi_1$ be an abbreviation for $(\phi_0 \Longrightarrow \phi_1) \wedge (\phi_1 \Longrightarrow \phi_0)$.

The following notation considers formulas which define some functions.

Notation 2.2.9 (Notation for functions)**.** Let $d, d' \in \mathbb{N}$, and let $\mathcal{V}$ be a vocabulary. Let $\mathcal{U}$ be an universe. The notation $\phi(x_0, \ldots, x_{d-1}; y_0, \ldots, y_{d'-1})$ denotes the fact that, for every d-tuple $\boldsymbol{n} \in \mathcal{U}^d$, there exists exactly one d'-tuple $\boldsymbol{n'} \in \mathcal{U}^{d'}$ such that $\mathcal{S}[\boldsymbol{x}/\boldsymbol{n}][\boldsymbol{y}/\boldsymbol{n'}] \models \phi(x_0, \ldots, x_{d-1}, y_0, \ldots, y_{d'-1})$.

Then, let $\phi(\boldsymbol{n})$ denote $\boldsymbol{n'}$.

The following notation states that some variables are interpreted by the minimal value such that a formula holds.

Notation 2.2.10. Let F be a finite ordered set. Let $(\phi_i)_{i \in F}$ be a set of $\mathsf{FO}[\mathcal{V}]$-formulas. Let $i \in F$.

A $\mathsf{FO}[\mathcal{V}]$-formula $\min_i\{\phi_i\}$ is introduced which states that ϕ_i holds and i is minimal with this property. Let:

$$\min_i\{\phi_i\} = \phi_i \wedge \bigwedge_{j \in F \mid j < i} \neg\phi_j.$$

Similarly, let $\boldsymbol{x} = (x_0, \cdots, x_{d-1})$ be a tuple of variables and let $\phi(\boldsymbol{x})$ be a $\mathsf{FO}[\mathcal{V}]$-formula. A $\mathsf{FO}[\mathcal{V}, <]$-formula $\min_{\boldsymbol{x}}\{\phi_i(\boldsymbol{x})\}$ is introduced, which states that $\phi(\boldsymbol{x})$ holds and $\boldsymbol{x}$ is lexicographically minimal with this property. Let:

$$\min_{\boldsymbol{x}}\{\phi_i(\boldsymbol{x})\} = \phi(\boldsymbol{x}) \wedge \forall \boldsymbol{y}.\left\{\bigvee_{j=0}^{d-1}\left[y_j < x_j \wedge \bigwedge_{k=0}^{j-1} y_k \doteq x_k\right]\right\} \Longrightarrow \{\neg\phi_i(\boldsymbol{y})\}.$$

Finally, for ϕ_i a family of $\mathsf{FO}[\mathcal{V}]$-formulas, let $\min_{i,\boldsymbol{x}}\{\phi_i(\boldsymbol{x})\}$ be a $\mathsf{FO}[\mathcal{V}, <]$-formula which states that $\phi_i(\boldsymbol{x})$ holds and $(i, \boldsymbol{x})$ is lexicographically minimal with this property. Let:

$$\min_{i,\boldsymbol{x}}\{\phi_i(\boldsymbol{x})\} = \min_i\{\exists \boldsymbol{y}.\phi_i(\boldsymbol{y})\} \wedge \min_{\boldsymbol{x}}\{\phi_i(\boldsymbol{x})\}.$$

Notations for implications and equivalences are standard. A notation of the form "if then else" is also needed. It is now introduced.

Notation 2.2.11. Let F be a finite set. Let ψ be a $\mathsf{FO}[\mathcal{V}]$-formula. For $i \in F$, let $\phi_i(\boldsymbol{x})$ and $\chi_i(\boldsymbol{x})$ be $\mathsf{FO}[\mathcal{V}]$-formulas. Let

$$\langle \bigvee_{i \in F} \exists \boldsymbol{x}.\phi_i(\boldsymbol{x}) \mid \chi_i(\boldsymbol{x}) \mid \psi \rangle$$

be a $\mathsf{FO}[\mathcal{V}]$-formula which states that if there exists $i \in F$ and $\boldsymbol{n} \in \mathbb{N}^d$ such that $\phi_i(\boldsymbol{n})$ holds, then $\chi_i(\boldsymbol{n})$, otherwise ψ. Formally, the formula is:

$$\left\{ \bigvee_{i \in F} \exists \boldsymbol{x}.\phi_i(\boldsymbol{x}) \wedge \chi_i(\boldsymbol{x}) \right\} \vee \left\{ \bigwedge_{i \in F} \forall \boldsymbol{x}.\neg\phi_i(\boldsymbol{x}) \wedge \psi \right\}.$$

In general, the two preceding notations are used together, stating that, if there are some $i \in F$ and $\boldsymbol{x} \in \mathbb{N}^d$, the minimal one are used in $\chi_i(\boldsymbol{x})$.

Functions Let us say a word about functions in this manuscript. Usually in finite model theory and in two-variable logic, the vocabulary does not contain function symbols, hence the only terms are the constants. Instead, formally, unary functions f are replaced with a binary relation $f(x, y)$, such that for every $n \in \mathcal{U}$ there is at most one $r \in \mathcal{U}$ such that $f(n, r)$ holds. For example, the addition of 1 is denoted by the binary relation $+1(x; y)$ interpreted in $[n]$ by $\{(x, x+1) \mid x < n\}$. The distinction is important because over the universe $[n]$, the value of $n + 1$ is undefined.

On the other hand, for the sake of clarity, "$+1(x, y)$" is written "$x + 1 \doteq y$", and more generally if f is a unary function, then "$f(x; y)$" is written "$f(x) \doteq y$".

In particular, most vocabularies considered in this manuscript contain the successor function. Hence, the notation $x + c$ for $c \in \mathbb{N}$ is used, as an abbreviation for $x + (1 + (\ldots(1 + 1)\ldots))$.

In this manuscript, we specify the number of alternations of quantifiers and the number of variables used in formulas. For the sake of simplicity, we introduce abbreviations such as $f(g(x))$. The following lemmas explain how to encode formally all of those abbreviations in fragments of the logic.

Lemma 2.2.12. *Let f and g be two unary function symbols, then $f(g(x)) \doteq y$ is equivalent to a $\Sigma_1[f, g]$-formula.*

Proof. The formula $f(g(x)) = y$ is equivalent to the $\Sigma_1[f, g]$-formula:

$$\exists z.g(x) \doteq z \wedge f(z) \doteq y.$$

Clearly, if $g^{\mathcal{S}}(x^{\mathcal{S}})$ is not defined then this formula does not hold in $\mathcal{S}$, which is the intended behaviour as $f(g(x))$ is not defined either. □

For R a unary relation symbol, the notation $R(f(g(x)))$ can be used in two-variable logic.

Lemma 2.2.13. *Let f and g be two unary function symbols, and let R be a unary relation symbol, then $R(f(g(x)))$ is equivalent to a $\Sigma_1^2[f, g, x]$-formula.*

Proof. The formula $R(f(g(x)))$ is equivalent to

$$\exists y.\{g(x) \doteq y \wedge (\exists x.f(y) \doteq x \wedge R(x))\}.$$

□

The two preceding lemmas extend easily to the application of more than two function symbols.
In general, $f(g(x)) \doteq y$ is not equivalent to a $\Sigma_1^2[f,x,y]$-formula. Indeed, a formula defining the set

$$\{(x,y) \mid f(g(x)) = y\}$$

should quantify a variable to store the value of $g(x)$, but in two-variable logic, there is no guarantee that such a variable is available.

Constants Similarly, for the sake of simplicity, our formula uses constant symbols, such as 2 or (last -2) where the value "last" corresponds to the greatest integer of the universe.

Lemma 2.2.14. *The formulas $x \doteq c$ and $x \doteq \text{last} - c$ for $c \in \mathbb{N}$, are equivalent to a $\Sigma_2^2[+1,x]$-formula and to a $\Pi_2^2[+1,x]$-formula.*

Proof. By symmetry, the proofs are similar for $x \doteq c$ and $x \doteq \text{last} - c$. Therefore, only the first case is proven. The proof proceeds by induction over c. If $c = 0$ then $x \doteq 0$ is equivalent to $\forall y.y + 1 \neq x$. If $c \in \mathbb{N}^{>0}$, then $x \doteq c$ is equivalent to

$$\exists y.y + 1 \doteq x \wedge y \doteq (c-1)$$

and to

$$\{\exists y.y + 1 \doteq x\} \wedge \{\forall y.y + 1 \doteq x \Longrightarrow y \doteq c - 1\}.$$

□

This result allows us to use constants as parameters of unary relations, even when the vocabulary does not contain the constants.

Lemma 2.2.15. *The formulas $R(c)$ and $R(\text{last} - c)$, for $c \in \mathbb{N}$, are equivalent to a $\Sigma_2^2[+1]$-formula and to a $\Pi_2^2[+1]$-formula.*

Proof. As in the previous proof, we consider only the case $R(c)$ since the other one is similar. The formula $R(c)$ is equivalent to $\exists x.x \doteq c \wedge R(x)$ and to $\forall x.x \doteq c \Longrightarrow R(x)$. □

2.2.2 Quantifier elimination for fragments of FO[+]

This manuscript mostly considers logics which admit the elimination of quantifiers – the main exception being $\mathsf{FO}[+,V_b]$, considered in Theorem 2.3.5, and the logics with uninterpreted functions considered in Section 4.3. Note that a quantifier-free formula is simpler to analyze. In general, algorithm of elimination of quantifiers output formulas whose size is not polynomially bounded in the size of the input, but this is generally not a problem as the quantifier-free formulas are used in our proofs and not in our algorithms.

In this section, the quantifier elimination algorithm for logic over integers are considered. Let us first recall the well-known result of Presburger.

Theorem 2.2.16 ([Pre27])**.** *Every $\mathsf{FO}[+]$-formula is equivalent over $\mathbb{N}$ and over $\mathbb{Z}$ to a quantifier-free $\Sigma_0[\doteq_{\mathbb{N}},+,<,\text{mod}]$-formula.*

In this manuscript, Cooper's algorithm [Coo72] is used instead of Presburger's algorithm. The main interest of Cooper's algorithm over Presburger's algorithm, in this manuscript, is that Cooper's algorithm also holds for some fragments of $\mathsf{FO}[<,\text{mod}]$.

Let $M \subseteq \mathbb{N}$, it represents the set of possible modulus. In this manuscript, M is always equal, either to a singleton, either to $\mathbb{N}$, or to the set of integers coprime to an integer b fixed. Cooper's algorithm is now given for the vocabulary $\{\doteq_{\mathbb{Z}},<,+_{\mathbb{N}},-_{\mathbb{Z}},\text{mod}\,M\}$. The algorithm $\text{Cooper}^{\mathbb{I}}$, for $\mathbb{I}$ being $\mathbb{N}$ or $\mathbb{Z}$:

- takes as input a $\mathsf{FO}[\doteq\mathbb{Z},<,+\mathbb{N},-\mathbb{Z},\mathrm{mod}\,M]$-formula $\phi(\boldsymbol{x})$ and
- returns a Boolean combination of atomic formulas of the form $x_i + c \sim x_j$, $x_i \sim c$, and $x_i \equiv k \mod m$ with $\sim$ belonging to $\{<,\doteq,>\}$, $c \in \mathbb{N}$, $m \in M$ and $k \in [m-1]$.

The input and the output of the algorithm are two equivalent formulas.

Definition 2.2.17 ($\mathrm{Cooper}^{\mathbb{Z}}$)**.** Let $\phi(\boldsymbol{x})$ be a $\mathsf{FO}[\doteq\mathbb{Z},<,+\mathbb{N},-\mathbb{Z},\mathrm{mod}\,M]$-formula and let $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$ be the $\Sigma_0[\doteq\mathbb{Z},<,+\mathbb{N},-\mathbb{Z},\mathrm{mod}\,M]$-formula defined by induction on ϕ as follows:

- If $\phi(\boldsymbol{x})$ is an atomic formula then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x}) = \phi(\boldsymbol{x})$.
- If $\phi(\boldsymbol{x})$ is of the form $\neg\psi(\boldsymbol{x})$, then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x}) = \neg\Big(\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})\Big)$.
- If $\phi(\boldsymbol{x})$ is of the form $\psi_0(\boldsymbol{x}) \vee \psi_1(\boldsymbol{x})$, then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x}) = \mathrm{Cooper}^{\mathbb{Z}}(\psi_0)(\boldsymbol{x}) \vee \mathrm{Cooper}^{\mathbb{Z}}(\psi_1)(\boldsymbol{x})$.
- If $\phi(\boldsymbol{x})$ is of the form $\psi_0(\boldsymbol{x}) \wedge \psi_1(\boldsymbol{x})$, then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x}) = \mathrm{Cooper}^{\mathbb{Z}}(\psi_0)(\boldsymbol{x}) \wedge \mathrm{Cooper}^{\mathbb{Z}}(\psi_1)(\boldsymbol{x})$.
- If ϕ is of the form $\exists y.\psi(y,\boldsymbol{x})$ then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$ is defined as follows. Let $\psi'(y,\boldsymbol{x}) = \mathrm{Cooper}^{\mathbb{Z}}(\psi)(y,\boldsymbol{x})$. By induction, $\psi'(y,\boldsymbol{x})$ is a Boolean combination of atomic formulas of the form:
  - $y < t$ or $y = t$ or $y > t$, where t is either an integer, a term of the form $x_i + c$ or a term of the form $c - x_i$ with $c \in \mathbb{Z}$, or
  - $y \equiv c_i \mod m_i$, where m_i belongs to M and $c_i \in [m_i - 1]$.

  Let m be the least common multiple of the m_i. Let $T(\psi'(y,\boldsymbol{x}))$ be the set containing the integer 0 and the terms t. Then let $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$ be:

$$\bigvee_{t\in T(\psi'(y,\boldsymbol{x}))}\ \bigvee_{j\in\{-m,\ldots,m\}} \psi'(t+j,\boldsymbol{x}).$$

- Finally, if $\phi(\boldsymbol{x})$ is of the form $\forall y.\psi(y,\boldsymbol{x})$, then

$$\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x}) = \neg\,\mathrm{Cooper}^{\mathbb{Z}}(\exists y.\neg\psi)(y,\boldsymbol{x}).$$

Example 2.2.18. Let ϕ be the formula

$$\exists x.(x \doteq y \wedge x \doteq 0) \vee (x + 4 \leq y \wedge x \equiv 0 \mod 2).$$

Then $T(\phi) = \{y, y-4, 0\}$ and $m = 2$. Then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)$ is equal to :

$$\begin{array}{l}
\bigvee_{i=-2}^{2}\{(\quad i\doteq y\wedge\quad i\doteq 0)\vee(\quad i+4\leq y\wedge\quad i\equiv 0 \mod 2)\}\vee\\
\bigvee_{i=-6}^{-2}\{(y+i\doteq y\wedge y+i\doteq 0)\vee(y+i+4\leq y\wedge y+i\equiv 0 \mod 2)\}\vee\\
\bigvee_{i=-2}^{2}\{(y+i\doteq y\wedge y+i\doteq 0)\vee(y+i+4\leq y\wedge y+i\equiv 0 \mod 2)\}.
\end{array}$$

The algorithm of [Coo72] tends to simplify the formula when possible. Some steps that decrease the length of the formula are ignored. For example, in the definition of $\mathrm{Cooper}^{\mathbb{Z}}(\phi)$, the symbol j takes its values in $\{-m,m\}$ whereas in [Coo72], it takes its values either in $[m-1]$ or in $\{1,\ldots,m\}$, depending of the type of predicate where t occurs in ψ and of the number of negation before the occurrence of this predicate. Furthermore, instead of considering negative values for j, [Coo72] introduced a formula similar to $\psi'(y,\boldsymbol{x})$, where y behaves similarly to $-\infty$ for the predicates $<$, $\doteq$ and $>$.

Let us prove that the algorithm $\mathrm{Cooper}^{\mathbb{Z}}$ behaves as expected.

First-order logic $\mathsf{FO}[\mathcal{V}]$	Equivalent quantifier-free logic $\Sigma_0[\mathcal{W}]$
$\mathsf{FO}[\ <, -, \bmod M\ ]$	$\Sigma_0[\ \doteq\mathbb{Z}, \doteq, <, +\mathbb{N}, \mathbb{Z}-, 0>, <-, \bmod M\ ]$
$\mathsf{FO}[\ 0>, +1, -, \bmod M\ ]$	$\Sigma_0[\ \doteq\mathbb{Z}, \doteq, +\mathbb{N}, \mathbb{Z}-, 0>, \bmod M\ ]$
$\mathsf{FO}[\ +1, -, \bmod M\ ]$	$\Sigma_0[\ \doteq\mathbb{Z}, \doteq, +\mathbb{N}, \mathbb{Z}-, \bmod M\ ]$
$\mathsf{FO}[\ \doteq 0, <, \bmod M\ ]$	$\Sigma_0[\ \doteq\mathbb{Z}, \doteq, <, +\mathbb{N}, 0>, \bmod M\ ]$
$\mathsf{FO}[\ <, \bmod M\ ]$	$\Sigma_0[\ \doteq, <, +\mathbb{N}, \bmod M\ ]$
$\mathsf{FO}[\ 0>, +1, \bmod M\ ]$	$\Sigma_0[\ \doteq\mathbb{Z}, \doteq, +\mathbb{N}, 0>, \bmod M\ ]$
$\mathsf{FO}[\ \doteq 0, +1, \bmod M\ ]$	$\Sigma_0[\ \doteq\mathbb{Z}, \doteq, +\mathbb{N}, \bmod M\ ]$
$\mathsf{FO}[\ +1, \bmod M\ ]$	$\Sigma_0[\ \doteq, +\mathbb{N}, \bmod M\ ]$

Table 2.1: List of equivalent logics over $\mathbb{Z}$

Proposition 2.2.19. Let $M \subseteq \mathbb{N}^{>0}$. Let $\mathsf{FO}[\mathcal{V}]$ be a logic belonging to the left column of Table 2.1 and let $\Sigma_0[\mathcal{W}]$ be a logic of the second column. Let $\phi(\boldsymbol{x}) \in \mathsf{FO}[\mathcal{V}]$, then $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$ belongs $\Sigma_0[\mathcal{W}]$.

For all $\boldsymbol{n} \in \mathbb{Z}^d$, let $\mathcal{Z}' = \mathcal{Z}[\boldsymbol{x}/\boldsymbol{n}]$. Then $\mathcal{Z}' \models \phi(\boldsymbol{x})$ is equivalent to $\mathcal{Z}' \models \mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$.

Note that [Smo91, p. 322] states that some logics, such as $\mathsf{FO}[<,+1,0]$ and $\mathsf{FO}[+1,0]$ admits quantifier elimination over integers. It states, without proof nor reference, that it suffices to apply Presburger's algorithm to obtain this result. The vocabulary $\mathcal{W}$ of the second column of Table 2.2 and 2.1 is systematically constructed from $\mathcal{V}$ using the following rules:

(a). If $<$ belongs to V then $<$ belongs to W.

(b). Either $<$ or $+1$ belongs to V.

(c). $+\mathbb{N}$ and $\doteq$ belong to $\mathcal{W}$.

(d). If $0>$ belongs to V then $0>$ belongs to W.

(e). If $-$ belongs to V then $\mathbb{Z}-$ belongs to W.

(f). If $-$ belongs to V and $<$ belongs to V then $<-$ belongs to W.

(g). If $0>$, $\doteq 0$ or $-$ belong to $\mathcal{V}$ then $\doteq\mathbb{Z}$ belongs to W,

The proof of this proposition follows closely the proof of [Coo72].

Proof. Let us first prove by induction on $\phi(\boldsymbol{x})$ that $\mathrm{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$ belongs to $\Sigma_0[\mathcal{W}]$.

If ϕ is an atomic formula, there is nothing to prove as the atomic formulas belong to $\Sigma_0[\mathcal{W}]$. If ϕ is $\neg\psi_0$, $\psi_0 \vee \psi_1$, $\psi_0 \wedge \psi_1$ or $\forall y.\psi(y,\boldsymbol{x})$, the induction is trivial. Let us suppose that ϕ is $\exists y.\psi(y,\boldsymbol{x})$.

The set $T(\psi'(y,\boldsymbol{x}))$ of terms contains only terms of the form:

- a variable x_i if $\doteq$ belongs to W,
- a constant k, if $\doteq\mathbb{N}$ belongs to W,
- a variable plus a constant, $x_i + k$, if $+\mathbb{N}$ belongs to W and
- a constant minus a variable, $k - x_i$, $\mathbb{Z}-$ belongs to W

where the k's belong to $\mathbb{Z}$. The terms $t + j$ with $t \in T(\psi'(y,\boldsymbol{x}))$ and $j \in [m]$ are of the form

- if $\doteq$ belongs to W then $x_i + k$, a variable plus a constant,
- if $\doteq\mathbb{N}$ belongs to W then k, a constant,
- if $\mathbb{Z}-$ belongs to W then $k - x_i$, a constant minus a variable.

Then $\text{Cooper}^{\mathbb{Z}}(\phi)$ belongs to $\Sigma_0[\mathcal{W}]$.

Let us now prove the equivalence of $\phi(\boldsymbol{x})$ and of $\text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$. Let $\boldsymbol{n} \in \mathbb{Z}^d$ and let $\mathcal{Z}' = \mathcal{Z}[\boldsymbol{x}/\boldsymbol{n}]$. Let us prove that $\mathcal{Z}' \models \phi(\boldsymbol{x})$ is equivalent to $\mathcal{Z}' \models \text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$. The proof goes by induction on ϕ. The only non-trivial case is when $\phi(\boldsymbol{x})$ is of the form $\exists y.\psi(y,\boldsymbol{x})$.

Let $\psi'(y,\boldsymbol{x}), T(\psi')$ and m be as in Definition 2.2.17. By the induction hypothesis $\psi(y,\boldsymbol{x})$ is equivalent to $\psi'(y,\boldsymbol{x})$. Hence, it remains to prove that $\mathcal{Z}' \models \exists y.\psi'(y,\boldsymbol{x})$ is equivalent to $\mathcal{Z}' \models \text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$.

Let us first assume that $\mathcal{Z}' \models \text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$, and let us prove that $\mathcal{Z}' \models \exists y.\psi'(y,\boldsymbol{x})$. Since $\mathcal{Z}' \models \text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$, there exists $t \in T(\psi')$ and $j \in [m]$ such that $\mathcal{Z}' \models \psi'(t + j,\boldsymbol{x})$, hence $\mathcal{Z}'[y/t'^{\mathcal{Z}'} + j] \models \psi'(y,\boldsymbol{x})$ and then $\mathcal{Z}' \models \exists y.\psi'(y,\boldsymbol{x})$.

Let us now assume that $\mathcal{Z}' \models \exists y.\psi'(y,\boldsymbol{x})$, and let us prove that $\mathcal{Z}' \models \text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$. Two cases must be considered, depending on whether there exists $n \in \mathbb{N}$ such that $\mathcal{Z}'[y/n] \models \psi'(y,\boldsymbol{x})$ or whether there exists $n \in \mathbb{N}$ such that $\mathcal{Z}'[y/-n] \models \psi'(y,\boldsymbol{x})$. Let us assume that $\mathcal{Z}'[y/n] \models \psi'(y,\boldsymbol{x})$ holds, the other case is similar by symmetry.

Let $n \in \mathbb{N}$ be the least non-negative integer such that $\mathcal{Z}'[y/n] \models \psi'(y,\boldsymbol{x})$. Let us prove that n is of the form $t + j$ with $t \in T(\phi')$ and $j \in [m]$, which implies that $\mathcal{Z}' \models \text{Cooper}^{\mathbb{Z}}(\phi)(\boldsymbol{x})$. For the sake of contradiction, let us assume that n is not of the form $t + j$ with $t \in T(\phi')$. Hence $n > m$. Then, by an easy induction on the subterms ξ of ϕ', $\mathcal{Z}'[y/n] \models \xi$ is equivalent to $\mathcal{Z}'[y/n - m] \models \xi$, which contradicts the minimal hypothesis about n. □

Let us now give a similar result for logics over non-negative integers.

Definition 2.2.20 ($\text{Cooper}^{\mathbb{N}}$)**.** Let $\phi(\boldsymbol{x})$ be a $\mathsf{FO}[\doteq\mathbb{N}, <, +\mathbb{N}, \text{mod } M]$-formula. Let $\phi'(\boldsymbol{x})$ be the formula $\phi(\boldsymbol{x})$ where each occurrence of $\exists x.\psi$ is replaced by $\exists x.x \geq 0 \wedge \psi$ and where each occurrence of $\forall x.\psi$ is replaced by $\forall x.(x > 0 \Longrightarrow \psi)$. Let $\phi''(\boldsymbol{x})$ be $\text{Cooper}^{\mathbb{Z}}(\phi')(\boldsymbol{x})$. Finally, let $\text{Cooper}^{\mathbb{N}}(\phi')(\boldsymbol{x})$ be $\phi''(\boldsymbol{x})$ where each atomic formula of the form $x < c$ is replaced by False if $c \leq 0$, and by $\bigvee_{i=0}^{c-1} x \doteq i$ otherwise.

Proposition 2.2.21. Let $M \subseteq \mathbb{N}^{>0}$. Let $\mathsf{FO}[\mathcal{V}]$ be a logic belonging to the left column of Table 2.2 and let $\Sigma_0[\mathcal{W}]$ be a logic of the second column. Let $\phi(\boldsymbol{x}) \in \mathsf{FO}[\mathcal{N}]$, then $\text{Cooper}^{\mathbb{N}}(\phi)(\boldsymbol{x})$ belongs to the logic $\Sigma_0[\mathcal{W}]$.

First-order logic $\mathsf{FO}[\mathcal{V}]$	Equivalent quantifier-free logic $\Sigma_0[\mathcal{W}]$
$\mathsf{FO}[\ \doteq 0,\ <,\ \text{mod } M\ ]$	$\Sigma_0[\ \doteq\mathbb{N},\ \doteq,\ <,\ +\mathbb{N},\ \text{mod } M\ ]$
$\mathsf{FO}[\quad +1,\ \text{mod } M\ ]$	$\Sigma_0[\ \doteq\mathbb{N},\ \doteq,\quad +\mathbb{N},\ \text{mod } M\ ]$

Table 2.2: List of equivalent logics over $\mathbb{N}$

For all $\boldsymbol{n} \in \mathbb{Z}^d$, let $\mathcal{N}' = \mathcal{Z}[\boldsymbol{x}/\boldsymbol{n}]$. Then $\mathcal{N}' \models \phi(\boldsymbol{x})$ is equivalent to $\mathcal{N}' \models \text{Cooper}^{\mathbb{N}}(\phi)(\boldsymbol{x})$.

Proof. The equivalence is a simple corollary of Proposition 2.2.21. Concerning the vocabulary, it suffices to remark that the only introduced predicates are of the form $x < 0$. And those predicates does not appear in $\text{Cooper}^{\mathbb{N}}(\phi')(\boldsymbol{x})$. □

2.2.3 Sections, diagonals and subsets

In this section some notations are introduced to transform sets into sets which are, intuitively, smaller.

Definition 2.2.22 (Section, diagonal and straight subspace)**.** Let $d \geq 1$, $R \subseteq \mathbb{N}^d$, i, j be distinct elements of $[d-1]$, and $c \in \mathbb{N}$. Then we define the section $\mathrm{sec}(R; x_i = c) \subseteq \mathbb{N}^{d-1}$ as the set obtained from R by fixing the i-th component to c:

$$\mathrm{sec}(R; x_i = c) = \left\{(x_0, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{d-1}) \in \mathbb{N}^{d-1} \mid (x_0, \cdots, x_{i-1}, c, x_{i+1}, \cdots, x_{d-1}) \in R\right\}.$$

Similarly, the *diagonal* $\mathrm{diag}(R; x_i = x_j + c) \subseteq \mathbb{N}^{d-1}$ is defined as follows:

$$\mathrm{diag}(R; x_i = x_j + c) = \left\{(x_0, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{d-1}) \in \mathbb{N}^{d-1} \mid (x_0, \cdots, x_{i-1}, x_j + c, x_{i+1}, \cdots x_{d-1}) \in R\right\}.$$

The set of *straight subspaces* of R of dimension $d' \in [d-1]$ is defined by induction on $d - d'$ as $\{R\}$ if $d' = d$, and as the set of sections and diagonals of straight subspaces of dimension $d' + 1$ otherwise.

Example 2.2.23. The sections and diagonals of the addition relation $x_0 + x_1 = x_2$ are now studied. Let $c \in \mathbb{N}$. One has:

$$\begin{array}{rlll}
\mathrm{sec}(+; x_0 = c) & = \mathrm{sec}(+; x_1 = c) & = \{(n, n+c) \mid n \in \mathbb{N}\}, \\
 & \mathrm{sec}(+; x_2 = c) & = \{(n, c-n) \mid n \leq c\}, \\
\mathrm{diag}(+; x_0 = x_1 + c) & = \mathrm{diag}(+; x_1 = x_0 + c) & = \{(n, 2n+c) \mid n \in \mathbb{N}\}, \\
 & \mathrm{diag}(+; x_2 = x_1 + c) & = \{(c, n) \mid n \in \mathbb{N}\}, \\
\mathrm{diag}(+; x_0 = x_2 + c + 1) & = \mathrm{diag}(+; x_1 = x_2 + c + 1) & = \emptyset \\
 & \mathrm{diag}(+; x_2 = x_0 + c) & = \{(n, c) \mid n \in \mathbb{N}\}.
\end{array}$$

A notation for straight subspaces is now introduced. A pair of d-tuples $(\boldsymbol{t}, \boldsymbol{c})$ is associated with each straight subspace. The d-tuple $\boldsymbol{t}$ belongs to

$$(\{\mathrm{var}, \mathrm{const}\} \cup \{\mathrm{add}(i) \mid i \in [d-1]\})^d.$$

Intuitively $t_i = \mathrm{const}$ means that the i-th dimension is fixed, $t_i = \mathrm{add}(j)$ means that the distance between the j-th and the i-th dimension is fixed, and $t_i = \mathrm{var}$ means that the i-th dimension is free.

The formal definition is now introduced.

Notation 2.2.24. Let $d \in \mathbb{N}^{>0}$, let $\boldsymbol{t} \in (\{\mathrm{var}, \mathrm{const}\} \cup \{\mathrm{add}(i) \mid i \in [d-1]\})^d$ and let $\boldsymbol{c} \in \mathbb{N}^d$. Let $\dim(t)$ be the number of indices i such that $t_i = \mathrm{var}$. Then let $\mathrm{sub}(R; \boldsymbol{t}, \boldsymbol{c})$ denote the set

$$\left\{(x_i)_{t_i = \mathrm{var}} \in \mathbb{N}^{\dim(t)} \mid (x_0, \ldots, x_{d-1}) \in R, x_i = c_i \text{ if } t_i = \mathrm{const}, x_i = x_j + c_i \text{ if } t_i = \mathrm{add}(j)\right\}.$$

The following lemma is an easy consequence of the definition.

Lemma 2.2.25. *Let $d \in \mathbb{N}^{>0}$, $R \subseteq \mathbb{N}^d$, $d' < d$ and $S \subseteq \mathbb{N}^{d'}$. The two following statements are equivalent:*

1. *the set S is a straight subspace of R,*
2. *there exists $(\boldsymbol{t}, \boldsymbol{c})$ such that $S = \mathrm{sub}(R; (\boldsymbol{t}, \boldsymbol{c}))$ and there are d' integers i such that $t_i = \mathrm{var}$.*

A formula which defines $\mathrm{sub}(R; \boldsymbol{t}, \boldsymbol{c})$ is now introduced.

Notation 2.2.26. Let $\mathcal{L}$ be a fragment of logic and let $\mathcal{V}$ be a vocabulary. Let $\chi(\boldsymbol{x})$ be an $\mathcal{L}[\mathcal{V}]$-formula. Let $\boldsymbol{t}, \boldsymbol{c}$ be as in Notation 2.2.24.

Then let $\mathrm{sub}(\chi, \boldsymbol{t}, \boldsymbol{c})(\boldsymbol{x})$ denote the $\mathcal{L}[\doteq\mathbb{N}, +\mathbb{N}\mathcal{V},]$-formula $\chi(\boldsymbol{x})$ where each terms x_i is replaced by:

- y_h, if $t_i = \text{var}$, and h is the i-th value such that $t_h = \text{var}$,
- c_i if $t_i = \text{const}$ and
- $y_h + c_i$ if $t_i = \text{add}(j)$, and h is the j-th value such that $t_h = \text{var}$.

In particular, $\text{sub}(R, \boldsymbol{t}, \boldsymbol{c})$ is a $\Sigma_0[\dot{=}\mathbb{N}, +\mathbb{N}, R]$-formula.

The following lemma is a straightforward application of the definitions.

Lemma 2.2.27. *Let $d \in \mathbb{N}$, let $\mathcal{V}$ be a vocabulary and let $\mathcal{S}$ be a $\mathcal{V}$-structure. Let $\mathcal{L}$ be a logical fragment.*

Let $\chi(\boldsymbol{x})$ be an $\mathcal{L}[\mathcal{V}]$-formula, then $\text{sub}(\chi(\boldsymbol{x}), \boldsymbol{t}, \boldsymbol{c})(\boldsymbol{x})^{\mathcal{S}}$ *equals* $\text{sub}\Big(\chi(\boldsymbol{x})^{\mathcal{S}}; \boldsymbol{t}, \boldsymbol{c}\Big)$.

Definition 2.2.28 (Fixed order)**.** Recall that $\mathbb{S}_d$ is the set of permutations of $[d-1]$. For every permutation σ of $\mathbb{S}_d$, let $\mathbb{N}^d_\sigma$ be the subset of $\mathbb{N}^d$ where for each $i \in [d-2]$, the relation $x_{\sigma(i)} \leq x_{\sigma(i+1)}$ holds. It is defined by the $\Sigma_0[<]$-formula $\bigwedge_{i=0}^{d-2} x_{\sigma(i)} \leq x_{\sigma(i+1)}$.

It should be noted that $\mathbb{N}^d$ is the union of the $\mathbb{N}^d_\sigma$'s. Therefore, for every vocabulary $\mathcal{V}$ which contains $<$, for every logical fragment $\mathcal{L}$, a set $R \subseteq \mathbb{N}^d$ is $\mathcal{L}[\mathcal{V}]$-definable if and only if for each $\sigma \in \mathbb{S}_d$, the set R is $\mathcal{L}[\mathcal{V}]$-definable in $\mathbb{N}^d_\sigma$.

2.2.4 Logic over $\mathbb{N}$ and over finite models.

In Chapter 5, finite models are considered, using results given in this section. Hence, a notion of *convergence* is needed to state that properties of formulas over $\mathbb{N}$ can also be used over finite models.

Definition 2.2.29 (Set convergence)**.** Let $\mathcal{V}$ be a vocabulary. Let $\mathcal{S}$ be a $\mathcal{V}$-structure over $\mathbb{N}$. Let $\phi(\boldsymbol{x})$ be a formula with arity d such that its interpretation in $\mathcal{S}_{|n}$ (respectively, in $\mathcal{S}$) is a set E_n (respectively, E). Then $\phi(\boldsymbol{x})$ is said to be converging to E in $\mathcal{S}$, if for all $\boldsymbol{c} \in \mathbb{N}^d$, there exists $N \in \mathbb{N}$ such that for all $i \geq N$, $\boldsymbol{c} \in E_i$ if and only if $\boldsymbol{c} \in E$.

For formulas that define functions, this notion is equivalent to point-wise convergence.

Example 2.2.30. Let f_n be defined on $[n-1]$ by $f_n(c) = c + \left\lfloor \frac{2c}{n} \right\rfloor$. Then for all $c \in \mathbb{N}$, $(f_n(c))_{n>c}$ is a sequence of integers converging to c, so $(f_n)_{n\in\mathbb{N}}$ converges to the identity function.

In fact, in our proofs, the values of f_n are only studied on $[c_n - 1]$ for some $c_n \leq n$ and c_n increasing to infinity, i.e. the values of $f_n(b)$ for $b \geq c_n$ are not considered.

The following lemma is straightforward from the definition.

Lemma 2.2.31. *Let $f, g : \mathbb{N} \to \mathbb{N}$ be two converging functions, then $f \circ g$ is a converging function.*

2.3 Automaton, words and monoid

2.3.1 Monoid, semigroup and actions

A set S is a *semigroup* for a binary operation $\cdot$ if this operation is associative, that is, if for all $s, s', s'' \in S$, $s \cdot (s' \cdot s'') = (s \cdot s') \cdot s''$. A *monoid* S is a semigroup such that there exists *an identity element* $1_S \in S$ such that $s \cdot 1_S = s = 1_S \cdot 1_S$ for all $s \in S$. An element $i \in S$ is a *left identity* if $i \cdot s = s$ for all $s \in S$. An element $l \in S$ is said to be a *left inverse* of s if $l \cdot s = 1_S$.

For $n \in \mathbb{N}$, let $(s_0, \cdots, s_{n-1})$ be a sequence of elements of S, then $\Pi_{i=0}^n s_i$ is the product of the s_i's. It can formally be defined recursively on n by $\Pi_{i=0}^0 s_i = s_0$ and for $s > 0$, $\Pi_{i=0}^n s_i = \Pi_{i=0}^{n-1} s_i \cdot s_n$. If S is a monoid, then $\Pi_{i=0}^{-1} s_i$ denotes 1_S.

Subsemigroup A *subsemigroup* T of S is a subset of S which is a semigroup, that is $t \cdot t' \in T$ for all $t,t' \in T$. If S is a monoid, T is a *submonoid* if $1_S \in T$. For S and T two semigroups, a *semigroup morphism* is a function $f : S \to T$ such that $f(s \cdot s') = f(s) \cdot f(s')$ for all $s,s' \in S$. If S and T are monoids, then f is a *monoid morphism* if $f(1_S) = 1_T$.

Ordered semigroup Let $\leqslant$ be an order relation on S. The triplet $(S,\cdot,\leqslant)$ is an *ordered semigroup* if $(S,\cdot)$ is a semigroup and, for all $s,s',t,t' \in S$ such that $s \leqslant t$ and $s' \leqslant t'$, then $s \cdot s' \leqslant t \cdot t'$.

Actions Let S be a semigroup, F be a set, the function $\circ : F \times S \to F$ is a *right action* of S on F if $(f \circ s) \circ s' = f \circ (s \cdot s')$ for all $f \in F, s,s' \in S$. A left action $\circ : S \times F \to F$ is defined similarly.

Note that $\cdot$ is a left and a right action of S on S. A subset G of F is invariant under S for the right action $\circ$ if $g \circ s \in G$ for all $g \in G, s \in S$. If S is a monoid, $f \circ 1_S = f$ for all $f \in F$.

A left action $\circ$ of S on F is extended as a left action of S on $\mathcal{P}(F)$. Let $F' \subseteq F$, then $s \circ F'$ denotes $\{s \circ f \mid f \in F'\}$. The left quotient of $\circ$, which is a right action, is defined by $s^{-1} \circ F' = \{f \in F \mid s \circ f \in F'\}$. The set F' is a *strict quotient* of $F'' \subseteq F$ if there exists $s \in S$, different from 1_S, such that $F' = s^{-1} \circ F''$. A set can be its own strict quotient.

For $s \in S$, an *s-cycle* is a sequence $q_0, \ldots, q_{m-1} \in F$ such that $q_i \circ s = q_{i+1}$ for $i \in [m-2]$ and $q_{m-1} \circ s = q_0$. The s-cycles of length l are sent onto s-cycles of length l' by morphism, with l' which divides l.

Congruences An equivalence relation $\approx$ over S is said to be a congruence relation if $s \approx t$ and $s' \approx t'$ imply $s \cdot s' \approx t \cdot t'$.

For a congruence relation $\approx$, $S/\approx$ denotes the *quotient semigroup*, containing the equivalence classes of S. The function $\cdot$ is extended to elements of $S/\approx$ by $s \cdot t = \{x \cdot y \mid x \in s, y \in t\}$.

In particular, if f is a semigroups morphism, then let $\approx_f$ be the equivalence relation such that $s \approx_f t$ if and only if $f(s) = f(t)$. Then S/f denotes $S/\approx_f$.

2.3.2 Words and Languages

The notion of words and of languages are now introduced. See e.g. [Lee90].

Let A be an *alphabet*, that is a finite set of letters. A *word* w over A, called an A-word, is a finite sequence $w[0] \ldots w[n-1]$ of n letters. Let $|w|$ denote its length. Let ϵ denote the empty word. For all words w and w', their *concatenation* $w \cdot w'$ is the word of length $|w| + |w'|$ such that $(w \cdot w')[i] = w[i]$ for $i < |w|$ and $(w \cdot w')[i + |w|] = w'[i]$ for $i < |w'|$. For a word w of length n and for $n' \leq n$, let $w[< n']$ denote the *prefix* of w of length n', that is, the word of length n' such that $w[i] = w'[i]$ for all $i \in [n'-1]$.

Let A^* denote the set of finite A-words and A^+ denote the set of non-empty A-words. The pair $(A^+,\cdot)$ is a semigroup and the pair $(A^*,\cdot)$ is a monoid.

A language over A is a subset of A^*. For any language L, let $w \cdot L$ denote the concatenation of w and L, that is $\{w \cdot w' \mid w' \in L\}$. Let $w^{-1}L$ denote the left quotient of L, that is the set $\{w' \mid w \cdot w' \in L\}$. The concatenation is a left action of A^* on the set of languages. The left quotient is a right action of A^* on the set of languages, and not a left action, because $(w \cdot w')^{-1}L = w'^{-1}\left(w^{-1}L\right)$.

Regular expressions are defined by the grammar:

$$R ::= a \mid R + R \mid R \cdot R \mid \emptyset \mid \epsilon \mid R^*$$

where $a \in A$ and R is a regular expression. They are used to simplify the example of languages, but are not formally used by proofs nor by theorems.

In this manuscript, the symbol a usually represents a letter and the symbol w represents a word. The symbol a can also be considered as the word w of length 1 such that $w[0] = a$. A word w is either the empty word ϵ or the concatenation $a \cdot w'$ of a letter a and a word w'.

This manuscript deals with A_b^d-words. For example $(2,2)(2,0)(1,0)$ is a A_3^2-word. Formally, a A_b^d-word is a sequence of d-tuples, but it can straightforwardly be seen as a tuple of d words which all have the same length. For a word $\boldsymbol{w} = \boldsymbol{w}[0]\dots\boldsymbol{w}[m-1]$ let w_i denote the $[b-1]$-word, $w_i[0]\dots w_i[m-1]$.

2.3.3 Integers in Base b

The notion of integers written in a given base b is now introduced. This is the notion which links integers to automata.

In this section, the set $\mathbb{I}$ is fixed to be $\mathbb{Z}$ or to $\mathbb{N}$.

Integers are represented by their *least significant digit first* representation. Integers are represented using *b-complement* notation. Let $\overline{w}^{\mathbb{N}}$ and $\overline{w}^{\mathbb{Z}}$ denote the non-negative integers and the integers represented by w respectively.

Formally, let $w = w[0]\dots w[l]$ be a $[b-1]$-word, then let $\overline{w}^{\mathbb{N}}$ denotes $\sum_{i=0}^{l} w[i]b^i$. If $w[l]$ is 0, then $\overline{w}^{\mathbb{Z}}$ denotes $\sum_{i=0}^{l-1} w[i]b^i$, if $w[l] = b-1$ then it denotes $\sum_{i=0}^{l-1} w[i]b^i - b^l$, and otherwise $\overline{w}^{\mathbb{Z}}$ is not defined. The formula can be summarized as $\overline{w}^{\mathbb{Z}} = \sum_{i=0}^{l-1} w[i]b^i - b^l \frac{w[l]}{b-1}$. It can also be defined by induction on $|w|$, by $\overline{0}^{\mathbb{Z}} = 0$, $\overline{b-1}^{\mathbb{Z}} = -1$, $\overline{\epsilon}^{\mathbb{N}} = 0$, and for $a \in [b-1]$, $\overline{aw}^{\mathbb{I}} = a + b\overline{w}^{\mathbb{I}}$. For example, in base $b = 3$, $\overline{112}^{\mathbb{N}} = 22$ and $\overline{112}^{\mathbb{Z}} = -5$. It should be noted that for any $w \in [d-1]$, $\overline{w}^{\mathbb{N}} = \overline{w0}^{\mathbb{Z}}$.

A corollary of the inductive definition is that, $\overline{w \cdot w'}^{\mathbb{I}} = \overline{w}^{\mathbb{N}} + b^{|w|}\overline{w'}^{\mathbb{I}}$. By extension, let $\cdot$ be a left action of A_b^* on $\mathbb{Z}$ such that for every $n \in \mathbb{Z}$, $w \cdot n$ is $\overline{w}^{\mathbb{N}} + b^{|w|}n$. In [Ler06], $w \cdot n$ is denoted $\gamma_{b,d,w}$, this function should note be confused with the relation $\gamma_{t,q}$ introduced in [Pél92]. Then the concatenation and the left quotient are extended to set of integers. For a set $R \subseteq \mathbb{Z}$, $w \cdot R$ is equal to $\{w \cdot n \mid n \in R\}$, that is, to $\overline{w}^{\mathbb{N}} + b^{|w|}R$ and $w^{-1}R$ is equal to $\{n \mid w \cdot n \in R\}$, that is, to the set $\frac{R - \overline{w}^{\mathbb{N}}}{b^{|w|}} \cap \mathbb{Z}$. The concatenation is a left action, and the left quotient is a right action, of A_b^* on $\mathbb{Z}$.

It should be noted that any integer n have an infinite number of representations in base b. Let w and w' be two representations of different length of the same integer. One of this representation is the prefix of the other one. Let assume that $|w| \geq |w'|$, if $n \geq 0$ then $w' \in w0^*$, otherwise $w' \in w(b-1)^*$. The smallest representation is denoted by $\underline{n}_{\mathbb{I}}$.

The function $\overline{w}^{\mathbb{I}}$ is extended to A_b^d-words by setting $\overline{\boldsymbol{w}}^{\mathbb{I}}$ as the d-tuple of integers such that $(\overline{w}^{\mathbb{I}})_i = \overline{w_i}^{\mathbb{I}}$. For instance, $\overline{(1,2)(1,0)(2,0)}^{\mathbb{N}} = (22,2)$ because $\overline{112}^{\mathbb{N}} = 22$ and $\overline{200}^{\mathbb{N}} = 2$. For a language $L \subseteq \left(A_b^d\right)^*$, let $\overline{L}^{\mathbb{I}}$ be $\left\{\overline{\boldsymbol{w}}^{\mathbb{I}} \mid \boldsymbol{w} \in L\right\}$. And for $R \subseteq \mathbb{I}^d$, let $\underline{R}_{\mathbb{I}}$ be the set of words that represent an integer of R, that is $\left\{\underline{\boldsymbol{n}}_{\mathbb{I}} \mid \boldsymbol{n} \in R\right\}$.

The letters of $\{0, b-1\}^d$ are called sign letters. They fix the sign of the d-tuples of integers.

Some example of quotients are now given.

Example 2.3.1. Let R be $\left\{(p,q) \in \mathbb{N}^2 \mid p < q,\ p \equiv q \mod 3\right\}$. Let $b = 2$. Then:

- $(0,0)^{-1}R = (1,1)^{-1}R = (0,1)^{-1}(1,0)^{-1}R = R$,
- $(0,1)^{-1}R = (1,0)^{-1}(1,0)^{-1}R = \left\{(p,q) \in \mathbb{N}^2 \mid p < q,\ p \equiv q+1 \mod 3\right\}$.

- $(1,0)^{-1}R = (0,1)^{-1}(0,1)^{-1}R = \left\{(p,q) \in \mathbb{N}^2 \mid p < q,\ p+1 \equiv q \mod 3\right\}$.
- $(1,0)^{-1}(0,1)^{-1}R = \left\{(p,q) \in \mathbb{N}^2 \mid p \leq q,\ p \equiv q \mod 3\right\}$,

An algorithm which, given ϕ, computes a formula $\boldsymbol{w}^{-1}\phi$ which defines $\boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}}$, is given in Definition 7.2.1.

2.3.4 Deterministic automata

In this section, deterministic automata are introduced. For a complete introduction to automata, see e.g. [Sip96].

A *deterministic automaton* is a 5-tuple $\mathcal{A} = \left(Q, A_b^d, \delta, q_0, F\right)$ where:

- Q is the finite *set of states*,
- $\delta : Q \times A \to Q$ is the *transition function*,
- $q_0 \in Q$ is the *initial state*, and
- $F \subseteq Q$ is the *set of accepting states*.

In this manuscript, the symbol $\mathcal{A}$ always denotes a deterministic automaton. From now on, in this manuscript, all automata are assumed to be deterministic.

The function δ is now extended on $Q \times A^*$ such that δ is a right action of A^* on Q. The function δ is defined by induction by $\delta(q,\varepsilon) = q$ and $\delta(q,aw) = \delta(\delta(q,a),w)$ with $a \in A$ and $w \in A^*$. Let $\underline{\mathcal{A}} = \{w \in A^* \mid \delta(q_0,w) \in F\}$, it is the set of words accepted by the automaton $\mathcal{A}$. A state q' is said to be accessible from a state q if there exists a word w such that $\delta(q,w) = q'$. A state q is said to be *cyclic* if there exists a non-empty word $w_q \in A^+$ such that $\delta(q,w_q) = q$. An automaton whose initial state is cyclic is said to be *initially-cyclic*

Let $\mathcal{A} = (Q,A,\delta,q_0,F)$ and $A' = \left(Q',A,\delta',q_0',F'\right)$ be two automata, a function $\mu : Q \to Q'$ is a *morphism of automaton* from $\mathcal{A}$ to A' if:

- $\mu(q_0) = q_0'$,
- for each $q \in Q$, $q \in F \Longleftrightarrow \mu(q) \in F'$,
- for each $a \in A$, $\mu(\delta(q,a)) = \delta'(\mu(q),a)$ and
- for each $q' \in Q'$, $\mu^{-1}(q') = \{q \in Q \mid \mu(q) = q'\}$ is not empty.

The automaton A' is said to be a quotient of $\mathcal{A}$.

For $q \in Q$, let $\mathcal{A}_q$ denote an automata similar to $\mathcal{A}$, but with q as initial state, and restricted to states accessible from q. Formally, let Q_q be the set of states accessible from q, let $F_q = F \cap Q_q$, and finally let $\mathcal{A}_q$ be $\left(Q_q,A,\delta,q,F_q\right)$. This notion is related to the notion of left quotient of languages. For any word w, $w^{-1}\underline{\mathcal{A}} = \underline{\mathcal{A}_{\delta(q_0,w)}}$.

Two states q and q' are said to be *syntactically equivalent* if $\underline{\mathcal{A}_q} = \underline{\mathcal{A}_{q'}}$. An automaton is said to be minimal if there are no two distinct syntactically equivalent states. For each automaton $\mathcal{A} = (Q,A,\delta,q_0,F)$ there exists (up to isomorphism) a unique minimal automaton $A' = \left(Q',A,\delta',q_0',F'\right)$ such that $\underline{\mathcal{A}} = \underline{A'}$ [Moo56]. There exists a morphism μ from $\mathcal{A}$ to A'.

Definition 2.3.2 (Strongly connected component)**.** Let $\mathcal{A}$ be an automaton over an alphabet A and let q be a state of $\mathcal{A}$. The *strongly connected component* of q is the set of states q' such that q is accessible from q' and q' is accessible from q.

2.3.4.1 Automata reading tuples of integers

The alphabet of the automata of this manuscript are mostly A_b^d. Hence the set of tuples of integers accepted by an automaton must be considered. For this the following notation must be introduced. Let $\overline{\mathcal{A}}^{\mathbb{I}} = \left\{\overline{\boldsymbol{w}}^{\mathbb{I}} \mid \boldsymbol{w} \in \underline{\mathcal{A}}\right\}$ be the subset of tuples of integers of $\mathbb{I}^d$ which have at least one representation accepted by $\mathcal{A}$.

The automaton that accepts the set of Example 2.3.1 is given.

Example 2.3.3 (Example 2.3.1)**.** The minimal automaton $\mathcal{A}$ of figure 2.1 is such that $\overline{\mathcal{A}}^{\mathbb{N}} = R$ where R is the set already considered in Example 2.3.1.

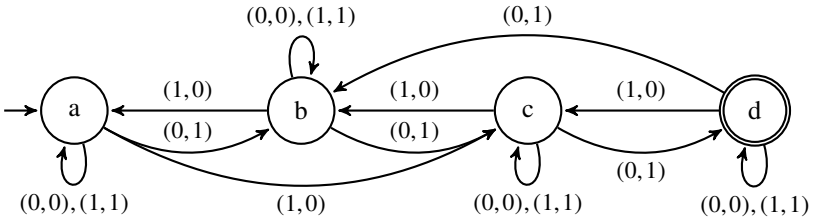


Figure 2.1: $x_0 \equiv x_1 \mod 3 \wedge x_0 \geq x_1$ in $\mathbb{N}^2$

Definition 2.3.4 (b-recognizable)**.** Following [BHMV94], a set accepted by an automaton in base b is said to be b-recognizable. Let $b-\mathrm{REC}$ be the set of b-recognizable sets.

The following theorem characterizes the b-recognizable sets.

Theorem 2.3.5 ([BHMV94])**.** *A set is b-recognizable if and only if it is $\mathsf{FO}[+, V_b]$-definable. The function V_b maps 0 to 0 and each positive integer n to the greatest power of b which divides n.*

An integers (respectively, a tuple of integers) has an infinite number of representations. An automaton may accept a representations and may reject another one. It is easier to work with an automaton which accepts none or all of the representation of a tuple of integers, the next definition introduces those automata and the next lemma shows that it is possible to transform any automaton in an automaton satisfying this constraint in linear time.

Definition 2.3.6. [Automata over $\mathbb{N}$ and over $\mathbb{Z}$] An *automaton over* $\mathbb{N}$ is an automaton $\mathcal{A} = (Q, A, \delta, q_0, F)$ such that for all q, $q \in F \Longleftrightarrow \delta(q, \mathbf{0}) \in F$.

An *automaton over* $\mathbb{Z}$ is an automaton $\mathcal{A} = (Q, A, \delta, q_0, F)$ such that $q_0 \notin F$, and such that $\delta(q, a) \in F \Longleftrightarrow \delta(q, aa) \in F$ for all state q and for all sign letter $a \in \{0, b-1\}^d$.

The next lemma shows how to decide whether an automaton is an automaton over $\mathbb{N}$ or $\mathbb{Z}$.

Lemma 2.3.7. *Let $\mathcal{A}$ be an automaton of alphabet A_b^d with n states. It is decidable in time $O(n)$ whether $\mathcal{A}$ is an automaton over $\mathbb{N}$.*

Proof. The algorithm runs over each state q. If $\delta(q, \mathbf{0}) \in F \Longleftrightarrow q \notin F$, then the algorithm rejects. Otherwise, if the algorithm has not rejected, it accepts. □

Lemma 2.3.8. *Let $\mathcal{A}$ be an automaton of alphabet A_b^d with n states. It is decidable in time $O\left(n2^d\right)$ whether $\mathcal{A}$ is an automaton over $\mathbb{Z}$.*

Proof. The algorithm runs over each state q and all sign letter $\boldsymbol{a} \in A_b^d$. If $\delta(q,\boldsymbol{a}) \in F$ is not equivalent to $\delta(q,\boldsymbol{aa}) \in F$, then the algorithm rejects. Otherwise, if the algorithm has not rejected, it accepts. □

The next lemma shows that each automaton over the alphabet A_b^d is equivalent to an automaton over $\mathbb{N}$, and to an automaton over $\mathbb{Z}$, that accepts the same set of integers.

Lemma 2.3.9. *Let $\mathcal{A} = (Q, A, \delta, q_0, F)$ be an automaton with n states, let $R = \overline{\mathcal{A}}^{\mathbb{I}}$. There exists an automaton A' over the alphabet A_b^d with $c_{\mathbb{I}} \times n$ states, computable in time $O\left(c_{\mathbb{I}} n b^d\right)$ such that A' accepts every representation of tuples of R and nothing else, where $c_{\mathbb{N}} = 2$ and $c_{\mathbb{Z}} = 2^d + 1$.*

Proof. The case $\mathbb{I} = \mathbb{N}$ is first studied. Let $A' = \left(Q \times \{\top, \bot\}, A_b^d, \delta', q_0', Q \times \{\top\}\right)$, with $\delta'\left(q_0', \boldsymbol{w}\right)$ equal to $(\delta(q_0, \boldsymbol{w}), \top)$ if $\overline{\boldsymbol{w}}^{\mathbb{N}} \in R$ and to $(\delta(q_0, \boldsymbol{w}), \bot)$ otherwise. Hence A' respects the hypothesis of the lemma.

Let q_0' be $(q_0, \top)$ if $\mathbf{0} \in R$, and let q_0' be $(q_0, \bot)$ otherwise. For i being $\top$ or $\bot$, let $\delta'((q,i), \mathbf{0}) = (\delta(q, \mathbf{0}), i)$ and for $\boldsymbol{a} \in A_b^d \setminus \{\mathbf{0}\}$, let $\delta'((q,i), \boldsymbol{a})$ be $(\delta(q,\boldsymbol{a}), \top)$ if there exists $l \in \mathbb{N}$ such that $\delta(q, \boldsymbol{a}\mathbf{0}^l) \in F$ and let $\delta'((q,i), \mathbf{0})$ be $(\delta(q,\boldsymbol{a}), \bot)$ otherwise.

To obtain a linear computation time, the set Q' of states q such that there exists $l \in \mathbb{N}$ with $\delta(q, \mathbf{0}^l) \in F$ is computed first. Indeed, q belongs to Q' if $q \in F$ or if $\delta(q, \mathbf{0})$ belongs to Q'. Hence it is computed by fixpoint algorithm in which each state is seen at most twice. Then $\delta'((q,i), \boldsymbol{a})$ is $(\delta(q,\boldsymbol{a}), \top)$ if $\delta(q,\boldsymbol{a}) \in Q'$, and is $(\delta(q,\boldsymbol{a}), \bot)$ otherwise.

The case $\mathbb{I} = \mathbb{Z}$ is similar, except that instead of having $\mathbf{0}$ as special case, each sign letters are special cases. Let $A' = \left(Q \times (\{\bot\} \cup \{0, b-1\}^d), A_b^d, \delta', (q_0, \bot), Q \times \{0, b-1\}^d\right)$. For $\boldsymbol{a} \in A_b^d$, let $\delta'\left(q_0', \boldsymbol{wa}\right)$ be $(\delta(q_0, \boldsymbol{wa}), \boldsymbol{a})$ if ($\boldsymbol{a}$ is a sign letter and $\overline{\boldsymbol{wa}}^{\mathbb{Z}} \in R$), and be $(\delta(q_0, \boldsymbol{wa}), \bot)$ otherwise. Hence A' respects the hypothesis of the lemma.

For a sign letter $\boldsymbol{a}$, let $\delta'((q,\boldsymbol{a}),\boldsymbol{a})$ be $(\delta(q,\boldsymbol{a}),\boldsymbol{a})$ and for $i \neq \boldsymbol{a}$, let $\delta'((q,i),\boldsymbol{a})$ be $(\delta(q,\boldsymbol{a}),\boldsymbol{a})$ if there exists $l \in \mathbb{N}$ such that $\delta(q,\boldsymbol{a}\boldsymbol{a}^l) \in F$ and $(\delta(q,\boldsymbol{a}), \bot)$ otherwise.

The $O\left(2^d n\right)$-time algorithm, where n is the number of states, is similar to the last one. The main differences is that the algorithm computes the 2^d sets $Q'_{\boldsymbol{a}} = \left\{q \in Q \mid \exists l \in \mathbb{N}. \delta(q,\boldsymbol{a}^l) \in F\right\}$ for each sign letter $\boldsymbol{a}$, and then $\delta'((q,i),\boldsymbol{a})$ is $(\delta(q,\boldsymbol{a}),\boldsymbol{a})$ if $\delta(q,\boldsymbol{a}) \in Q'_{\boldsymbol{a}}$, and $(\delta(q,\boldsymbol{a}), \bot)$ otherwise. □

Definition 2.3.10. Let ϕ be a $\mathsf{FO}[\doteq_{\mathbb{Z}}, \doteq, <, +_{\mathbb{Z}}, >0, \mathrm{mod}]$-formula.

Let $\mathcal{A}_{\phi,\mathbb{N}} = \left(Q^\phi, A_b^d, \delta^\phi, q_0^\phi, F^\phi\right)$ be the minimal automaton such that $\overline{\mathcal{A}_{\phi,\mathbb{N}}}^{\mathbb{N}} = \overline{\phi}^{\mathbb{N}}$.

Let $\mathcal{A}_{\phi,\mathbb{Z}} = \left(Q^\phi, A_b^d, \delta^\phi, q_0^\phi, F^\phi\right)$ be the minimal automaton such that $\overline{\mathcal{A}_{\phi,\mathbb{Z}}}^{\mathbb{Z}} = \overline{\phi}^{\mathbb{Z}}$.

It is proven in [BHMV94] that there exists automata $\mathcal{A}_{\mathbb{N}}$ and $\mathcal{A}_{\mathbb{Z}}$ such that $\overline{\mathcal{A}_{\mathbb{Z}}}^{\mathbb{Z}} = \overline{\phi}^{\mathbb{Z}}$ and $\overline{\mathcal{A}_{\mathbb{N}}}^{\mathbb{N}} = \overline{\phi}^{\mathbb{N}}$, which implies that there exists minimal automata.

Part I

Logic

Chapter 3

Characterizations of first-order definable relations

In this part, characterizations of sets definable in a fragment of FO[+] are given. In Section 3.1, some results dealing with sets of integers and unary functions are recalled. A characterization of FO[+]-definable sets is given in Section 3.2. Then, two characterizations of FO[<, mod m]-definable sets are given in Section 3.3. Finally, one characterization of FO[<, mod]-definable is given in Section 3.4.

Contents

3.1 Sets of integers and unary functions **39**
3.2 Characterization of FO[$\mathbb{N}$, +] **41**
3.2.1 Muchnik's theorem 42
3.2.2 The theorem 44
3.3 Characterizations of FO[<, mod m] **49**
3.3.1 Local and recursive characterization of FO[<, mod m]-definable sets 50
3.3.2 Extracting a unary set from a non FO[<, mod m]-definable set 56
3.4 Extracting a unary function from a non FO[<, mod]-definable set **63**
3.5 Conclusion **65**
Notations used in Chapter 3 . . . . . **67**

3.1 Sets of integers and unary functions

In this section, some well-known results are recalled, and some easy corollaries of those results are given.

The first results given in this section deal with FO[+]-, FO[<, mod]- and FO[<, mod m]-definable sets. The first lemma deals with unary sets which are FO[+] or FO[<, mod]-definable. Before giving this lemma, the following definition is needed.

Definition 3.1.1 (Ultimately (m-)periodic)**.** A set $R \subseteq \mathbb{N}$, is *ultimately m-periodic* if there exists an integer $\tau \in \mathbb{N}$ (which is called the threshold) such that for all $n \geq \tau$, $n \in R$ if and only if $n + m \in R$. In particular the ultimately 1-periodic unary sets are the finite or co-finite sets. The set R is *ultimately periodic* if it is ultimately m-periodic for some $m \in \mathbb{N}^{>0}$.

For R an ultimately periodic set of integers, let $\text{thres}_m(R) \in \mathbb{N}$ denote the minimal integer such that for all $n \geq \text{thres}_m(R)$, $n \in R$ is equivalent to $n + m \in R$.

Let $\mathrm{mod}_m(R) \subseteq [m-1]$ denote the subset of $[m-1]$ such that, for all $n \geq \mathrm{thres}_m(R)$, $n \in R$ if and only if $n \equiv p \mod m$ for some $p \in \mathrm{mod}_m(R)$.

Intuitively, $\mathrm{mod}_m(R)$ is the set of congruence classes modulo m which ultimately belong to R, and $[m-1] \setminus \mathrm{mod}_m(R)$ is the set of congruence classes modulo m which are ultimately disjoint from R.

Lemma 3.1.2 ([Pre27])**.** *Let R be a subset of $\mathbb{N}$.*

- *The set R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable if and only if it is ultimately m-periodic.*
- *The set R is $\mathsf{FO}[+]$-definable if and only if it is ultimately periodic.*
- *The set R is $\mathsf{FO}[<, \mathrm{mod}]$-definable if and only if it is ultimately periodic.*

The second lemma deals with unary functions over integers which are $\mathsf{FO}[+]$-definable or $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable.

Lemma 3.1.3 ([FL08])**.** *A unary function $f : \mathbb{N} \to \mathbb{N}$ is $\mathsf{FO}[+]$-definable if and only if there exist $m, \tau \in \mathbb{N}$, $r_0, \cdots, r_{m-1} \in \mathbb{Q}^{\geq 0}$ and $s_0, \cdots, s_{m-1} \in \mathbb{Q}$ such that $f(n) = r_j n + s_j$ for all $n \geq \tau$ such that $n \equiv j \mod m$.*

Furthermore, f is $\mathsf{FO}[<, \mathrm{mod}]$-definable if and only if $r_k \in \{0, 1\}$ for every $k \in [m-1]$.

It should be noted that if f is a unary $\mathsf{FO}[+]$-definable function which is not $\mathsf{FO}[<, \mathrm{mod}]$-definable, then one of the r_i is different from 0 and 1.

In particular, several proofs of this manuscript involve $\mathsf{FO}[+]$-definable functions which are increasing. They are now characterized.

Lemma 3.1.4. *A unary increasing function $f : \mathbb{N} \to \mathbb{N}$ is $\mathsf{FO}[+]$-definable if and only if there exist $m \in \mathbb{N}^{>} 0$, $\tau \in \mathbb{N}$ and $r \in \mathbb{Q}^{\geq 0}$ and $s_0, \cdots, s_{m-1} \in \mathbb{Q}$ such that $f(n) = rn + s_j$ for all $n \geq \tau$ congruent to j modulo m.*

The value of r is called the *slope* of f.

Proof. By Lemma 3.1.3, there exist $m \in \mathbb{N}^{>} 0$, $\tau \in \mathbb{N}$, $r_0, \cdots, r_{m-1} \in \mathbb{Q}^{\geq 0}$, and $s_0, \cdots, s_{m-1} \in \mathbb{Q}$ such that $f(n) = r_j n + s_j$ for all $n \geq \tau$ congruent to j modulo m. It suffices to prove that $r_i = r_j$ for all $i, j \in [m-1]$.

For the sake of contradiction, let us assume that there exist $i, j \in [m-1]$ such that $r_i > r_j$. Without loss of generality, let us assume that $j > i$. Since $j > i$ and f is increasing, $f(n+j) \geq f(n+i)$.

Let $n \in \mathbb{N}$ be such that $n \equiv 0 \mod m$ and $n > \max(\frac{r_j(j-i)+s_j-s_i}{r_i-r_j}, \tau)$. Then:

$$\begin{array}{ll} n & > \frac{r_j j - r_i i + s_j - s_i}{r_i - r_j}, \\ (r_i - r_j)n & > r_j j - r_i i + s_j - s_i, \\ r_i(n+i) + s_i & > r_j(n+j-i) + s_j, \\ f(n+i) & > f(n+j). \end{array}$$

which is a contradiction. □

Some proofs of this manuscript consider increasing FO[+]-definable functions whose slope is strictly greater than 1. It is now proven that such a function allows to define a function whose slope is as great as needed.

Lemma 3.1.5. *Let f be a unary function symbol and let $\mathcal{S}$ be a $\{f, <\}$-structure such that $f^{\mathcal{S}}$ is an increasing FO[+]-definable function with slope $c > 1$. Let $c', e \in \mathbb{N}^{>0}$. There exists a converging $\Sigma_1[\mathbb{N}, <, +\mathbb{N}, f]$-formula $\mu_{f^{\mathcal{S}}}(x; y)$ which defines a function $g : \mathbb{N} \to \mathbb{N}$ in $\mathcal{S}$ such that for all $n \in \mathbb{N}$, $g(n) \geq c'n + e$.*

Proof. The proof consists in two parts: defining a function $h : \mathbb{N} \to \mathbb{N}$ with slope at least c', and then defining the function g.

By an easy induction on i, the i-th iterate f^i of f, is increasing, FO[+]-definable, and its slope is c^i. Let $k = \max(1, \lceil \log_c(c') \rceil)$. It suffices to set h equal to f^k.

Let us assume that h is increasing, FO[+]-definable, with slope at least c. Then there exists τ, m, s_0, $\ldots$, s_{m-1} as in Lemma 3.1.3. Then it suffices to take $g(n)$ to be:

- $c'n + e$ for $n < \tau$, and
- $h(n) + \lceil e - \min(\{s_i \mid i \in [d-1]\} \cup \{e\}) \rceil$ for $n \geq \tau$

It should be noted that $\min(\{s_i \mid i \in [d-1]\} \cup \{e\}) \leq e$, hence

$$e - \min(\{s_i \mid i \in [d-1]\} \cup \{e\}) \geq 0.$$

The formula $\mu_{f^{\mathcal{S}}}(x; y)$ is then:

$$y \doteq f^k(x) + e - \min(\{s_i \mid i \in [d-1]\} \cup \{e\}).$$

By Lemma 2.2.31, the set of converging functions is closed by composition, hence f^k is converging. □

3.2 Characterization of FO[$\mathbb{N}$, +]

A characterization of FO[$\mathbb{N}, +, <$]-definable sets is given in [MV96, Theorem 5.1]. This characterization states that for any $d \in \mathbb{N}$, if a set $R \subseteq \mathbb{N}^d$ is not FO[$\mathbb{N}, +, <$]-definable, then there exists a set of integers which is FO[$\mathbb{N}, +, R$]-definable and which is not FO[$\mathbb{N}, +$]-definable.

The main result of this section, Theorem 3.2.12, is slightly stronger than [MV96, Theorem 5.1]. It states that, for all integers $d > 0$, there exists a FO[$\mathbb{N}, +, <, R$]-formula $\nu_d(x)$ such that, for every set $R \subseteq \mathbb{N}^d$ which is not FO[$\mathbb{N}, +, <$]-definable, the set $\nu_d(x)$ defines a set which is not ultimately periodic. That is, the set $\nu_d(x)$ defines a set which is not FO[$\mathbb{N}, +, <$]-definable.

The "central idea" of Michaux-Villemaire theorem, as stated in [MV96, page 272], is the following. If $R \subseteq \mathbb{N}^d$ is not FO[$\mathbb{N}, +, <$]-definable and all sets of integers which are FO[$\mathbb{N}, +, <, R$]-definable are ultimately periodic, then the negation of Muchnik's characterization of FO[$\mathbb{N}, +, <$]-definable sets ([Muc03, Theorem 1], recalled here as Theorem 3.2.5) does not hold. Which is a contradiction.

A careful analysis of the proof of [MV96, Theorem 5.1] shows that the use of proof by contradiction can be avoided. Removing the proof by contradiction leads to a constructive proof. In general, the constructive proof does not lead to an algorithm because R is potentially infinite. However, in the case where R is definable in a decidable logic which extends FO[$+, <$], such as FO[$V_b, +, <$], then this constructive proof yields an algorithm which generates ν_R.

Finally, a few changes to the constructive proof allow us to create a formula which does not depend on the relation R.

It should also be noted that the changes mentioned above allow to give a shorter proof of the theorem.

3.2.1 Muchnik's theorem

In this section, [Muc03, Theorem 1] is recalled as Theorem 3.2.5. This theorem is used by [MV96, Theorem 5.1] and by our proof of Theorem 3.2.12. It is also an inspiration for the proof of Theorem 3.3.1.

More precisely, Theorem 3.2.5 is a variant of the characterization of $\mathsf{FO}[\mathbb{N},+,<]$-definable relations given in [Muc03, Theorem 1]. This presentation of the theorem is inspired of [MV96, Theorem 5.5]. This characterization of $\mathsf{FO}[\mathbb{N},+,<]$-definable sets consists in two properties, a local property and a recursive property.

The recursive property of [MV96, Theorem 5.5] uses the notion of section, introduced in Definition 2.2.22. The local property of [MV96, Theorem 5.5] uses the notion of cube.

Notation 3.2.1. Let $d \in \mathbb{N}$, $R \subseteq \mathbb{N}^d$, $\boldsymbol{x} \in \mathbb{N}^d$ and $k \in \mathbb{N}$. The *R-cube* at $\boldsymbol{x}$ of size k, denoted by $C_R(\boldsymbol{x},k)$, is defined as:

$$C_R(\boldsymbol{x},k) = \left\{\boldsymbol{y} \in [k]^d \mid \boldsymbol{x}+\boldsymbol{y} \in R\right\}$$

The following lemma considers equality of cubes.

Lemma 3.2.2. *Let $d \in \mathbb{N}$, and R be a d-ary relation symbol. Let $\mathcal{S}$ be a $\{\mathbb{N},+,<,R\}$-structure. There exists a $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\beta_d(\boldsymbol{x},\boldsymbol{y},k)$ which states that the cubes $C_{R^{\mathcal{S}}}(\boldsymbol{x},k)$ and $C_{R^{\mathcal{S}}}(\boldsymbol{y},k)$ are equal.*

Proof. The formula is

$$\beta_d(\boldsymbol{x},\boldsymbol{y},k) = \forall z.[\max(z) \leq k] \Longrightarrow [R(\boldsymbol{x}+z) \Longleftrightarrow R(\boldsymbol{y}+z)],$$

where $\max(\boldsymbol{z}) < k$ denotes $\bigwedge_{i=0}^{d-1} z_i < k$. □

The local property of [MV96, Theorem 5.5] also uses the notion of *shifting* a cube. It is now introduced.

Definition 3.2.3. Let $d \in \mathbb{N}$, $R \subseteq \mathbb{N}^d$, $\boldsymbol{x} \in \mathbb{N}^d$ and $\boldsymbol{r} \in \mathbb{Z}^d$. Then it is said that $C_R(\boldsymbol{x},k)$ can be *shifted by* $\boldsymbol{r}$ if $C_R(\boldsymbol{x},k) = C_R(\boldsymbol{x}+\boldsymbol{r},k)$.

Note that, formally, being shiftable is a property of $\boldsymbol{x},\boldsymbol{r},k$ and $R^{\mathcal{S}}$, and not of the set $C_R(\boldsymbol{x},k)$.

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\sigma_d(\boldsymbol{r},k,\boldsymbol{x})$ is now given, which states that the cube $C_{R^{\mathcal{S}}}(\boldsymbol{x},k)$ can be shifted by $\boldsymbol{r}$.

$$\sigma_d(\boldsymbol{r},k,\boldsymbol{x}) = \beta_d(\boldsymbol{x},\boldsymbol{x}+\boldsymbol{r},k).$$

Note that $\boldsymbol{r} \in \mathbb{Z}^d$. Formally, the variables takes values in $\mathbb{N}$ in our formalism. It is trivial to simulate such variables taking values in $\mathbb{Z}$ by using twice as many variables $\boldsymbol{r}^0,\boldsymbol{r}^1 \in \mathbb{N}^d$ and considering $\boldsymbol{r}$ as $\boldsymbol{r}^0 - \boldsymbol{r}^1$.

The notion of cubes which can be shifted is now extended to set a set of possible shifts.

Definition 3.2.4. Let $d > 0$, $R \subseteq \mathbb{N}^d$, $\boldsymbol{x} \in \mathbb{N}^d$, and $s \in \mathbb{N}$. If there exists $\boldsymbol{r} \in \mathbb{Z}^d \setminus (0,\ldots,0)$ such that $\max(|r|) \leq s$ and such that the cube $C_R(\boldsymbol{x},k)$ can be shifted by $\boldsymbol{r}$, then the cube $C_R(\boldsymbol{x},k)$ is said to be s-shiftable.

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\varsigma_d(s,k,\boldsymbol{x})$ is now given, which states that the cube $C_{R^{\mathcal{S}}}(\boldsymbol{x},k)$ is s-shiftable. Let:

$$\varsigma_d(s,k,\boldsymbol{x}) = \exists \boldsymbol{r} \in \mathbb{Z}^d.\, \max(|\boldsymbol{r}|) \leq s \wedge \bigvee_{i=0}^{d-1} r_i \neq 0 \wedge \sigma_d(\boldsymbol{r},k,\boldsymbol{x}).$$

A variant of Muchnik's theorem is now recalled.

Theorem 3.2.5 ([Muc03, Theorem 1])**.** *Let $d > 0$ and $R \subseteq \mathbb{N}^d$. The following properties are equivalent;*

1. *The set R is $\mathsf{FO}[\mathbb{N},+,<]$-definable.*
2. *a. If $d > 1$, then all sections of R are $\mathsf{FO}[\mathbb{N},+,<]$-definable and*
   b. there exists $s \in \mathbb{N}$ such that, for every $k \in \mathbb{N}$, there exists $t \in \mathbb{N}$ such that, for all $\boldsymbol{c} \in \mathbb{N}^d$ with $\min(\boldsymbol{c}) \geq t$, the cube $C_R(\boldsymbol{c},k)$ is s-shiftable.

Intuitively, the integer s represents the shift, the integer k represents the size of the cube, the integer t represents a threshold and the d-tuple $\boldsymbol{c}$ represents the lowest corner of the cubes considered.

Let us say a word about the difference between [Muc03, Theorem 1], [MV96, Theorem 5.5] and Theorem 3.2.5. The version of [Muc03, Theorem 1] considers a notion of periodicity, while [MV96, Theorem 5.5] and Theorem 3.2.5 consider a notion of shift. Both notions are easily equivalent. The version of [Muc03, Theorem 1] consider relations over $\mathbb{Z}$ while [MV96, Theorem 5.5] and Theorem 3.2.5 only considers relations over $\mathbb{N}$. The condition about $\boldsymbol{c}$ in Condition (b.) of Theorem 3.2.5 is "$\min(\boldsymbol{c}) \geq t$", while it is "$\| \boldsymbol{c} \| \geq t$" in [Muc03, Theorem 1] and it is "$\max(\boldsymbol{c}) \geq t$" in [MV96, Theorem 5.5]. It can be easily shown that no change is required in the proof when replacing one condition by another one, when only relations over $\mathbb{N}$ are considered.

A corollary of this version of the theorem is now given.

Corollary 3.2.6. *Let $d > 0$ and $R \subseteq \mathbb{N}^d$. If R is not $\mathsf{FO}[\mathbb{N},+,<]$-definable, then one of the two following statements hold:*

a. the dimension is at least 2 and a section of R is not $\mathsf{FO}[\mathbb{N},+,<]$-definable or

b. for every $s \in \mathbb{N}$, there exists $k(R,s) \in \mathbb{N}$ such that for every $t \in \mathbb{N}$ there exists $\boldsymbol{c}(R,s,t) \in \mathbb{N}^d$ with $\min(\boldsymbol{c}(R,s,t)) \geq t$ such that the cube $C_R(\boldsymbol{c}(R,s,t),k(R,s))$ is not s-shiftable.

Let $\mathcal{S}$ be a $\{\mathbb{N},+,<,R\}$-structure such that $R^{\mathcal{S}}$ is not $\mathsf{FO}[\mathbb{N},+,<]$-definable. Let $s,t \in \mathbb{N}$. There may exist many values $k(R^{\mathcal{S}},s)$ and $\boldsymbol{c}(R^{\mathcal{S}},s,t)$ for which Condition (b.) holds. Let us assume that $k(R^{\mathcal{S}},s)$ and $\boldsymbol{c}(R^{\mathcal{S}},s,t)$ represent the lexicographically minimal ones.

Two examples of applications of this corollary are now given.

Example 3.2.7.
- Let $R_0 = \left\{(x_0^2, x_1) \mid x_0, x_1 \in \mathbb{N}\right\}$. In this case, Condition (a.) of Corollary 3.2.6 clearly holds, for the section $x_1 = 0$.
- Let $R_1 = \left\{(x_0,x_1) \in \mathbb{N}^2 \mid x_1 \equiv 1 \mod 2, x_0 \leq x_1^2\right\}$, it is pictured in Figure 3.1.

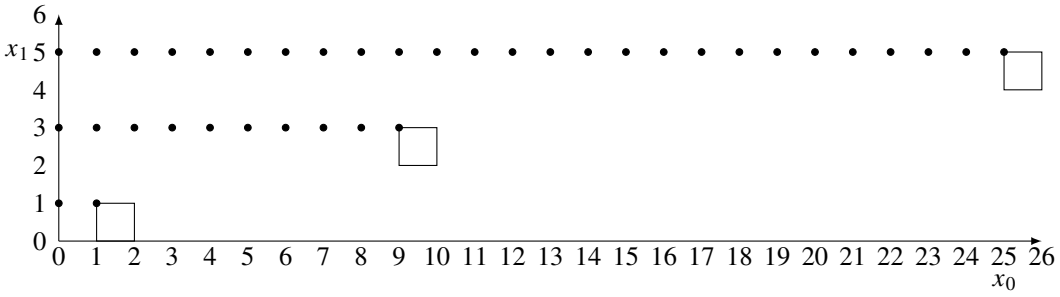


Figure 3.1: $R_1 = \left\{(x_0,x_1) \in \mathbb{N}^2 \mid x_1 \equiv 1 \mod 2, x_0 \leq x_1^2\right\}$ from Example 3.2.7

In this case, Condition (a.) does not hold and Condition (b.) holds. For every $s \in \mathbb{N}^{>0}$, it suffices to consider cubes of size 1, that is $k(R,s) = 1$. Indeed, there is an infinite number of cubes of size 1 which are equal to $\{(0,1)\}$ and which are not s-shiftable. For small values of s, some of those cubes are shown in Figure 3.1.

More precisely, for every $t \in \mathbb{N}$ and for every $s \in \mathbb{N}^{>0}$, $\boldsymbol{c}(R^{\mathcal{S}},s,t)$ equals $((n+1)^2,n)$ where n is the least integer greater or equal to $\max\left(t, \frac{s}{4}\right)$.

The following lemma formally defines the functions k and $\boldsymbol{c}$.

Lemma 3.2.8. *Let $d > 1$ and $R \subseteq \mathbb{N}^d$. If R is not $\mathsf{FO}[\mathbb{N},+,<]$-definable and all sections of R are $\mathsf{FO}[\mathbb{N},+,<]$-definable then the functions $s \mapsto k(R^{\mathcal{S}},s)$ and $(s,t) \mapsto \boldsymbol{c}(R^{\mathcal{S}},s,t)$ are $\mathsf{FO}[\mathbb{N},+,<,R]$-definable.*

Proof. A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\kappa_d(s;K)$ is given which states that $K = k(R^{\mathcal{S}},s)$. The integer $k(R^{\mathcal{S}},s)$ is the minimal integer such that, for all $t \in \mathbb{N}$, there is a d-tuple $\boldsymbol{c} \in \mathbb{N}^d$ with $\min(\boldsymbol{c}) \geq t$ such that the cube $C_{R^{\mathcal{S}}}\left(\boldsymbol{c}, k(R^{\mathcal{S}},s)\right)$ is not s-shiftable.

$$\kappa_d(s;K) = \min_K\{\forall t.\exists \boldsymbol{c}.\, \min(\boldsymbol{c}) \geq t \wedge \neg\varsigma_d(s,K,\boldsymbol{c})\}.$$

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\gamma_d(s,t,k;\boldsymbol{c})$ is now given, which states that $\boldsymbol{c}$ is lexicographically minimal such that:

- $\min(\boldsymbol{c}) \geq t$ and
- the cube $C_{R^{\mathcal{S}}}(\boldsymbol{c},k(s))$ is not s-shiftable.

Let

$$\gamma_d(s,t;\boldsymbol{c}) = \min_{\boldsymbol{c}}\{\min(\boldsymbol{c}) \geq t \wedge \neg\varsigma_d(s,\kappa_d(s),\boldsymbol{c})\}.$$

□

The characterization of Theorem 3.2.5 is expressible in first-order logic with addition.

Theorem 3.2.9 ([Muc03, Theorem 1])**.** *There exists a $\mathsf{FO}[\mathbb{N},+,<,R]$-formula μ_d such that, for every $\{\mathbb{N},R,+,<\}$-structure $\mathcal{S}$, $\mathcal{S} \models \mu_d$ if and only if $R^{\mathcal{S}}$ is $\mathsf{FO}[\mathbb{N},+,<]$-definable.*

3.2.2 The theorem

In this section, the main theorem of this section is proven. It is similar to [MV96, Theorem 5.1], which is now recalled.

Theorem 3.2.10 ([MV96, Theorem 5.1])**.** *Let $d \in \mathbb{N}^{>0}$ and $R \subseteq \mathbb{N}^d$. Then R is $\mathsf{FO}[\mathbb{N},+,<]$-definable if and only if every subset of $\mathbb{N}$ which is $\mathsf{FO}[\mathbb{N},+,<,R]$-definable is ultimately periodic.*

This theorem can be equivalently stated as: Let $d \in \mathbb{N}^{>0}$. For all $R \subseteq \mathbb{N}^d$ which is not $\mathsf{FO}[\mathbb{N},+,<]$-definable, there exists a set of integers $\mathbb{N}$ which is $\mathsf{FO}[\mathbb{N},+,<,R]$-definable and which is not $\mathsf{FO}[\mathbb{N},+,<]$-definable. Resuming Example 3.2.7, two examples of such sets are given.

Example 3.2.11. Let $\mathcal{V} = \{\mathbb{N},+,<,R\}$ where R is a binary relational symbol.

- Let $\mathcal{S}^0$ be the $\mathcal{V}$-structure such that $R^{\mathcal{S}^0} = \left\{(x_0^2,x_1) \mid x_0,x_1 \in \mathbb{N}\right\}$. In this case, it suffices to consider the section $x_1 = 0$. Then the formula $\nu(x) = R(x,0)$, defines the set $\left\{n^2 \in \mathbb{N} \mid n \in \mathbb{N}\right\}$ which is not ultimately periodic.

- Let $\mathcal{S}^1$ be the $\mathcal{V}$-structure such that $R^{\mathcal{S}^1} = \left\{(x_0, x_1) \in \mathbb{N}^2 \mid x_1 \equiv 1 \mod 2, x_0 \leq x_1^2\right\}$. Each section of the form $x_0 = c$ is ultimately periodic with period 2 and each section of the form $x_1 = c$ is finite.

  Let X be the set of pairs (x_0, x_1) such that $C_{R^{\mathcal{S}^1}}((x_0, x_1), 1) = \{(0, 1)\}$. The first of those elements are pictured as the lower-left corner of the square of Figure 3.1. Then it can be shown that $X = \left\{((c+1)^2, c) \mid c \in 2\mathbb{N}\right\}$. Hence the set of norms of elements of X is $\left\{c^2 + 3c + 1 \mid c \in 2\mathbb{N}\right\}$ which is not ultimately periodic. It is defined by

$$\nu(x) = \exists x_0, x_1 . x_0 + x_1 \doteq x \wedge \neg R(x_0, x_1) \quad \wedge R(x_0, x_1 + 1) \\ \wedge \neg R(x_0 + 1, x_1) \wedge \neg R(x_0 + 1, x_1 + 1).$$

Our theorem is now stated.

Theorem 3.2.12. *Let $d \in \mathbb{N}^{>0}$. Let R be a d-ary relation symbol. There exists a $\mathsf{FO}[\mathbb{N}, +, <, R]$-formula $\nu_d(x)$ such that, for every $\{R, +, <\}$-structure $\mathcal{S}$, if $R^{\mathcal{S}}$ is not $\mathsf{FO}[\mathbb{N}, +, <]$-definable then $\nu_d(x)^{\mathcal{S}}$ is not $\mathsf{FO}[\mathbb{N}, +, <]$-definable, i.e. not ultimately periodic.*

Before proving Theorem 3.2.12, the following lemma is needed.

Lemma 3.2.13. *Let $d \in \mathbb{N}$, let $f_0, \ldots, f_{d-1}$ be unary function symbols and let $\mathcal{V} = \{<, f_0, \ldots, f_{d-1}\}$. There exists a $\mathsf{FO}[\mathcal{V}]$-formula $\tau_d(t)$ such that, for every $\mathcal{V}$-structure $\mathcal{S}$ such that:*

$$\lim_{n \to +\infty} f_i^{\mathcal{S}}(n) = +\infty$$

for all $i \in [d-1]$, the set $\tau_d(t)^{\mathcal{S}}$ defines an infinite set $T \subseteq \mathbb{N}$ such that $t_0 < t_1$ implies $\boldsymbol{f}(t_0) < \boldsymbol{f}(t_1)$ for all $t_0, t_1 \in T$.

Proof. The proof is by induction on d. For $d = 0$, $T = \mathbb{N}$ can be chosen. Note that $\mathbb{N}$ is $\mathsf{FO}[\mathcal{V}]$-defined by the formula τ_0 equal to $\exists x . x \doteq x$.

Let us assume that $d > 0$ and that the property holds for $d - 1$. That is, let us assume that there exists a $\mathsf{FO}[\{<, f_0, \ldots, f_{d-2}\}]$-formula $\tau_{d-1}(t)$ such that for every $\mathcal{S}$ which satisfies the hypothesis, $\tau_{d-1}(t)$ defines an infinite set $T' \subseteq \mathbb{N}$ such that, for all $t_0, t_1 \in T'$, $t_0 < t_1$ implies that $f_j(t_0) < f_j(t_1)$ for all $j \in [d-2]$.

Let T be the set of elements $t \in T'$ such that $f_{d-1}(n) > f_{d-1}(t)$ for all $n \in T'$ with $n > t$.

Let us prove that T satisfies the required condition. Let $t_0, t_1 \in T$ be such that $t_0 < t_1$ and let us prove that $\boldsymbol{f}(t_0) < \boldsymbol{f}(t_1)$. By definition of T, having $t_0, t_1 \in T$ implies $t_0, t_1 \in T'$ hence $f_j(t_0) < f_j(t_1)$ for all $j \in [d-2]$. Moreover by definition of T, $f_{d-1}(t_0) < f_{d-1}(t_1)$ since $t_0 < t_1$.

Let us prove that T is infinite. For the sake of contradiction, let us assume that T is finite, hence $\{f_{d-1}(t) \mid t \in T\}$ is also finite. Let $m = \max\{f_{d-1}(t) \mid t \in T\}$, with $\max \emptyset = 0$, since $\{f_{d-1}(t) \mid t \in T\}$ is finite, m is correctly defined. Since

$$\lim_{n \to +\infty} f_{d-1}(n) = +\infty$$

and T' is infinite, the set $\{n \in T' \mid f_{d-1}(n) > m\}$ is non empty, hence

$$\{f_{d-1}(n) \mid n \in T', f_{d-1}(n) > m\}$$

is non empty. Let $c = \min\{f_{d-1}(n) \mid n \in T', f_{d-1}(n) > m\}$, note that $c > m$. Let $C = \{t' \in T' \mid f_{d-1}(t') = c\}$, by definition of c, C is non empty. Since $\lim_{n \to +\infty} f_{d-1}(n) = +\infty$, there exists an integer $N \in \mathbb{N}$ such that for all $n > N$, $f_{d-1}(n) > c$, hence C is finite. Since C is finite and non empty, there exists a greatest integer $t' \in C$. By definition of C and maximality of t', for all $n \in T'$ such that $n > t'$, $f_{d-1}(n) \neq f_{d-1}(t') = c$. By minimality of c, $f_{d-1}(n) \geq c$. Since $f_{d-1}(n) \neq c$ and $f_{d-1}(n) \geq c$ then $f_{d-1}(n) > c = f_{d-1}(t')$. Since $t' \in T'$ and for all $n > t'$, $f_{d-1}(n) > f_{d-1}(t')$, by definition of T, $t' \in T$. Since $t' \in T$, by definition of m, $m \geq f_{d-1}(t')$. Hence $m \geq f_{d-1}(t') = c > m$, which is a contradiction.

Finally, note that T can be $\mathsf{FO}[\mathcal{V}]$-defined as:

$$\tau_d(t) = \tau_{d-1}(t) \wedge \forall n > t.\tau_{d-1}(n) \Longrightarrow f_{d-1}(n) > f_{d-1}(t).$$

□

Theorem 3.2.12 is now proved.

Proof. The formula $\nu_d(x)$ is defined by induction on d. If $d = 1$, by Lemma 3.1.2, $R^{\mathcal{S}}$ is not ultimately periodic, hence it suffices to set $\nu_1(x) = R(x)$. Let us assume that $d > 1$ and that the theorem holds for $d - 1$.

Let F^0 be the set of structures $\mathcal{S}$ such that $R^{\mathcal{S}}$ is not $\mathsf{FO}[\mathbb{N}, +, <]$-definable. The proof is composed of two parts. In the first part, some functions are introduced. Their domain is $F^0 \times \mathbb{N}^{d'}$ for some $d' \in \mathbb{N}$. Their codomains are either the set of integers, the set of tuples of integers, or the set of subsets of $\mathbb{N}$. It is then shown that one of the set of integers is not ultimately periodic. In the second part of the proof, some $\mathsf{FO}[\mathbb{N}, +, <, R]$-formulas are given, which define each of those functions on any structure $\mathcal{S} \in F^0$.

Mathematical definition of a set which is not ultimately periodic

A decreasing sequence F^0, F^1, F^2 of sets of $\{\mathbb{N}, +, <, R\}$-structures is introduced, with $i \in [d - 1]$. For each structure $\mathcal{S} \in F^n$, a set $E(R^{\mathcal{S}}) \subseteq \mathbb{N}$ is defined, such that $E(R^{\mathcal{S}})$ is not ultimately periodic. The problem of defining $E(R^{\mathcal{S}})$ for $\mathcal{S} \in F^n$ with $n < 2$ is reduced to the problem of defining $E(R^{\mathcal{S}})$ for $\mathcal{S} \in F^{n+1}$. Example 3.2.11 is used to illustrate the two first cases. No example of the third case is known.

The set F^0 Let $\mathcal{S} \in F^0$. Since $R^{\mathcal{S}}$ is not $\mathsf{FO}[\mathbb{N}, +, <]$-definable, one of the two properties of Corollary 3.2.6 is satisfied. Let $F^1 \subseteq F^0$ be the set of structures $\mathcal{S}$ such that all sections of $R^{\mathcal{S}}$ are $\mathsf{FO}[\mathbb{N}, +, <]$-definable. For each $\mathcal{S}$ in $F^0 \setminus F^1$, there exists $i \in [d - 1]$ and $j \in \mathbb{N}$ such that $\mathrm{sec}(R^{\mathcal{S}}; x_i = j)$ is not $\mathsf{FO}[\mathbb{N}, +, <]$-definable. In this case, the induction on d can be used on the lexicographically minimal pair (i, j). In Example 3.2.11, $\mathcal{S}^0 \in F^0 \setminus F^1$ and $\mathcal{S}^1 \in F^1$.

The set F^1 Let us now assume that $\mathcal{S} \in F^1$. This case is more complex than the preceding one. By definition of F^1, the set $R^{\mathcal{S}}$ does not satisfy the property (a.) of Corollary 3.2.6. Hence the set $R^{\mathcal{S}}$ does satisfy property (b.).

The set $E(R^{\mathcal{S}})$ is extracted from the sets $T(R^{\mathcal{S}}, s) \subseteq \mathbb{N}$ defined in Lemma 3.2.13. Having

$$\lim_{t \to +\infty} \min(\boldsymbol{c}(R^{\mathcal{S}}, s, t)) = +\infty,$$

implies

$$\lim_{t \to +\infty} (c_i(R^{\mathcal{S}}, s, t)) = +\infty$$

for all $i \in [d - 1]$, hence Lemma 3.2.13 can be applied.

For the structure $\mathcal{S}^1$ of Example 3.2.11, $T(R^{\mathcal{S}^1}, s) = 2\mathbb{N}$, and, as explained in Example 3.2.7, $\boldsymbol{c}(R^{\mathcal{S}^1}, s, t)$ is of the form $((c + 1)^2, c)$.

For $s,t \in \mathbb{N}$, let $C(R^{\mathcal{S}},s,t)$ denote the cube $C_{R^{\mathcal{S}}}\Big(\boldsymbol{c}(R^{\mathcal{S}},s,t),k(R^{\mathcal{S}},s)\Big)$.

For each $s \in \mathbb{N}$, the set $\{C(R^{\mathcal{S}},s,t) \mid t \in T(R^{\mathcal{S}},s)\}$ is a set of subsets of $[k]^d$, hence is finite. It implies that there exists some cube $C(R^{\mathcal{S}},s,t) \in [k(s)-1]^d$ that appears infinitely often in the sequence $(C(R^{\mathcal{S}},s,t))_{t\in T(R^{\mathcal{S}},s)}$. More precisely, there exists an integer $f(R^{\mathcal{S}},s) \in T(R^{\mathcal{S}},s)$ such that $C(R^{\mathcal{S}},s,f(R^{\mathcal{S}},s))$ appears infinitely often in the sequence $(C(R^{\mathcal{S}},s,t))_{t\in T(R^{\mathcal{S}},s)}$. As for k and $\boldsymbol{c}$, the value of $f(R^{\mathcal{S}},s)$ is chosen minimal.

For the structure $\mathcal{S}^1$ of Example 3.2.11, $f(R^{\mathcal{S}^1},s) = 0$ and $C\Big(R^{\mathcal{S}^1},s,f(R^{\mathcal{S}^1},s)\Big) = C_{R^{\mathcal{S}^1}}\Big(\boldsymbol{c}(R^{\mathcal{S}^1},s,0),0\Big) = \{(0,1)\}$.

The set $E(R^{\mathcal{S}})$ is extracted from the sequence of sets $\Big(X(R^{\mathcal{S}},s)\Big)_{s\in\mathbb{N}^{>0}}$ where $X(R^{\mathcal{S}},s) = \{t \in T(R^{\mathcal{S}},s) \mid C(R^{\mathcal{S}},s,t) = C(R^{\mathcal{S}},s,f(R^{\mathcal{S}},s))\}$.

By definition of $f(R^{\mathcal{S}},s)$, for each $s \in \mathbb{N}$, the set $X(R^{\mathcal{S}},s)$ is infinite. Furthermore, for all $t \in \mathbb{N}$, by definition of $\boldsymbol{c}$, $\min(\boldsymbol{c}(R^{\mathcal{S}},s,t)) \geq t$, hence for each $s \in \mathbb{N}$, the set $\{\boldsymbol{c}(R^{\mathcal{S}},s,t) \mid t \in X(R^{\mathcal{S}},s)\}$ is also infinite.

For the structure $\mathcal{S}^1$ of Example 3.2.11, $X(R^{\mathcal{S}^1},s) = T(R^{\mathcal{S}^1},s) = 2\mathbb{N}$.

Let us prove that, for all $s \in \mathbb{N}$, $t,t' \in X(R^{\mathcal{S}},s)$ such that $t < t'$ then $\| \boldsymbol{c}(R^{\mathcal{S}},s,\boldsymbol{t'}) \| - \| \boldsymbol{c}(R^{\mathcal{S}},s,\boldsymbol{t}) \| > s$.

Since $C(R^{\mathcal{S}},s,t)$ is not s-shiftable and

$$C(R^{\mathcal{S}},s,t) = C(R^{\mathcal{S}},s,f(R^{\mathcal{S}},s)) = C(R^{\mathcal{S}},s,t'),$$

either $\boldsymbol{c}(R^{\mathcal{S}},s,t) = \boldsymbol{c}(R^{\mathcal{S}},s,t')$ or

$$\max(|\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)|) > s.$$

Since $t,t' \in X(R^{\mathcal{S}},s)$, by definition of X, $t,t' \in T(R^{\mathcal{S}},s)$. Since $t,t' \in T(R^{\mathcal{S}},s)$ and $t < t'$, by definition of $T(R^{\mathcal{S}},s)$, $\boldsymbol{c}(R^{\mathcal{S}},s,t) < \boldsymbol{c}(R^{\mathcal{S}},s,t')$. Since $\boldsymbol{c}(R^{\mathcal{S}},s,t) < \boldsymbol{c}(R^{\mathcal{S}},s,t')$ and (either $\boldsymbol{c}(R^{\mathcal{S}},s,t) = \boldsymbol{c}(R^{\mathcal{S}},s,t')$ or $\max(|\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)|) > s$) then

$$\max(|\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)|) > s.$$

Since $\boldsymbol{c}(R^{\mathcal{S}},s,t) < \boldsymbol{c}(R^{\mathcal{S}},s,t')$,

$$(\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)) = |\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)|,$$

hence

$$\max(\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)) = \max(|\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)|) > s.$$

Since $\max(\boldsymbol{c}(R^{\mathcal{S}},s,t') - \boldsymbol{c}(R^{\mathcal{S}},s,t)) > s$, there exists $i \in [d-1]$ such that $c_i(R^{\mathcal{S}},s,t') - c_i(R^{\mathcal{S}},s,t) > s$. From $c_j(R^{\mathcal{S}},s,t') - c_j(R^{\mathcal{S}},s,t) > 0$ for all $j \in [d-1]$, and $c_i(R^{\mathcal{S}},s,t') - c_i(R^{\mathcal{S}},s,t) > s$ it follows that $\| \boldsymbol{c}(R^{\mathcal{S}},s,t') \| - \| \boldsymbol{c}(R^{\mathcal{S}},s,t) \| > s$

For all $s \in \mathbb{N}$, let $N(R^{\mathcal{S}},s) = \{\| c(R^{\mathcal{S}},s,t) \| \mid t \in X(R^{\mathcal{S}},s)\}$. By construction of $X(R^{\mathcal{S}},s)$, the set $N(R^{\mathcal{S}},s)$ is infinite and, as proved above, the difference between two distinct integers of $N(R^{\mathcal{S}},s)$ is strictly greater than s. Hence $N(R^{\mathcal{S}},s)$ is not ultimately p-periodic for any $p \leq s$.

Similarly to the case F^1, two cases must be considered, depending on whether there exists s such that $N(R^{\mathcal{S}},s)$ is not ultimately periodic, or not. If there exists such a $s \in \mathbb{N}$, then let $E(R^{\mathcal{S}})$ be $N(R^{\mathcal{S}},s)$, with s minimal. Let F^2 be the set of structures $\mathcal{S} \in F^1$ such that for all $s \in \mathbb{N}$, the set $N(R^{\mathcal{S}},s)$ is ultimately periodic. The problem is now reduced to the study of structures of F^2.

For the structure $\mathcal{S}^1$ of Example 3.2.11,

$$N(R^{\mathcal{S}^1},s) = \left\{c + (c+1)^2 \mid c \equiv 0 \mod 2,\ c > \frac{s}{4}\right\}.$$

The set F^2 Let us assume that $\mathcal{S} \in F^2$. For all $s \in \mathbb{N}$, since $N(R^{\mathcal{S}}, s)$ is ultimately periodic, let $p(R^{\mathcal{S}}, s)$ be its minimal period. The set $E(R^{\mathcal{S}})$ is defined using $(p(R^{\mathcal{S}}, s))_{s\in\mathbb{N}}$.

It should be noted that $(p(R^{\mathcal{S}}, s))_{s\in\mathbb{N}}$ is the first sequence of this proof such that s is a parameter of the sequence and is not assumed to be fixed.

As noted above, $N(R^{\mathcal{S}}, s)$ is infinite and the distance between two integers of $N(R^{\mathcal{S}}, s)$ is strictly greater than s, hence $p(R^{\mathcal{S}}, s) > s$.

Let $e(R^{\mathcal{S}}, s) = \mathrm{lcm}\{p(R^{\mathcal{S}}, t) \mid t \leq s\}$. Then, $E(R^{\mathcal{S}})$ is chosen as $\left\{e(R^{\mathcal{S}}, n) \mid n \in \mathbb{N}\right\}$. It remains to prove that this set is not ultimately periodic.

Clearly $e(R^{\mathcal{S}}, s)$ divides $e(R^{\mathcal{S}}, s+1)$, hence either $e(R^{\mathcal{S}}, s+1) = e(R^{\mathcal{S}}, s)$ or $e(R^{\mathcal{S}}, s+1) \geq 2e(R^{\mathcal{S}}, s)$, and since $\left(p(R^{\mathcal{S}}, s)\right)_{s\in\mathbb{N}}$ is unbounded, then $\left(e(R^{\mathcal{S}}, n)\right)_{n\in\mathbb{N}}$ grows infinitely often and the difference between two successive integers of $E(R^{\mathcal{S}})$ is not bounded. Hence $E(R^{\mathcal{S}})$ is not ultimately periodic.

It should be noted that, for an arbitrary finite set F, the value of $\mathrm{lcm}(F)$ does not seem to be $\mathsf{FO}[+, F]$-definable. In this case, the function $e(R^{\mathcal{S}}, s)$ is equivalently defined by stating that $e(R^{\mathcal{S}}, s)$ is the least integer such that for all $t < s$, the set $N(R^{\mathcal{S}}, t)$ is $e(R^{\mathcal{S}}, s)$-periodic.

The $\mathsf{FO}[\mathbb{N}, +, <, R]$-formula which defines E in $\mathcal{S}$

In this part of the proof, $\mathsf{FO}[\mathbb{N}, +, <, R]$-formulas are given for all functions given in the first part of the proof.

Three formulas, $\nu_{d,0}(x)$, $\nu_{d,1}(x)$ and $\nu_{d,2}(x)$ are given such that, for each $\mathcal{S} \in F^n$ with n being 0, 1 or 2 the set $\nu_{d,n}(x)^{\mathcal{S}}$ is not ultimately periodic. For n being 0 or 1, the formulas $\nu_{d,n}(x)$ use:

- the formula $\nu_{d,n+1}(x)$,
- a formula which characterizes the structures of $F^n \setminus F^{n+1}$ and
- a formula which defines a set which is not ultimately periodic for any structure $\mathcal{S} \in F^n \setminus F^{n+1}$.

The formula $\nu_{d,0}$ Let us define the $\mathsf{FO}[\mathbb{N}, +, <, R]$-formula $\nu_{d,0} = \nu_d(x)$. Let us assume that there exists a $\mathsf{FO}[\mathbb{N}, +, <, R]$-formula $\nu_{d,1}(x)$ such that, for all $\mathcal{S} \in F^1$, the set $\nu_{d,1}(x)^{\mathcal{S}}$ is not ultimately periodic.

Then, $\nu_{d,0}$ uses:

- the formula $\nu_{d,1}$ for any structure belonging to F^1, and
- the induction on d for any structure which does not belong to F^1. More precisely, the induction is used on the lexicographically least pair (i, s) such that $\mathrm{sec}(R^{\mathcal{S}}; x_i = s)$ is not $\mathsf{FO}[\mathbb{N}, +, <]$-definable.

To formally define this set, let $\mu_{d,i}(s)$ be the $\mathsf{FO}[\mathbb{N}, +, <, R]$-formula which states that $\mathrm{sec}(R^{\mathcal{S}}; x_i = s)$ is $\mathsf{FO}[\mathbb{N}, +, <]$-definable. It is defined by the formula μ_{d-1} of Theorem 3.2.9 where $R(n_0, \ldots, n_{d-2})$ is replaced by $R(n_0, \ldots, n_{i-1}, s, n_i, \ldots, n_{d-2})$. Recall that the notation $\langle \cdot \mid \cdot \mid \cdot \rangle$ is introduced in Notation 2.2.11.

$$\nu_{d,0}(x) = \langle \bigvee_{i=0}^{d-1} \exists s. \min_{i\in[d-1],s} \{\neg\mu_{d,i}(s)\} \mid \nu'_{d-1,i}(x, s) \mid \nu_{d,1}(x) \rangle,$$

where $\nu'_{d-1,i}(x, s)$ is the formula $\nu'_{d-1}(x)$ where $R(n_0, \ldots, n_{d-2})$ is replaced by $R(n_0, \ldots, n_{i-1}, s, n_i, \ldots, n_{d-2})$ for all terms $\boldsymbol{n}$.

The formula $\nu_{d,1}$ Let us define the $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\nu_{d,1}(x)$.

By Lemma 3.2.8, there exists two $\mathsf{FO}[\mathbb{N},+,<,R]$-formulas $\kappa_d(s;K)$ and $\gamma_d(s,t;c)$ which define $k(R^{\mathcal{S}},s)$ and $\boldsymbol{c}(R^{\mathcal{S}},s,t)$, respectively. By Lemma 3.2.13, there exists a $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\tau_d(s,t)$ which states that $t \in T(R^{\mathcal{S}},s)$.

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\phi(s;F)$ which states that $F = f(R^{\mathcal{S}},s)$ is now given. Let:

$$\phi(s;F) = \min_{F}\{\tau_d(s,F) \wedge \forall t \in \mathbb{N}.\exists t' > t.\tau_d(s,t') \wedge \beta_d(\boldsymbol{x}(s,F),\boldsymbol{x}(s,t'),\kappa_d(s))\}.$$

where $\beta_d(\boldsymbol{x},\boldsymbol{y},k)$ is the $\mathsf{FO}[\mathbb{N},+,<,R]$-formula given in Lemma 3.2.2 which states that the cube $C_{R^{\mathcal{S}}}(\boldsymbol{x},k)$ is equal to the cube $C_{R^{\mathcal{S}}}(\boldsymbol{y},k)$.

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\xi_d(s,t)$ is now given, which states that $t \in X(R^{\mathcal{S}},s)$. Let:

$$\xi_d(s,t) = \tau_d(s,t) \wedge \beta_d(\psi_d(s,t),\psi_d(s,\phi(s)),\kappa_d(s)).$$

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\zeta_d(s,x)$ is given, which states that $x \in N(R^{\mathcal{S}},s)$. Let:

$$\zeta_d(s,x) = \exists t.\xi_d(s,t) \wedge x \doteq \| \boldsymbol{\gamma}(s,t) \| .$$

Let us assume that there exists a $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\nu_{d,2}(x)$ such that $\nu_{d,2}(x)^{\mathcal{S}}$ is not ultimately periodic for all $\mathcal{S} \in F^2$.

Similarly to $\nu_{d,0}(x)$, the formula $\nu_{d,1}(x)$ is a disjunction of two cases. If there is $s \in \mathbb{N}$ such that some $N(R^{\mathcal{S}},s)$ is not ultimately periodic then $\nu_{d,1}(x)$ defines $N(R^{\mathcal{S}},s)$ with s minimal. Otherwise $\nu_{d,1}(x)$ uses the formula $\nu_{d,2}(x)$. Let:

$$\nu_{d,2}(x) = \langle \min_{s}\left\{\neg\mu_1'(s)\right\} \mid \zeta_d(s,x) \mid \nu_d^2(x)\rangle,$$

where $\mu_1'(s)$ is the formula μ_1, of Theorem 3.2.9, where $R(x)$ is replaced by $\zeta_d(s,x)$.

The formula $\nu_{d,2}$ Let us define the $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\nu_{d,2}(x)$. As in the previous cases, before giving $\nu_{d,2}(x)$, two $\mathsf{FO}[\mathbb{N},+,<,R]$-formulas are given, to define $p(R^{\mathcal{S}},s)$ and $e(R^{\mathcal{S}})$.

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\rho_d(s,p)$ is given, which states that p is a period of $N(R^{\mathcal{S}},s)$. Let:

$$\rho_d(s,p) = \exists N.(\forall n > N)[\zeta_d(s,n) \Longleftrightarrow \zeta_d(s,n+p)].$$

A $\mathsf{FO}[\mathbb{N},+,<,R]$-formula $\epsilon_d(s;p)$ is given, which states that $p = e(R^{\mathcal{S}},s)$. Let:

$$\epsilon_d(s;p) = \min_{p}\{\forall t \leq s.\rho_d(t,p)\}.$$

Finally let $\nu_{d,2}(x)$ be:

$$\exists s.\epsilon_d(s;x).$$

□

3.3 Characterizations of $\mathsf{FO}[<,\mathrm{mod}\, m]$

In this Section, two characterizations of $\mathsf{FO}[<,\mathrm{mod}\, m]$ are given.

In Section 3.3.1, a first characterization of $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable sets is given, in term of local properties and recursive properties. In Section 3.3.2, it is proven that, from a set of tuples of integers which is not $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable, a set of integers which is not $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable can be defined.

3.3.1 Local and recursive characterization of $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable sets

In this section, a characterization of $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable sets is given. Then some easy consequences of this characterization are given. This characterization is similar to Muchnik's characterization of $\mathsf{FO}[\mathbb{N}, +]$, given as Theorem 3.2.5.

Theorem 3.3.1. *Let $d \in \mathbb{N}^{>0}$, $R \subseteq \mathbb{N}^d$, and $m \in \mathbb{N}$. The following three statements are equivalent:*

1. *The set R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable.*
2. *a. There exists $t \in \mathbb{N}$ such that R is m-periodic in $(\mathbb{N}^{\geq t})^d$ and*
   b. if $d > 1$, then all sections and diagonals of R are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable.
3. *For every straight subspace S of dimension $d' \geq 1$ of R, there exists $t \in \mathbb{N}$ such that S is $(\overline{m, \ldots, m}^{d'})$-periodic in $(\mathbb{N}^{\geq t})^{d'}$.*

The notation $\mathrm{thres}_m(R)$ is introduced in Definition 3.1.1 for $R \subseteq \mathbb{N}$. It is now generalized to any dimension $d \in \mathbb{N}^{>0}$.

Notation 3.3.2. Let $d \in \mathbb{N}^{>0}$, $R \subseteq \mathbb{N}^d$, and $m \in \mathbb{N}$. If R satisfies Condition (b.) of Theorem 3.3.1, let $\mathrm{thres}_m(R)$ denote the least integer t which satisfies this condition.

An example of application of Theorem 3.3.1 is given first.

Example 3.3.3. As seen in Example 2.2.23, all strict straight subspaces of $+$ are $\mathsf{FO}[<, \mathrm{mod}]$-definable sets. So $+$ satisfies the criterion (b.) of Theorem 3.3.1. For each $l \in \mathbb{N}$, one has $(l, l, 2l) \in +$. For every $m \in \mathbb{N}$, the 3-tuple $(l + m, l + m, 2l + m)$ does not belong to the relation $+$, so $+$ does not satisfy the criterion (a.).

Let us consider another example. Let $R = \left\{(0, n^2) \mid n \in \mathbb{N}\right\}$. The set R is 1-periodic in $(\mathbb{N}^{\geq 1})^2$, so it satisfies the criterion (a.). But clearly $R^{x_0=0} = \left\{n^2 \mid n \in \mathbb{N}\right\}$ is not $\mathsf{FO}[<, \mathrm{mod}]$-definable, so it does not satisfy the criterion (b.).

Theorem 3.3.1 is now proven.

Proof of Theorem 3.3.1. Let us show by induction on $d \in \mathbb{N}$ that properties (1), (2) and (3) are equivalent for every $R \subseteq \mathbb{N}^d$.

Let us first assume that $d = 1$. Lemma 3.1.2 proves the equivalence of (1) and of (2). Since R is the only straight subspace of R of dimension at least 1, (3) and (a.) are equivalent. Moreover, (b.) holds since $d = 1$. Hence (2) and (3) are equivalent.

Let us now assume that $d > 1$ and that the property holds for $d - 1$.

Proof of (1)$\Longrightarrow$(3) Assume that R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable and let us prove that for every integer $d' \leq d$, and every straight subspace S of R of dimension d', there exists $\mathrm{thres}_m(S)$ such that S is $(\overline{m, \ldots, m}^{d'})$-periodic in $(\mathbb{N}^{\geq \mathrm{thres}_m(S)})^{d'}$.

By Proposition 2.2.21, there exists a quantifier-free $\Sigma_0[\doteq_{\mathbb{Z}}, <, +_{\mathbb{N}}, -_{\mathbb{Z}}, \mathrm{mod}\, M]$-formula $\chi(\boldsymbol{x})$ which defines R. Let S be a straight subspace of R, then by Lemma 2.2.27, there exists a $\Sigma_0[\doteq_{\mathbb{Z}}, <, +_{\mathbb{N}}, -_{\mathbb{Z}}, \mathrm{mod}\, M]$-formula $\chi_S(\boldsymbol{x})$ which defines S. Let

$$\mathrm{thres}_m(S) = \max\{c \in \mathbb{N} \mid x_i \sim c \text{ appears in } \chi_S(\boldsymbol{x}), \sim \text{ being } <, = \text{ or } >\} + 1.$$

Let us prove by induction on the subformulas $\xi(\boldsymbol{x})$ of $\chi_S(\boldsymbol{x})$ that the set $\xi(\boldsymbol{x})^{\mathcal{N}}$ is $(\overline{m, \ldots, m}^{d})$-periodic in $(\mathbb{N}^{\geq \mathrm{thres}_m(S)})^{d'}$. Let $\boldsymbol{n} \in \mathbb{N}^{d'}$ with $\min(\boldsymbol{n}) > \mathrm{thres}_m(S)$, it must be proven that $\xi(\boldsymbol{n})$ is equivalent to $\xi(\boldsymbol{n} + (\overline{m, \ldots, m}^{d}))$. The induction case is trivial. Let us consider the base case:

- if $\xi(\boldsymbol{x})$ is of the form $x_i \equiv a \mod m$, then $n_i \equiv a \mod m$ is equivalent to $n_i + m \equiv a \mod m$,
- if $\xi(\boldsymbol{x})$ is of the form $x_i - x_j \sim c$ for $\sim$ being $<$ or $\doteq$, then $n_i - n_j \sim c$ is equivalent to $(n_i + m) - (n_j + m) \sim c$,
- if $\xi(\boldsymbol{x})$ is of the form $x_i < c$ or $x_i \doteq c$, then by hypothesis $c < \mathrm{thres}_m(S)$, hence neither $\xi(\boldsymbol{n})$ nor $\xi(\boldsymbol{n} + (\overline{m, \ldots, m}^d))$ hold.
- if $\xi(\boldsymbol{x})$ is of the form $x_i > c$ then by hypothesis $c < \mathrm{thres}_m(S)$, hence $\xi(\boldsymbol{n})$ and $\xi(\boldsymbol{n} + (\overline{m, \ldots, m}^d))$ hold.

Proof of (3)$\Longrightarrow$(2) The set R is a straight subspace of R hence by hypothesis, there exists $\mathrm{thres}_m(R) \in \mathbb{N}$ such that R is $(\overline{m, \ldots, m}^d)$-periodic in $(\mathbb{N}^{\geq d})^{\mathrm{thres}_m(R)}$.

Proof of (2)$\Longrightarrow$(1) Let R be such that all sections $\mathrm{sec}(R; x_i = c)$ and diagonals $\mathrm{diag}(R; x_i = x_j + c)$ are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Then, for all distinct elements $i, j \in [d-1]$ and for all $c \in \mathbb{N}$, let $\psi_{\mathrm{sec}(R; x_i = j)}(x_0, \cdots, x_{d-2})$ and $\psi_{\mathrm{diag}(R; x_i = x_j + c)}(x_0, \cdots, x_{d-2})$ be $\mathsf{FO}[\doteq\mathbb{Z}, <, +\mathbb{N}, -\mathbb{Z}, \mathrm{mod}\, M]$-formulas which define $\mathrm{sec}(R; x_i = c)$, and $\mathrm{diag}(R; x_i = x_j + c)$, respectively. Those formulas exist by hypothesis.

Figure 3.2 serves as example for the proof. It represents the set R defined by the formula $\phi(x_0, x_1)$ equal to:

$$\{(x_0 + 2 \geq x_1 \wedge x_0 + 4 \neq x_1) \vee x_1 \doteq 1\} \wedge x_0 \equiv 1 \mod 2. \tag{3.1}$$

In this example, $m = 2$ and $\mathrm{thres}_m(R) = 2$.

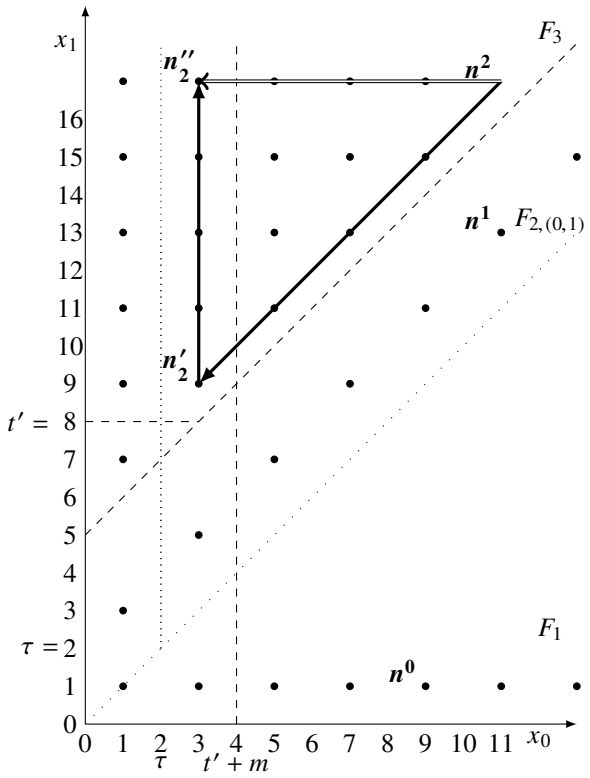


Figure 3.2: $\{(x_0 + 2 \geq x_1 \wedge x_0 + 4 \neq x_1) \vee x_1 \doteq 1\} \wedge x_0 \equiv 1 \mod 2$

A $\subseteq$-decreasing sequence $F_0, F_1, F_{2,\sigma}, F_3, F_4$ of subsets of $\mathbb{N}^d$, with $F_0 = \mathbb{N}^d$, is introduced. The proof consists in reducing the problem of defining R in F_i to the problem of defining R in F_{i+1}. A formula $\phi_i(\boldsymbol{x})$ is then given, such that $\phi_i(\boldsymbol{x})^{\mathcal{N}}$ defines R in F_i. The formula ϕ_i uses a formula which defines R in F_{i+1}, a formula which defines R in $F_i \setminus F_{i+1}$ and the formula ϕ_{i+1}.

It is proven that $\phi_i(\boldsymbol{n})$ defines R in F_i.

The set F_0 Let $\tau = \text{thres}_m(R)$ and let $F_1 = (\mathbb{N}^{\geq\tau})^d$. The set F_1 is considered, because, by definition of τ, the set R is m-periodic in F_1.

The formula ϕ_0 is constructed using a formula which defines R in $F_0 \setminus F_1$, a formula which defines R in F_1 and a formula which defines F_1. It should be noted that $F_0 \setminus F_1$ is included in a finite union of sections of R, and hypothesis (a.) can be used on each of those sections. Let us assume that $\phi_1(\boldsymbol{x})$ defines R in F_1. Then let ϕ_0 be:

$$\phi_0(\boldsymbol{x}) = \langle \bigvee_{i=0}^{d-1} \bigvee_{j=0}^{l-1} x_i \doteq j \mid \psi_{\text{sec}(R;x_i=j)}(x_0, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{d-2}) \mid \phi_1(\boldsymbol{x}) \rangle.$$

In the example of Figure 3.2, let $n^0 = (9,1)$, $n^1 = (11,11)$ and $n^2 = (11,17)$, then $n^0 \notin F_1$ and $n^1, n^2 \in F_1$. The vertical and horizontal dotted line represent the boundary of F_1.

Let us prove that $\boldsymbol{n} \in R$ if and only if $\mathcal{N}' \models \phi_0(\boldsymbol{x})$ holds, where $\mathcal{N}' = \mathcal{N}[\boldsymbol{x}/\boldsymbol{n}]$. Let us first assume that $\boldsymbol{n} \in R$ and let us prove that $\mathcal{N}' \models \phi_0(\boldsymbol{x})$. Two cases must be considered, depending on whether $\min(\boldsymbol{n}) < \tau$ or not.

- Let us assume that $\min(\boldsymbol{n}) < \tau$, then there exist $i \in [d-1]$ and $j \in [\tau - 1]$ such that $n_i = j$. Hence $\mathcal{N}' \models x_i \doteq j$. Let $\boldsymbol{n'}$ be $\boldsymbol{n}$ without its i-th component. By definition of section, $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n'} \in \text{sec}(R; x_i = j)$, and by definition of $\psi_{\text{sec}(R;x_i=j)}(\boldsymbol{x})$, it implies that $\mathcal{N}' \models \psi_{\text{sec}(R;x_i=j)}(\boldsymbol{n'})$. Hence $\mathcal{N}' \models \phi_0(\boldsymbol{x})$.
- Let us now assume that $\min(\boldsymbol{n}) \geq \tau$, then, $\mathcal{N}' \models \neg\left(\bigvee_{i=0}^{d-1} \bigvee_{j=0}^{l-1} x_i \doteq j\right)$ and by hypothesis about $\phi_1(\boldsymbol{x})$, $\boldsymbol{n} \in R$ is equivalent to $\mathcal{N}' \models \phi_1(\boldsymbol{x})$. Hence $\mathcal{N}' \models \phi_0(\boldsymbol{x})$.

Finally, in both cases, $\mathcal{N}' \models \phi_0(\boldsymbol{x})$.

Let us now assume that $\mathcal{N}' \models \phi_0(\boldsymbol{x})$ and let us prove that $\boldsymbol{n} \in R$. Again, two cases must be considered. Since ϕ_0 is a disjunction, one of the two subformulas holds over $\mathcal{N}'$. Either $\mathcal{N}' \models \bigvee_{i=0}^{d-1} \bigvee_{j=0}^{l-1} x_i \doteq j \wedge \psi_{\text{sec}(R;x_i=j)}(x_0, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{d-2})$ or $\mathcal{N}' \models \neg\left(\bigvee_{i=0}^{d-1} \bigvee_{j=0}^{l-1} x_i \doteq j\right) \wedge \phi_1(\boldsymbol{x})$. In the first case, there exists $i \in [d-1]$ such that $n_i < \tau$ and for $\boldsymbol{n'}$ defined as above, $\boldsymbol{n'}$ belongs to $\text{sec}(R; x_i = n_i)$, hence $\boldsymbol{n} \in R$. Otherwise, by hypothesis, $\boldsymbol{n} \in R$.

The set F_1 Let us now consider the set F_1.

Recall that $\mathbb{S}_d$ is the set of permutation of $[d-1]$. For all $\sigma \in \mathbb{S}_d$, let $F_{2,\sigma} = F_1 \cap \mathbb{N}^d_\sigma$. The sets $F_{2,\sigma}$ are considered because, for each $\boldsymbol{n} \in F_{2,\sigma}$, $n_{\sigma(0)}$ is the smallest of the n_i's. The set $R \cap F_1$ is equal to the union of the sets $R \cap F_{2,\sigma}$ for $\sigma \in \mathbb{S}_d$. Using this idea, the formula ϕ_1 is constructed as the disjunction of the $d!$ formulas which state that $\boldsymbol{x} \in \mathbb{N}^d_\sigma$ and that $\phi_{2,\sigma}(\boldsymbol{x})$ holds (for each $\sigma \in \mathbb{S}_d$).

Let us assume that $\phi_{2,\sigma}(\boldsymbol{x})$ defines the set $R \cap \mathbb{N}^d_\sigma$ in $F_{2,\sigma}$, then let $\phi_1(\boldsymbol{x})$ be:

$$\bigvee_{\sigma \in \mathbb{S}_d} \left(\bigwedge_{i=0}^{d-2} x_{\sigma(i)} \leq x_{\sigma(i+1)} \right) \wedge \phi_{2,\sigma}(\boldsymbol{x}).$$

In the example of Figure 3.2, n^1 and n^2 belongs to $F_{2,(1,0)}$ while n^0 belongs to $F_{2,(0,1)}$. The dashed diagonal line represents the boundary between those two sets.

Let us prove that $\boldsymbol{n} \in R$ if and only if $\mathcal{N}' \models \phi_0(\boldsymbol{x})$ holds. Let us assume that $\boldsymbol{n} \in R$ and let us prove that $\mathcal{N}' \models \phi_0(\boldsymbol{x})$. Let σ be a permutation such that $\boldsymbol{n} \in F_{2,\sigma}$, then by hypothesis about $\phi_{2,\sigma}(\boldsymbol{x})$, $\mathcal{N}' \models \phi_{2,\sigma}(\boldsymbol{x})$, and furthermore $\mathcal{N}' \models \bigwedge_{i=0}^{d-2} x_{\sigma(i)} \leq x_{\sigma(i+1)}$, hence $\mathcal{N}' \models \phi_0$.

Let us assume that $\mathcal{N}' \models \phi_0(\boldsymbol{x})$ and let us prove that $\boldsymbol{n} \in F_{2,\sigma}$. Let $\sigma \in \mathbb{S}_d$ be such that $\mathcal{N}' \models (\bigwedge_{i=0}^{d-2} x_{\sigma(i)} \leq x_{\sigma(i+1)} \wedge \phi_{2,\sigma}(\boldsymbol{x}))$. Then $\boldsymbol{n} \in \mathbb{N}^d_\sigma$, and by hypothesis about $\phi_{2,\sigma}(\boldsymbol{x})$, it implies that $\boldsymbol{n} \in R$.

The sets $F_{2,\sigma}$ For the sake of simplicity, let us consider the permutation $\sigma = (0, \ldots, d-1)$ and let $F_2 = F_{2,(0,\ldots,d-1)}$. For all $\boldsymbol{n} \in F_2$, for all $i \in [d-2]$, $n_i \leq n_{i+1}$.

It follows from hypothesis (a.) that, for all $p \in \mathbb{N}$, the section $\mathrm{sec}(R; x_0 = p)$ is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. By the induction hypothesis there exists an integer $t'_p = \mathrm{thres}_m(\mathrm{sec}(R; x_0 = p))$ such that $\mathrm{sec}(R; x_0 = p)$ is m-periodic in $(\mathbb{N}^{\geq t'_p})^{d-1}$. Let $t' = \max\left\{t'_p \mid p \in [\tau, \tau + m - 1]\right\}$.

In the example of Figure 3.2, $\mathrm{thres}_m(\mathrm{sec}(R; x_0 = 2)) = 0$ and $\mathrm{thres}_m(\mathrm{sec}(R; x_0 = 3)) = 8$. Hence $t' = 8$. The line $x_1 = 8$ is represented by the horizontal dashed line. It should be noted that the sections $\mathrm{sec}(R; x_0 = 2)$ and $\mathrm{sec}(R; x_0 = 3)$ are 2-periodic on the right side of this line.

Let $F_3 = \{\boldsymbol{x} \in F_2 \mid x_0 + t' \leq x_1\}$. The set F_3 is considered for two reasons:

- for $p \in [\tau, \tau + m - 1]$, $\mathrm{sec}(R; x_0 = p)$ is m-periodic in $\mathrm{sec}(F_3; x_0 = p)$, and
- it is proven below that, for $p \geq \tau + m$, the study of sections $\mathrm{sec}(R; x_0 = p)$ can be reduced to the study of the m sections $\mathrm{sec}(R; x_0 = p')$ for $p' \in [\tau, \tau + m - 1]$.

As for F_1, the formula $\phi_2(\boldsymbol{x})$ which defines R in F_2 is constructed, using the formula $\phi_3(\boldsymbol{x})$ which defines R in F_3, a formula which defines R in $F_2 \setminus F_3$, and a formula which defines F_3 in F_2. By the induction hypothesis, for each $i \in \mathbb{N}$, there exists a formula $\psi_{\mathrm{diag}(R; x_1 = x_0 + i)}(x_0 \cdots, x_{d-2})$ which defines the diagonal $\mathrm{diag}(R; x_1 = x_0 + i)$ in $\mathbb{N}^d$, hence in F_2. Let us assume that $\phi_3(\boldsymbol{x})$ is a formula which defines R in F_3. Then R is defined in F_2 by the formula $\phi_2(\boldsymbol{x})$:

$$\langle \bigvee_{i=0}^{t'-1} x_0 + i \doteq x_1 \mid \psi_{\mathrm{diag}(R; x_1 = x_0 + i)}(x_0, x_2 \cdots, x_{d-1}) \mid \phi_3(\boldsymbol{x}) \rangle.$$

In the example of Figure 3.2, n^1 belongs to F_3 and n^2 does not belong to F_3. The diagonal dashed line represents the boundary of F_3.

The proof that $\boldsymbol{n} \in R$ is equivalent to $\mathcal{N}' \models \phi_3$ is similar to the proof for F_1, except that diagonals are considered instead of sections.

The set F_3 Let us now consider the set F_3. Note that $n_0 + t' \leq n_1$ for all $\boldsymbol{n} \in F_3$.

For all $\boldsymbol{n} \in F_3$, let n''_0 the be least integer greater than τ equivalent to n_0 modulo m. Equivalently, n''_0 is the only element of $[\tau, \tau + m - 1]$ equivalent to n_0 modulo m.

In the example of Figure 3.2, the vertical dashed line represents $x_0 = 4 = \tau + m$.

Then, let $\boldsymbol{n''} \in \mathbb{N}^d$ be the d-tuple such that $n''_i = n_i$ for each $i > 0$.

For Figure 3.2 when $\boldsymbol{n} = \boldsymbol{n^2}$, then $\boldsymbol{n''}$ is equal to $(3, 17)$, which is denoted by $\boldsymbol{n''_2}$ in the figure.

Let us claim that for all $\boldsymbol{n} \in F_3$, $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n''} \in R$. In this case, R is defined in F_3 by the formula $\phi_3(\boldsymbol{x})$:

$$\bigvee_{k=\tau}^{\tau+m-1} x_0 \equiv k \mod m \wedge \psi_{\mathrm{sec}(R; x_0 = k)}(x_1, \cdots, x_{d-1}).$$

It remains to prove that $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n''} \in R$. Let $k = \frac{n_0 - n_0''}{m}$ and let $\boldsymbol{n'} \in \mathbb{N}^d = \boldsymbol{n} - k(\overline{m,\dots,m}^d)$. It suffices to prove that $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n'} \in R$ and that $\boldsymbol{n'} \in R$ is equivalent to $\boldsymbol{n''} \in R$. For Figure 3.2 with $\boldsymbol{n} = \boldsymbol{n}^2$, the value $\boldsymbol{n'}$ is $\boldsymbol{n}'_{\boldsymbol{2}}$ in the figure.

Let us first prove that $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n'} \in R$. By induction on $i \in \mathbb{N}$, $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n} - i(\overline{m,\dots,m}^d) \in R$ when $n_0 - im \geq \tau$. And since $\boldsymbol{n'} = \boldsymbol{n} - k(\overline{m,\dots,m}^d)$ and $n'_0 = n''_0 \geq \tau$ by construction, $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n'} \in R$.

Let us now prove that $\boldsymbol{n'} \in R$ is equivalent to $\boldsymbol{n''} \in R$. Let $\boldsymbol{N'}$ and $\boldsymbol{N''}$ be $\boldsymbol{n'}$ and $\boldsymbol{n''}$ without their first component, respectively. Since $n'_0 = n''_0$, it suffices to prove that $\boldsymbol{N'} \in \mathrm{sec}(R; x_0 = n'_0)$ is equivalent to $\boldsymbol{N''} \in \mathrm{sec}(R; x_0 = n'_0)$.

It should be noted that $n_0 \geq 0$ and $n_1 - n_0 \geq t'$, hence $n_1 \geq t'$. And by definition of t', $\mathrm{sec}(R; x_0 = n'_0)$ is m-periodic in $(\mathbb{N}^{\geq t'})^{d-1}$. Hence, by induction on $i \in \mathbb{N}$, $\boldsymbol{N'} \in \mathrm{sec}(R; x_0 = n'_0)$ is equivalent to $\boldsymbol{N'} + i(\overline{m,\dots,m}^{d-1}) \in \mathrm{sec}(R; x_0 = n'_0)$. In particular, $\boldsymbol{N''} = \boldsymbol{N'} + k(\overline{m,\dots,m}^{d-1})$, hence $\boldsymbol{N'} \in \mathrm{sec}(R; x_0 = n'_0)$ is equivalent to $\boldsymbol{N''} \in \mathrm{sec}(R; x_0 = n'_0)$. □

Since the characterization given in Theorem 3.3.1 is $\mathsf{FO}[<]$-expressible, Theorem 3.3.1 admits the following corollary, similar to Theorem 3.2.9.

Corollary 3.3.4. *Let $d, m \in \mathbb{N}^{>0}$, and R be a relation symbol of arity d. There exists a $\Pi_3[<,+,R]$-formula $\mu_{d,m}$ which holds over $\{R\}$-structures $\mathcal{S}$ such that $R^{\mathcal{S}}$ is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable.*

Proof. The proof mostly uses the formula $\mathrm{sub}(R, \boldsymbol{t}, \boldsymbol{c})$ introduced in Notation 2.2.26. Let $\mu_{d,m}$ be:

$$\bigwedge_{\boldsymbol{t} \in (\{\mathrm{var},\mathrm{const}\} \cup \{\mathrm{add}(i) \mid i \in [d-1]\})^d} \forall \boldsymbol{c}.\exists N.\forall (n_i > N)_{t_i = \mathrm{var}} \Big\{ \mathrm{sub}(R,\boldsymbol{t},\boldsymbol{c})(\boldsymbol{n}) \Longleftrightarrow \mathrm{sub}(R,\boldsymbol{t},\boldsymbol{c})(\boldsymbol{n} + (\overline{m,\dots,m}^{\dim(t)})) \Big\}.$$

□

The formula which defines the value of $\mathrm{thres}_m(R)$ is now given.

Lemma 3.3.5. *Let $d \in \mathbb{N}^{>0}$, let $m \in \mathbb{N}$. Let R be a relation symbol with arity d.*

There exists a $\Pi_1[+m, <, R]$-formula $\theta_{d,m}(x)$ such that if $R^{\mathcal{S}}$ is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable then:

- $\theta_{d,m}(x)^{\mathcal{S}} = \left\{ \mathrm{thres}_m\left(R^{\mathcal{S}}\right) \right\}$ *and*
- $\theta_{d,m}(x)^{\mathcal{S}_{|n}} = \left\{ \mathrm{thres}_m\left(R^{\mathcal{S}}\right) \right\}$ *for all* $n > \mathrm{thres}_m\left(R^{\mathcal{S}}\right) + m$.

It should be noted that the interpretation of $\theta_{d,m}(x)^{\mathcal{S}_{|n}}$ for $n < \mathrm{thres}_m\left(R^{\mathcal{S}}\right) + m$ is undefined.

Proof. The $\Pi_1[<, +\mathbb{N}, R]$-formula $\theta_{d,m}(x)$ is the conjunction of two subformulas. The first one, $\phi_{\geq}(x)$ states that the threshold is at most x. It is:

$$\forall n_0, \cdots, n_{d-1} \left(\bigwedge_{i=0}^{d-1} n_i \geq x \right) \Longrightarrow [R(n_0, \cdots, n_{d-1}) \iff R(n_0 + m, \cdots, n_{d-1} + m)].$$

The second formula, $\phi_{>-1}(x)$, states that the threshold is strictly greater than $x - 1$. That is, either $x = 0$, or there exists $\boldsymbol{n} \in \mathbb{N}^d$ with $\min(\boldsymbol{n}) = x - 1$ and $\boldsymbol{n} \in R$ is not equivalent to $\boldsymbol{n} + (\overline{m,\dots,m}^d) \in R$. It is:

$$x \doteq 0 \vee \exists \boldsymbol{y}. \left(\bigvee_{i=0}^{d-1} y_i + 1 \doteq x \wedge \bigwedge_{i=0}^{d-1} y_i \geq x - 1 \wedge \left(R(y) \Longleftrightarrow \neg R(y + (\overline{m,\dots,m}^d)) \right) \right).$$

Then, let $\theta_{d,m}(x)$ be $\phi_{\geq}(x) \vee \phi_{>-1}(x)$.

For any universe of cardinality greater than $\text{thres}_{d,m}\left(R^{\mathcal{S}}\right) + m$, the integer $\text{thres}_{d,m}\left(R^{\mathcal{S}}\right)$ is the only value which satisfies the formula. Hence $\theta_{d,m}(x)$ converges. □

In Section 3.3.2 and in Section 3.4, proofs consider the evolution of thresholds of sections.

Definition 3.3.6. Let $d \in \mathbb{N}^{>1}$, and let $R \subseteq \mathbb{N}^d$. Then let $\tau_{R,m}(n)$ be the function which maps $n \in \mathbb{N}$ to the greatest threshold of section $\text{sec}(R; x_0 = i)$ for $i \leq n$. Formally:

$$\tau_{R,m}(n) = \max\{\text{thres}_m(\text{sec}(R; x_0 = r)) \mid r \leq n\}.$$

Lemma 3.3.7. *Let $d \in \mathbb{N}^{>1}$, let R be a relation symbol with arity d and let $\mathcal{S}$ be a $\{<, +\mathbb{N}, R\}$-structure. There exists a $\Pi_2[<, +\mathbb{N}, R]$-formula $\tau_{d,m}(N; x)$ which defines the function $\tau_{R^{\mathcal{S}},m}$.*

The naive method would be to universally quantify the value $n \leq N$ and use $\text{thres}_m[R](x_1, \ldots, x_{d-1})$ on the sections $\text{sec}(R; x_0 = n)$. But such a formula does not belong to $\Pi_2[<, +\mathbb{N}, R]$.

Proof. The formula $\tau_{R^{\mathcal{S}},m}$ is now constructed. It is similar to the formula of Lemma 3.3.5.

The formula $\tau_{d,m}(N; x)$ is the conjunction of two formulas. The first formula $\phi_{\geq}(N, x)$, states that the threshold of every sections $\text{sec}(R; x_0 = n)$ is less than x for all $n \leq N$. Let $\phi_{\geq}(N, x)$ be the $\Pi_2[<, +\mathbb{N}, R]$-formula:

$$\forall n < N. \langle \forall z_1 \geq x, \cdots, z_{d-1} \geq x. \rangle (R(n, z_1, \cdots, z_{d-1}) \Longleftrightarrow R(z, z_1 + m, \cdots, z_{d-1} + m)).$$

The second formula, $\phi_{>-1}(N, x)$, states that there exists some $n \leq N$ such that the threshold of the sections $\text{sec}(R; x_0 = n)$ is strictly greater than $x - 1$. It is possible either if $x = 0$, or if there exists $\boldsymbol{n} \in \mathbb{N}^d$ with $n_0 \leq N$ and $\min\{n_1, \ldots n_{d-1}\} = x - 1$ such that $\boldsymbol{n} \in R$ is not equivalent to $\boldsymbol{n} + (0, \overline{m, \ldots, m}^{d-1}) \in R$. Let $\phi_{>-1}(N, x)$ be the $\Pi_2[<, +\mathbb{N}, R]$-formula:

$$x \doteq 0 \vee \exists \boldsymbol{n}. \left[n_0 \leq N \wedge \bigvee_{i=1}^{d-1} n_i \doteq x - 1 \wedge \left(R(\boldsymbol{n}) \Longleftrightarrow \neg R(\boldsymbol{n} + (\overline{m, \ldots, m}^d)) \right) \right].$$

Then let $\tau_{d,m}(N; x)$ be $\phi_{\geq}(N, x) \wedge \phi_{>-1}(N, x)$. □

Theorem 3.2.5 of [Muc03] admits the following easy corollary:

Theorem 3.3.8 ([Muc03, Theorem 3])**.** *Let M be a finite automaton over integers, as in Definition 2.3.6. It is decidable whether the set recognized by M is definable in Presburger Arithmetic.*

Similarly, Corollary 3.3.4 admits the following corollary:

Corollary 3.3.9. *Let M be a finite automaton as in Definition 2.3.6. It is decidable whether the set recognized by M is $\mathsf{FO}[<, \text{mod}\, m]$-definable (respectively, $\mathsf{FO}[<, \text{mod}]$-definable).*

The proof follows closely the proof of [Muc03, Theorem 3].

Proof. The addition and order relation are recognizable by finite automata. The family of recognizable sets is closed under logical operations. Therefore, it is possible to construct an automaton which encodes the formula $\mu_{d,m}$ (respectively, $\exists m. \mu_{d,m}$). It recognizes the empty set if $\mu_{d,m}$ (respectively, $\exists m. \mu_{d,m}$) does not hold, hence if the set recognized by M is not $\mathsf{FO}[<, \text{mod}\, m]$-definable (respectively, not $\mathsf{FO}[<, \text{mod}]$-definable). □

Corollary 3.3.4 admits another corollary, similar to Corollary 3.3.9, considering formulas as inputs instead of automata.

Corollary 3.3.10. *It is decidable whether a* $\mathsf{FO}[+, V_b]$*-formula is equivalent to a* $\mathsf{FO}[<, \mathrm{mod}]$*-formula (respectively, to a* $\mathsf{FO}[<, \mathrm{mod}\, m]$*-formula).*

Another algorithm to decide whether $\phi(\boldsymbol{x})$ defines a $\mathsf{FO}[<, \mathrm{mod}]$-definable set is given in [Cho08, Theorem 10].

Proof. Since $\mathsf{FO}[+]$ is decidable, by [Pre27], it suffices to test whether the formula $\exists m.\mu_{d,m}$ (respectively, $\mu_{d,m}$), where $R(\boldsymbol{x})$ is replaced by $\phi(\boldsymbol{x})$, holds. □

3.3.2 Extracting a unary set from a non $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable set

In this section, a theorem similar to Theorem 3.2.12 is proved, for $\mathsf{FO}[<, \mathrm{mod}\, m]$.

Theorem 3.3.11. *Let* $d, m \in \mathbb{N}^{>0}$*, and* R *be a relation symbol with arity* d*. Let* $\mathcal{S}$ *be a* $\{<, R\}$*-structure with universe* $\mathbb{N}$ *such that* $R^{\mathcal{S}}$ *is not* $\mathsf{FO}[<, \mathrm{mod}\, m]$*-definable.*

There exists a $\mathsf{FO}[<, R]$*-formula* $\nu_{m,R}(x)$ *such that* $\nu_{m,R}(x)^{\mathcal{S}}$ *is not ultimately* m*-periodic.*

In other words, a set R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable if and only if every unary $\mathsf{FO}[<, R]$-definable set is ultimately m-periodic.

The following proposition, which considers the simpler case of an increasing function, must be proved first.

Proposition 3.3.12. Let $m \in \mathbb{N}^{>0}$. Let f be a unary function symbol. Let $\mathcal{S}$ be a $\{<, f\}$-structure with universe $\mathbb{N}$ such that $f^{\mathcal{S}}$ is increasing, unbounded and not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Then there exists a $\mathsf{FO}[<, f]$-formula $\nu_{m,f}(x)$ such that $\nu_{m,f}(x)^{\mathcal{S}}$ is not ultimately m-periodic.

To prove this proposition, the two following lemmas must first be proved. The first lemma is similar to Proposition 3.3.12. The only difference is that $\mathrm{mod}\, m$ also belongs to the vocabulary. The second lemma let us encode the modular predicate using only the increasing function f and the order relation.

Lemma 3.3.13. *Let* $m \in \mathbb{N}^{>0}$*. Let* f *be a unary function symbol. Let* $\mathcal{S}$ *be a* $\{<, f\}$*-structure with universe* $\mathbb{N}$ *such that* $f^{\mathcal{S}}$ *is increasing, unbounded and not* $\mathsf{FO}[<, \mathrm{mod}\, m]$*-definable. Then there exists a* $\mathsf{FO}[<, \mathrm{mod}\, m, f]$*-formula* $\nu'_{m,f}(x)$ *such that* $\nu'_{m,f}(x)^{\mathcal{S}}$ *is not ultimately* m*-periodic.*

The proof of Lemma 3.3.13 consists in a disjunction between three cases. Let us first give an example of three applications of this lemma, considering each of the three cases.

Example 3.3.14. Let $m = 2$. Some $\{<, f\}$-structures $\mathcal{S}$ are given, such that $f^{\mathcal{S}}$ is not ultimately m-periodic. Then, for each structure, a $\mathsf{FO}[<, f]$-formula ϕ is given such that $\phi^{\mathcal{S}}$ is not ultimately 2-periodic.

- Let $f^{\mathcal{S}}(n) = 4n$. In this case, it suffices to consider the image of f. let $\phi(x)$ be $\exists y.f(y) \doteq x$, then $\phi(x)^{\mathcal{S}} = 4\mathbb{N}$, which is not ultimately 2-periodic.
- Let $f^{\mathcal{S}}(n) = \left\lfloor \frac{n}{2} \right\rfloor$. Its image is $\mathbb{N}$ which is ultimately 2-periodic. In this case, it suffices to consider the pre-image of an equivalence class. Let $\phi(x)$ be $f(x) \equiv 0 \mod 2$, then $\phi(x)^{\mathcal{S}} = 4\mathbb{N} \cup (4\mathbb{N} + 1)$, which is not ultimately 2-periodic.
- Let $f^{\mathcal{S}}(n) = 2\left\lfloor \frac{n}{4} \right\rfloor$. Its image is $2\mathbb{N}$, the pre-image of $2\mathbb{N}$ and of $2\mathbb{N} + 1$ are $\mathbb{N}$ and $\emptyset$, which are ultimately 2-periodic. In this case, it suffices to consider the part of $\mathbb{N}$ where f does not increase. Let $\phi(x)$ be $f(x) \doteq f(x + 2)$, then $\phi(x)^{\mathcal{S}} = 4\mathbb{N} \cup (4\mathbb{N} + 1)$, which is not ultimately 2-periodic.

Lemma 3.3.13 is now proved.

Proof of Proposition 3.3.12. Since $f^{\mathcal{S}}$ is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable, according to Lemma 3.1.3 there exists $k \in [m-1]$ such that there are no $N, r \in \mathbb{N}$ such that $f(n) = n + r$ for every $n > N$ and $n \equiv k \mod m$. From now on, let us consider $f_{|m\mathbb{N}+k} : m\mathbb{N} + k \to \mathbb{N}$, the restriction of $f^{\mathcal{S}}$ on the set $m\mathbb{N} + k$, and its image $Im(f_{|m\mathbb{N}+k})$.

Two cases must be considered, depending on whether $Im(f_{|m\mathbb{N}+k})$ is ultimately m-periodic or not. Let us first assume that $Im(f_{|m\mathbb{N}+k})$ is not ultimately m-periodic. Then, let $\nu'_{m,f}(x)$ be

$$\exists y \equiv k \mod m . f(y) \doteq x.$$

Let us now assume that the image $Im(f_{|m\mathbb{N}+k})$ of $f_{|m\mathbb{N}+k}$ is ultimately m-periodic. Since f is unbounded and increasing, then $Im(f_{|m\mathbb{N}+k})$ is infinite. Hence, there exists $\tau = \mathrm{thres}_m(Im(f_{|m\mathbb{N}+k})) \in \mathbb{N}$ and $P = \mathrm{mod}_m(Im(f_{|m\mathbb{N}+k})) \subseteq [m-1]$ as in Definition 3.1.1. That is, for all $n \geq \tau$, $n \in Im(f_{|m\mathbb{N}+k})$ if and only if $n \equiv p \mod m$ for some $p \in \mathbb{N}$. Since $Im(f_{|m\mathbb{N}+k})$ is infinite, then P is non-empty.

Two cases must be considered depending on whether $|P| = 1$ or $|P| \geq 2$. Let us first assume that P contains two distinct elements q and q'. Then the inverse of $m\mathbb{N} + q$ (respectively of $m\mathbb{N} + q'$) by $f_{|m\mathbb{N}+k}$ contains an infinite number of elements. It implies that the inverse of $m\mathbb{N} + q'$ by $f_{|m\mathbb{N}+k}$ is infinite, and its complement in $m\mathbb{N} + k$ is also infinite. Hence the inverse of $m\mathbb{N} + q'$ by $f_{|m\mathbb{N}+k}$ is not ultimately m-periodic. Then, let $\nu'_{m,f}(x)$ be:

$$f(x) \equiv q \mod m.$$

Let us now assume that P is the singleton $\{p\}$. Let us claim that the set

$$E = \{n \equiv k \mod m \mid f_{|m\mathbb{N}+k}(n) = f_{|m\mathbb{N}+k}(n+m)\}$$

is not ultimately m-periodic. In this case, let $\nu'_{m,f}(x)$ be:

$$f(x) \doteq f(x+m).$$

Let us now prove that E is not ultimately m-periodic. It suffices to prove that E is infinite and $(m\mathbb{N} + k) \setminus E$ is infinite.

Let us first prove that $(m\mathbb{N} + k) \setminus E$ is infinite. Let $N \equiv k \mod m$ and let us prove that there exists $n > N$ such that $n \notin E$, that is, such that $f(n) \neq f(n+m)$. Since $f_{|m\mathbb{N}+k}$ is unbounded, there exists $n' \equiv k \mod m$ such that $f(n') > f(N+m)$, and since f is increasing, $n' > N + m$. Let us assume that n' is chosen minimal. Let us prove that $n = n' - m$ is such that $f(n) \neq f(n+m)$.

By the minimality of n', $f(n'-m) \leq f(N+m)$. Finally, $f(n) = f(n'-m) \leq f(N+m) < f(n') = f(n+m)$.

Let us now prove that E is infinite. Let $N > \max(\tau, 2m)$ be such that $N \equiv k \mod m$ and let us prove that there exists $n \geq N$ belonging to E. Let $r = f_{|m\mathbb{N}+k}(N-m) - (N-m)$. Let n be the minimal integer such that $n \geq N + m$, $n \equiv k \mod m$ and $f_{|m\mathbb{N}+k}(n) \neq n + r$, by hypothesis about k it exists. Let us prove that $n - m \in E$, note that $n - m \geq N$. By definition of E, it suffices to prove that $f_{|m\mathbb{N}+k}(n) = f_{|m\mathbb{N}+k}(n-m)$. Since n is minimal, either $n = N + m$ or $f_{|m\mathbb{N}+k}(n-m) = n - m + r$. Note that $f(N-m) = N - m + r$ hence $n \neq N - m$. The two preceding statements implies that $f_{|m\mathbb{N}+k}(n-m) = n - m + r$.

For the sake of contradiction, let us now assume that $f_{|m\mathbb{N}+k}(n) \neq f_{|m\mathbb{N}+k}(n-m)$. Let us claim that $f_{|m\mathbb{N}+k}(n) \geq n + r + m$. Since $n + r \equiv p \mod m$ and $n + r \geq \tau$, by definition of τ, there exists $s \in m\mathbb{N} + k$ such that $f_{|m\mathbb{N}+k}(s) = n + r$. Since $n + r - m < n + r < n + r + m \leq f_{|m\mathbb{N}+k}(n)$, $n + r - m = f_{|m\mathbb{N}+k}(n-m)$,

$n + r = f_{|m\mathbb{N}+k}(s)$ and $f_{|m\mathbb{N}+k}$ is increasing, $n - m < s < n$. Since $s \equiv p$ and $p \equiv n \mod m$ then $s \equiv n \mod m$. Having both $s \equiv n \mod m$ and $n - m < s < n$ is a contradiction.

Let us now prove that $f_{|m\mathbb{N}+k}(n) \geq n + r + m$. It follows from the following (in)equalities:

- Since $f_{|m\mathbb{N}+k}$ is increasing, $f_{|m\mathbb{N}+k}(n) \geq f_{|m\mathbb{N}+k}(n - m)$.
- Since $f_{|m\mathbb{N}+k}(n) \neq f_{|m\mathbb{N}+k}(n - m)$, $f_{|m\mathbb{N}+k}(n) > f_{|m\mathbb{N}+k}(n - m)$.
- By minimality of n, $f_{|m\mathbb{N}+k}(n - m) = n - m + r$, hence $f_{|m\mathbb{N}+k}(n) > f_{|m\mathbb{N}+k}(n - m) = n - m + r$.
- Since $n \geq \tau$, $f_{|m\mathbb{N}+k}(n) \equiv p \mod m$. Let us claim that $n + r \equiv p \mod m$ then $f_{|m\mathbb{N}+k}(n) \geq n + r$. Let us now prove that $n + r \equiv p \mod m$. Since $n - m > \tau$, $n + r \equiv n + r - m = f_{|m\mathbb{N}+k}(n - m) \equiv p \mod m$.
- By $f_{|m\mathbb{N}+k}(n) \geq n + r$ and by definition of n, $f_{|m\mathbb{N}+k}(n) \neq n + r$, hence $f_{|m\mathbb{N}+k}(n) > n + r$.
- Having $f_{|m\mathbb{N}+k}(n) \equiv p \mod m$, $n + r \equiv p \mod m$ and $f_{|m\mathbb{N}+k}(n) > n + r$ imply $f_{|m\mathbb{N}+k}(n) \geq n + r + m$.

□

The following lemma states how to define a modular relation using an ultimately periodic set of integers.

Lemma 3.3.15. *Let R be a monadic relation symbol. Let $\mathcal{S}$ be an $\{<, R\}$-structure such that $R^{\mathcal{S}}$ is ultimately periodic. Let $m \in \mathbb{N}^{>0}$ be the least period of $R^{\mathcal{S}}$. Then $m\mathbb{N}$ is $\mathsf{FO}[<, R]$-definable in $\mathcal{S}$.*

Proof. Since $R^{\mathcal{S}}$ is ultimately m-periodic, there exist $\tau \in \mathbb{N}$ and $\mathrm{mod}_m(R^{\mathcal{S}}) \subseteq [m - 1]$ as in Definition 3.1.1. That is, for all $n \geq \tau$, $n \in Im(f_{|m\mathbb{N}+k})$ if and only if $n \equiv p \mod m$ for some $p \in \mathrm{mod}_m(R^{\mathcal{S}})$.

Let us assume that $\phi_{\geq\tau}(x)$ defines $m\mathbb{N}$ in $\mathbb{N}^{\geq\tau}$. Then $m\mathbb{N}$ is defined by

$$\phi(x) = \langle i < \tau \mid \bigvee_{i=0}^{\frac{\tau}{m}} x = im \mid \phi_{\geq\tau}(x) \rangle.$$

Let us now define $\phi_{\geq\tau}(x)$ which defines $m\mathbb{N}$ in $\mathbb{N}^{\geq\tau}$. Let us assume that $n \equiv 0 \mod m$ for all $n \geq \tau$ if and only if $n + p \in R^{\mathcal{S}}$ for all $p \in \mathrm{mod}_m(R^{\mathcal{S}})$ and $n + p \notin R^{\mathcal{S}}$ for all $p \in [m - 1] \setminus \mathrm{mod}_m(R^{\mathcal{S}})$. Then let $\phi_{\geq\tau}(x)$ be:

$$\bigwedge_{p \in \mathrm{mod}_m(R^{\mathcal{S}})} R(x + p) \wedge \bigwedge_{p \in [m-1] \setminus \mathrm{mod}_m(R^{\mathcal{S}})} \neg R(x + p).$$

Let us prove that for all $n \geq \tau$, the two following statements are equivalent:

1. $n \equiv 0 \mod m$ and
2. for all $p \in \mathrm{mod}_m(R^{\mathcal{S}})$, $n + p \in R^{\mathcal{S}}$ and for all $p \in [m - 1] \setminus \mathrm{mod}_m(R^{\mathcal{S}})$, $n + p \notin R^{\mathcal{S}}$.

The fact that (1) implies (2) follows directly from the definition of τ and $\mathrm{mod}_m(R^{\mathcal{S}})$. Let us prove that (2) implies (1).

For the sake of contradiction, let us assume that there exists $k \in [m-1] \setminus \{0\}$ such that $n \equiv k \mod m$. It implies that for all $p \in [m - 1]$, $p \in \mathrm{mod}_m(R^{\mathcal{S}})$ is equivalent to $p + k \in \mathrm{mod}_m(R^{\mathcal{S}})$ if $p + k < m$, and to $p + k - m \in \mathrm{mod}_m(R^{\mathcal{S}})$ otherwise.

Let us prove that $R^{\mathcal{S}}$ is ultimately

$$k$$

-periodic, which contradicts the minimal hypothesis about m. It suffices to prove that for all $n \geq \tau$, $n \in R^{\mathcal{S}}$ if and only if $n + k \in R^{\mathcal{S}}$.

Let $n \geq \tau$, the following statements are equivalent:

- $n \in R^{\mathcal{S}}$,
- by definition of $\mathrm{mod}_m(R^{\mathcal{S}})$: $n \mod m \in \mathrm{mod}_m(R^{\mathcal{S}})$,
- by hypothesis about k: $n + k \mod m \in \mathrm{mod}_m(R^{\mathcal{S}})$,
- by definition of $\mathrm{mod}_m(R^{\mathcal{S}})$: $n + k \in R^{\mathcal{S}}$.

□

Proposition 3.3.12 is now proved.

Proof of Proposition 3.3.12. The proof consists in exhibiting a $\mathsf{FO}[<, f]$-formula which defines a set which is not ultimately

$$m$$

-periodic.

Let $m_f \in \mathbb{N}^{>0}$ be the greatest integer which divides m and is such that $m_f\mathbb{N}$ is $\mathsf{FO}[<, f]$-definable in $\mathcal{S}$. Note that 1 divides m and $1\mathbb{N}$ is $\mathsf{FO}[<, f]$-definable in $\mathcal{S}$, hence m_f is correctly defined. Let ϕ_{m_f} be the $\mathsf{FO}[<, f]$-formula which defines $m_f\mathbb{N}$ in $\mathcal{S}$.

Since f is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable and m_f divides m, f is not $\mathsf{FO}\left[<, \mathrm{mod}\, m_f\right]$-definable. By Lemma 3.3.13 there exists a $\mathsf{FO}\left[<, f, \mathrm{mod}\, m_f\right]$-formula ξ'_E which defines a set $E \subseteq \mathbb{N}$ which is not ultimately

$$m_f$$

-periodic. Let ξ_E be the $\mathsf{FO}[<, f]$-formula ξ'_E where each occurrence of $x \equiv a \,\mathrm{mod}\, m_f$ is replaced by $\phi_{m_f}(x - a + m_f)$, it also defines E.

Let m_E be the least integer such that E is ultimately

$$m_E$$

-periodic. By Lemma 3.3.15, there exists a $\mathsf{FO}[<, E]$-formula ψ_{m_E} which defines $m_E\mathbb{N}$ in $\mathcal{S}$. Let ϕ_{m_E} be the $\mathsf{FO}[<, f]$-formula ψ_{m_E} where $E(x)$ is replaced by ξ_E; it defines $m_E\mathbb{N}$ in $\mathcal{S}$. Note that E is ultimately

$$n$$

-periodic if and only if m_E divides n, for all $n \in \mathbb{N}^{>0}$. Two cases must be considered, depending on whether m_E divides m or not. If m_E does not divide m, then E is not ultimately

$$m$$

-periodic, hence the result is proved. Let us now assume that m_E divides m. Since E is not ultimately

$$m_f$$

-periodic, m_E does not divide m_f.

Let $m_{\mathrm{lcm}} = \mathrm{lcm}(m_f, m_E)$. Since m_E does not divide m_f, $m_{\mathrm{lcm}} > m_f$. Since m_f and m_E divides m, m_{lcm} divides m. The set $m_{\mathrm{lcm}}\mathbb{N}$ is $\mathsf{FO}[<, f]$-defined by $\phi_{m_f} \wedge \phi_{m_E}$. Since $m_{\mathrm{lcm}}\mathbb{N}$ is $\mathsf{FO}[<, f]$-definable and m_{lcm} divides m, by maximality hypothesis about m_f, $m_{\mathrm{lcm}} \leq m_f$. Having $m_{\mathrm{lcm}} > m_f \geq m_{\mathrm{lcm}}$ is a contradiction. □

The following technical lemma states that, given some specific conditions about the evolution of thresholds of sections, it can be claimed that a set is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. This lemma is used both for Theorem 3.4.1 and for Theorem 3.3.11. Recall that the notation $\mathbb{N}^d_{0,\cdots,d-1}$, is introduced in Definition 2.2.28.

Lemma 3.3.16. *Let $d \geq 2$, $m \in \mathbb{N}^{>0}$ and $R \subseteq \mathbb{N}^d_{0,\cdots,d-1}$, be such that:*

- *all of its sections and diagonals are* $\mathsf{FO}[<, \mathrm{mod}\, m]$*-definable, and*
- *the function $\tau_{R,m}$ is* $\mathsf{FO}[+]$*-definable and its slope r is at most 1.*

Then R is $\mathsf{FO}[<, \mathrm{mod}\, m]$*-definable.*

It should be noted that if $\tau_{R,m}$ is $\mathsf{FO}[<, \mathrm{mod}]$-definable then its slope is 0 or 1. Hence this lemma implies that if $\tau_{R,m}$ is $\mathsf{FO}[<, \mathrm{mod}]$-definable then R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable.

Moreover the function $\tau_{R,m}$ is increasing, hence the notion of slope is defined for $\tau_{R,m}$.

Proof. Since $\tau_{R,m}$ is $\mathsf{FO}[<, \mathrm{mod}]$-definable, it is $\mathsf{FO}[<, \mathrm{mod}\, m']$-definable for some $m' \in \mathbb{N}$. The Figure 3.3 illustrates the proof, with the function $\tau_{R,m}$ represented by unfilled circles.

In the example, $\tau_{R,m}(0) = 0$ and $\tau_{R,m}(n) = 3\left\lceil \frac{n}{3} \right\rceil$ for all positive n, thus $\tau_{R,m}$ is $\mathsf{FO}[<, \mathrm{mod}\, 3]$ definable.

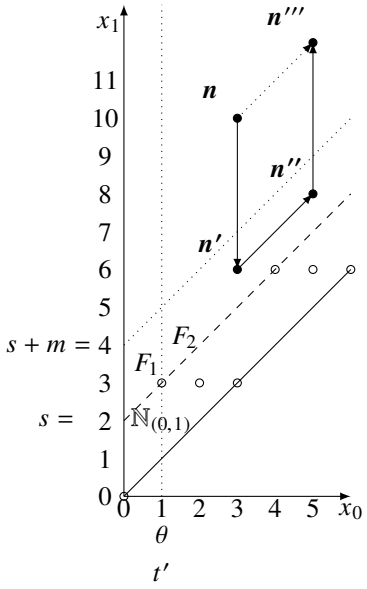


Figure 3.3: Example for Lemma 3.3.16

The diagonal line of Figure 3.3 represents the boundary of $\mathbb{N}^2_{0,1}$. By hypothesis, $R \subseteq \mathbb{N}^2_{0,1}$, hence R belongs to the upper-left half of the figure.

By Lemma 3.1.3 there exists $\theta \in \mathbb{N}$, a rational $r < 1$ and $s_0, \ldots, s_{m-1} \in \mathbb{Q}$ such that for all $i \geq \theta$, $\tau_{R,m}(I) = ri + s_{(i \mod m')}$. Let $s = \max\{s_i \mid i \in [m' - 1]\}$.

For the example of Figure 3.3, $r = 1$, $s_0 = 0$, $s_1 = 2$ and $s_2 = 1$ and then $s = 2$.

The $\mathsf{FO}[<, \mathrm{mod}\, m]$-formula ϕ_R which defines R is now constructed. The formula which defines $\tau_{R,m}$ is not used in ϕ_R.

The structure of the proof is similar to the part "(2)$\Longrightarrow$(1)" of the proof of Theorem 3.3.1. A $\subseteq$-decreasing sequence F_0, F_1, F_2 of subsets of $\mathbb{N}^d$, with $F_0 = \mathbb{N}^d$ is introduced. The proof consists in proving that R is definable in F_i by proving that it is definable in F_{i+1} and in $F_i \setminus F_{i+1}$.

The set F_0 Let $F_1 = \{\boldsymbol{x} \in F_0 \mid x_0 + s \leq x_1\}$. The set F_1 is considered, because, by definition of θ, for all $i \geq \theta$ each section $\mathrm{sec}(R; x_0 = i)$ is m-periodic in $\mathrm{sec}(F_1; x_0 = i)$. On Figure 3.3, the dashed diagonal represents the boundary of F_1.

The set $R \setminus F_1$ is equal to

$$\bigcup_{i=0}^{s-1} \{(x_0, x_0 + i, x_1, \ldots, x_{d-2}) \mid (x_0, \ldots, x_{d-2}) \in \mathrm{diag}(R; x_1 = x_0 + i)\},$$

and by hypothesis, each set $\mathrm{diag}(R; x_1 = x_0 + i)$ is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable, hence $R \setminus F_1$ is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Since F_1 is also $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable it remains to prove that R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable in F_1.

The set F_1 Let us now consider F_1. Let t' be the maximal threshold of the diagonals $\mathrm{diag}(R^{\mathcal{S}}; x_1 = x_0 + i)$ for $i \in [s, s + m - 1]$. Let $t'' = \max\{t', \theta\}$. Then let $F_2 = \{\boldsymbol{x} \in F_1 \mid x_0 \geq t''\}$. The set F_2 is considered for two reasons:

- all diagonals $\mathrm{diag}(R; x_1 = x_0 + i)$ are m-periodic for $i \in [s, s + m - 1]$,
- it is proven below that, for $i \geq s$, the study of diagonals $\mathrm{diag}(R; x_0 = x_1 + s)$ can be reduced to the study of the m diagonals $\mathrm{diag}(R; x_0 = x_1 + i')$ for $i' \in [s, s + m - 1]$.

The dotted vertical line of Figure 3.3 represents the boundary of F_2.

The set R in $F_1 \setminus F_2$ is the union of the sets $\mathrm{sec}(R; x_0 = i)$ for $i \in [t'' - 1]$. By hypothesis, those sections are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable hence R is also $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable in $F_1 \setminus F_2$. Furthermore F_2 is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable, hence it remains to prove that R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable in F_2.

The set F_2 Let us now consider the set F_2. Let us prove that R is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable in F_2. By Theorem 3.3.1 it suffices to prove Property 2 of Theorem 3.3.1. Property b. holds by hypothesis. Let us prove Property a. with the threshold being t''. That is, let $\boldsymbol{n} \in F_2$ and let $\boldsymbol{n'''} = \boldsymbol{n} + (\overline{m, \ldots, m}^d)$. It remains to prove that $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n'''} \in R$.

In the example of Figure 3.3, let $m = 2$, $\boldsymbol{n} = (3, 11)$ and $\boldsymbol{n'''} = (5, 12)$.

The equivalence between $\boldsymbol{n} \in R$ and $\boldsymbol{n'''} \in R$ follows from the following equivalences:

- Let $k = \left\lfloor \frac{n_1 - (n_0 + s)}{m} \right\rfloor$ and let $\boldsymbol{n'} = \boldsymbol{n} - k(0, \overline{m, \ldots, m}^{d-1})$, let us prove that $\boldsymbol{n} \in R$ is equivalent to $\boldsymbol{n'} \in R$.

  For the example of Figure 3.3, $k = 2$ and $\boldsymbol{n'} = (5, 8)$.

  Let $\boldsymbol{N}$ and $\boldsymbol{N'}$ be $\boldsymbol{n}$ and $\boldsymbol{n'}$ without their first component. It suffices to prove that $\boldsymbol{N} \in \mathrm{sec}(R; x_0 = n_0)$ is equivalent to $\boldsymbol{N'} \in \mathrm{sec}(R; x_0 = n_0)$. By definition of threshold, it suffices for this to prove that $N'_i \geq \mathrm{thres}_m(\mathrm{sec}(R; x_0 = n_0))$ for all $i \in [d - 2]$. It is a consequence of the following inequalities:

  - $\mathrm{thres}_m(\mathrm{sec}(R; x_0 = n_0)) \leq \tau_{R,m}(n_0)$ by definition of $\tau_{R,m}$,
  - since $\boldsymbol{n} \in F_2$ by definition of F_2 and of t'', $n_0 \geq t'' \geq \theta$. By definition of θ, $\tau_{R,m}(n_0) = rn_0 + s_{(n_0 \bmod m)}$,
  - since $r \leq 1$, then $rn_0 + s_{(n_0 \bmod m)} = n_0 + s_{(n_0 \bmod m)}$,
  - since $s \geq s_k$ for all $k \in [m - 1]$, then $s_{n_0 \bmod m} \leq n_0 + s$,
  - by definition of k, $n_0 + s = n_1 - (n_1 - (n_0 + s)) \leq n_1 - \left\lfloor \frac{n_1 - (n_0 + s)}{m} \right\rfloor m = n_1 - km = n'_1 = N'_0$ and
  - for all $i \in [d - 3]$, let us prove that $N'_i \leq N'_{i+1}$:

* $N'_i = n'_{i+1}$ by definition of $\boldsymbol{N'}$,
* $n'_{i+1} = n_{i+1} - km$ by definition of $\boldsymbol{n'}$
* $n_{i+1} - km \leq n_{i+2} - km$ since $\boldsymbol{n} \in \mathbb{N}^d_{(0,\dots,d-1)}$
* $n_{i+2} - km = n'_{i+2}$ by definition of $\boldsymbol{n'}$,
* $n'_{i+2} = N'_{i+1}$ by definition of N'.

Thus $N'_i = n'_{i+1} = n_i - km \leq n_{i+2} - km = n'_{i+2} = N'_{i+1}$.

Thus, for all $i \in [d-2]$, one has:

$$\begin{aligned}\mathrm{thres}_m(\mathrm{sec}(R; x_0 = n_0)) \leq \tau_{R,m}(n_0) &= rn_0 + s_{n_0 \mod m} \\ &= n_0 + s_{(n_0 \mod m)} \leq n_0 + s \leq N'_0 \leq \dots \leq N'_i.\end{aligned}$$

- Let $\boldsymbol{n''} = \boldsymbol{n'} + (\overline{m,\dots,m}^d)$ and let $k' = n'_1 - n'_0$.

  For the example of Figure 3.3, $\boldsymbol{n''} = (7,10)$ and $k' = 3$. Let us prove that $\boldsymbol{n'} \in R$ if and only if $\boldsymbol{n''} \in R$. Let $\boldsymbol{N''}$ be $\boldsymbol{n''}$ without its first component. It suffices to prove that $\boldsymbol{N'} \in \mathrm{diag}(R; x_1 = x_0 + k')$ is equivalent to $\boldsymbol{N''} \in \mathrm{diag}(R; x_1 = x_0 + k')$. By definition of threshold, it suffices to prove that for all $i \in [d-2]$, $N'_i \geq \mathrm{thres}_m(\mathrm{diag}(R; x_1 = x_0 + k'))$. It follows from the following inequalities:

  - Let us claim that $k' \in [s, s+m-1]$, then $\mathrm{thres}_m(\mathrm{diag}(R; x_1 = x_0 + k')) \leq t'$ by definition of t',
  - by definition of t'', $t' \leq t''$,
  - $t'' \leq n_0$ since $\boldsymbol{n} \in F_2$, by definition of F_2,
  - $n_0 = n'_0$ by definition of $\boldsymbol{n'}$,
  - $n'_0 < n'_1 = N'_0$ as proven in the previous case,
  - for all $i \in [d-2]$, $N'_i \leq N'_{i+1}$ as proven in the previous case.

  Thus, for all $i \in [d-2]$, one has:

  $$\mathrm{thres}_m(\mathrm{diag}(R; x_1 = x_0 + k')) \leq \theta \leq t'' \leq n_0 = n'_0 < n'_1 = N'_0 \leq \dots \leq N'_{i+1}.$$

  It remains to prove that $k' \in [s, s+m-1]$. It follows from the following statements:

  - $\frac{n_1-(n_0+s)}{m} - 1 < \left\lfloor \frac{n_1-(n_0+s)}{m} \right\rfloor \leq \frac{n_1-(n_0+s)}{m}$,
  - $\frac{n_1-(n_0+s)}{m} - 1 < k \leq \frac{n_1-(n_0+s)}{m}$, by definition of k,
  - $n_1 - (n_0 + s) - m < km \leq n_1 - (n_0 + s)$,
  - $-n_1 + n_0 + s \leq -km < -n_1 + n_0 + s + m$, by multiplying by -1,
  - $n_0 + s \leq n_1 - mk < n_0 + s + m$, by adding n_1,
  - $n'_0 + s \leq n'_1 < n'_0 + s + m$, by definition of $\boldsymbol{n'}$,
  - $s \leq n'_1 - n'_0 < s + m$.

- Finally, the proof that $\boldsymbol{n''} \in R$ if and only if $\boldsymbol{n'''} \in R$ is the same as the proof of equivalence of $\boldsymbol{n} \in R$ and $\boldsymbol{n'} \in R$.

□

Let us now prove Theorem 3.3.11.

Proof. The proof is by induction on d. If $d = 1$ then let $\nu_{m,R^{\mathcal{S}}}(x)$ be the formula $R(x)$. It is now assumed that $d > 1$ and that the theorem holds for $d - 1$.

Two cases must be considered, depending on whether there exists a section E of $R^{\mathcal{S}}$ which is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable or not. Let us first assume that there is a section $E = \mathrm{sec}(R^{\mathcal{S}}; x_i = c)$ for $i \in [d-1]$ and $c \in \mathbb{N}$ such that E is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Then by the induction hypothesis, there exists a formula $\nu_{m,S}(x)$ such that $\nu_{m,S}(x)$ defines E in $\mathcal{S}$. Then let $\nu_{m,R^{\mathcal{S}}}(x)$ be the formula $\nu_{m,S}(x)$ where $E(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{d-1})$ is replaced by $R(x_0, \ldots x_{i-1}, c, x_{i+1}, \ldots, x_{d-1})$.

Let us now assume that all sections of $R^{\mathcal{S}}$ are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Similarly, two cases must be considered, depending on whether there exists a diagonal E of $R^{\mathcal{S}}$ which is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. If there exists such a diagonal, the proof is similar to the preceding case. Let us now assume that all diagonals of $R^{\mathcal{S}}$ are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable.

The problem is reduced to the study of a set included in $\mathbb{N}^d_\sigma$ which is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable for some permutation σ.

The set $R^{\mathcal{S}}$ is the union of the $d!$ sets $R^{\mathcal{S}} \cap \mathbb{N}^d_\sigma$ for $\sigma \in \mathbb{S}_{d-1}$. Since $R^{\mathcal{S}}$ is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable, there exists $\sigma \in \mathbb{S}_{d-1}$ such that $R^{\mathcal{S}} \cap \mathbb{N}^d_\sigma$ is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. For the sake of simplicity, let us assume that σ is the identity permutation, that it $(0, \ldots, d-1)$.

Let $R' = R^{\mathcal{S}} \cap \mathbb{N}^d_{(0,\ldots,d-1)}$ and let $\mathcal{S}'$ be $\mathcal{S}[R/R']$. Let us assume that there exists a $\mathsf{FO}[<, R]$-formula $\phi_{R'}$ which defines in $\mathcal{S}'$ a set $E \subseteq \mathbb{N}$ which is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Then it suffices to set $\nu_{m,R}(x)$ as the formula obtained from $\phi_{R'}$ by replacing every atomic formula $R'(\boldsymbol{x})$ by $R(\boldsymbol{x}) \wedge \bigwedge_{i=0}^{d-2} x_i \leq x_{i+1}$.

By Lemma 3.3.16, the function $\tau_{m,R'}$ is not $\mathsf{FO}[<, \mathrm{mod}]$-definable. Then, by Proposition 3.3.12, there exists a set $E \subseteq \mathbb{N}$ which is $\mathsf{FO}[<, R]$-definable and which is not ultimately m-periodic. Since $\tau_{R^{\mathcal{S}},m}$ is $\mathsf{FO}[<, R]$-definable in $\mathcal{S}$, E is $\mathsf{FO}[<, R]$-definable. □

Note that, contrary to Theorem 3.2.12, the formula exhibited in Theorem 3.3.11 depends on the set R. This is because each diagonals must be considered and it is not possible to do it using $\mathsf{FO}[<, \mathrm{mod}]$-formula.

Let us give an example of application of Theorem 3.3.11. Some $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable sets R are considered. From them, some subsets of $\mathbb{N}$ which can be defined from R are considered.

Example 3.3.17. Let $m = 1$ and $R = \{\boldsymbol{x} \mid x_1 + x_2 = x_3 x_0\}$. Fixing x_0 to 1 gives the addition relation, which is not $\mathsf{FO}[<]$-definable. So a $\mathsf{FO}[R, <]$-definable set which is not $\mathsf{FO}[<]$-definable can be obtained by exhibiting a $\mathsf{FO}[+, <]$-definable set which is not $\mathsf{FO}[<]$-definable.

Every section of $+$ is $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable, so induction can not be used anymore. Let $\sigma = (0, 1, 2)$, then $S = + \cap \mathbb{N}^3_{(0,1,2)} = \{\boldsymbol{x} \mid x_0 \leq x_1, x_1 + x_0 = x_2\}$. Let $T_n = \mathrm{sec}(S; x_0 = n) = \{(x, x+n) \mid x \leq n\}$. Then $(n, 2n) \in T_n$ and $(n+1, 2n+1) \notin T_n$, so $\mathrm{thres}_1(n) > 2n$. Having $y, z > n$, $(y, z) \notin T_n$ and $(y+1, z+1) \notin T_n$ imply $\mathrm{thres}_1(n) = 2n+1$, and so $\tau_{R,m}(n) = 2n+1$.

The image of $\tau_{R^{\mathcal{S}},m}$ is the set of odd integers, which is not $\mathsf{FO}[<]$-definable. Note that this set is $\mathsf{FO}[<, \mathrm{mod}\, 2]$-definable.

3.4 Extracting a unary function from a non $\mathsf{FO}[<, \mathrm{mod}]$-definable set

In this section, a characterization of $\mathsf{FO}[<, \mathrm{mod}]$-definable sets is given. It is similar to Theorem 3.2.10.

Theorem 3.2.10 does not directly extend to $\mathsf{FO}[<,\mathrm{mod}]$. Indeed, the addition relation is not $\mathsf{FO}[<,\mathrm{mod}]$-definable but Lemma 3.1.2 states that every $\mathsf{FO}[<,+]$-definable subset of $\mathbb{N}$ is ultimately periodic, hence $\mathsf{FO}[<,\mathrm{mod}]$-definable.

Hence, instead of considering sets of integers, the following theorem considers unary functions.

Theorem 3.4.1. *Let $d \in \mathbb{N}^{>0}$ and R be a relation symbol with arity d. Let $\mathcal{S}$ be a $\{<,R\}$-structure with universe $\mathbb{N}$ such that $R^{\mathcal{S}}$ is $\mathsf{FO}[+]$-definable and not $\mathsf{FO}[<,\mathrm{mod}]$-definable.*

There exists a converging formula $\nu_R(x;y)$ in $\Pi_2[<,+\mathbb{N},R]$ such that $\nu_R(x;y)^{\mathcal{S}}$ is the graph of an increasing function f with slope greater than 1.

This result can be restated as: the function f is of the form $n :\mapsto rn + g(n)$ with $r > 1$ and $g(n)$ bounded.

By Lemma 3.1.3, a function is $\mathsf{FO}[<,\mathrm{mod}]$-definable if and only if its slope is 0 or 1. Hence the function of Theorem 3.4.1 is not $\mathsf{FO}[<,\mathrm{mod}]$-definable. Hence, Theorem 3.4.1 implies that a $\mathsf{FO}[+]$-definable set R is $\mathsf{FO}[<,\mathrm{mod}]$-definable if and only if every unary $\mathsf{FO}[<,R]$-definable function is $\mathsf{FO}[<,\mathrm{mod}]$-definable.

Two lemmas must first be proved. The following lemma states that, when $\mathsf{FO}[+]$-definable sets are considered, one can consider only one periodicity for all straight subspaces of dimension 1.

Lemma 3.4.2. *Let $d \in \mathbb{N}^{>0}$ and $R \subseteq \mathbb{N}^d$ be a $\mathsf{FO}[+]$-definable set. Then there exists $m \in \mathbb{N}^{>0}$ such that every straight subspace of R of dimension 1 is $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable.*

Proof. By Proposition 2.2.21, it can be assumed that R is defined by a quantifier-free formula $\phi \in \mathsf{FO}[+,<,\mathrm{mod}]$. Without loss of generality, it can be assumed that all modular relations are of the form $x_i \equiv a \mod m$ with only one value m.

Let T be a straight subspace of R of dimension 1. By Lemma 2.2.25, there exists $\boldsymbol{t}$ such that there is exactly one $i \in [d-1]$ such that $t_i = \mathrm{var}$, and there exists $\boldsymbol{c} \in \mathbb{N}^d$ such that $T = \mathrm{sub}(R;\boldsymbol{t},\boldsymbol{c})$. Then T is defined by the formula $\mathrm{sub}(R,\boldsymbol{t},\boldsymbol{c})(x)$ given in Notation 2.2.26.

Since x is the only variable, each occurrence of x in atomic formulas occurring in ψ is of the form $x \equiv k \mod m$ or $q \times x > p$ or $q \times x \doteq p$ or $q \times x < p$ with $k \in [m-1]$, $q \in \mathbb{N}^{>0}$, $p \in \mathbb{Z}$. Let $\phi'(x)$ be the formula obtained from $\phi(x)$ by replacing the atomic formulas $q \times x > p$ (respectively, $q \times x < p$, $q \times x \doteq p$) are rewritten as $x > \left\lfloor \frac{p}{q} \right\rfloor$ (respectively, $x < \left\lceil \frac{p}{q} \right\rceil$, $x \doteq \frac{p}{q}$ if q divides p and false otherwise). The formula $\phi'(x)$ is equivalent to $\phi(x)$ and belongs to $\mathsf{FO}[<,\mathrm{mod}\, m]$. □

Theorem 3.4.1 can now be proven.

Proof. The proof goes by induction on d. In the case of $d = 1$, there is no $\mathsf{FO}[+]$-definable set which is not $\mathsf{FO}[<,\mathrm{mod}]$-definable, hence the theorem trivially holds. Let us now assume that $d > 1$ and that it holds for $d-1$.

By Lemma 3.4.2, there exists $m \in \mathbb{N}^{>0}$ such that every straight subspace of dimension 1 of R is $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable.

Two cases must be considered, depending on whether all sections of R are $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable or not. Let us first assume that there is a section $S = \mathrm{sec}(R; x_i = c)$ for $i \in [d-1]$ and $c \in \mathbb{N}$ such that S is not $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable. Then by the induction hypothesis, there exists a $\Pi_2[<,+\mathbb{N},S]$-formula $\nu_S(x;y)$ which defines a non $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable unary function in $\mathcal{N}[S/\mathrm{sec}(R^{\mathcal{S}}; x_i = c)]$. Then let $\nu_{m,R}(x)$ be the $\Pi_2[<,+\mathbb{N},R]$-formula $\nu_S(x;y)$ where $S(x_0,\ldots,x_{i-1},x_{i+1},\ldots,x_{d-1})$ is replaced by $R(x_0,\ldots,x_{i-1},c,x_{i+1},\ldots,x_{d-1})$.

Let us now assume that all sections are $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable. Similarly to the last case, two cases must be considered, depending on whether all diagonals of R are $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable or not. If some diagonal is not $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable, the proof is similar to the case where a section is not $\mathsf{FO}[<,\mathrm{mod}\, m]$-definable.

Let us now assume that all sections and diagonals of $R^{\mathcal{S}}$ are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. Then there exists a permutation $\sigma \in \mathbb{S}_d$ such that $R^{\mathcal{S}} \cap \mathbb{N}^d_\sigma$ is not $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. For the sake of simplicity, let us assume that $\sigma = (0, \ldots, d-1)$ and let $R' = R^{\mathcal{S}} \cap \mathbb{N}^d_\sigma$.

By Lemma 3.3.5, the function $\tau_{R',m}$ is defined by a $\Pi_2[R', <, +\mathbb{N}]$-formula $\tau_{d,m}(N; x)$ which converges. To define $\nu_R(x; y)$, it suffices to replace in $\tau_{d,m}(N; x)$ the predicate $R'(\boldsymbol{x})$ by $R(\boldsymbol{x}) \wedge \bigwedge_{i=0}^{d-2} x_i < x_{i+1}$.

Since R is $\mathsf{FO}[+]$-definable, $\tau_{R',m}$ is $\mathsf{FO}[+]$-definable. Furthermore $\tau_{R',m}$ is increasing. Let r be its slope. The set R' is not $\mathsf{FO}[<, \mathrm{mod}]$-definable, thus $r > 1$ by Lemma 3.3.16. Hence $\nu_R(x; y)$ satisfies the conditions of the theorem. □

In the above theorem, R must be $\mathsf{FO}[+]$-definable because the proof of the theorem requires that there exists a positive integer m such that all straight subspaces of dimension 1 are $\mathsf{FO}[<, \mathrm{mod}\, m]$-definable. To the best of our knowledge, it is an open question to know whether a function f which is not $\mathsf{FO}[<, \mathrm{mod}]$-definable can be created for any R which is not $\mathsf{FO}[+]$-definable.

3.5 Conclusion

In this chapter, we have proven that the result [MV96, Theorem 5.1] can be improved, and that the $\mathsf{FO}[+, <, R]$-definition of a set of integers which is not $\mathsf{FO}[+, <]$-definable does not depend on a set R.

It is also proven that the logics $\mathsf{FO}[<, \mathrm{mod}]$ and $\mathsf{FO}[<, \mathrm{mod}\, m]$ admit some characterizations. In Theorem 3.4.1, it is assumed that the set R is $\mathsf{FO}[+, <]$-definable. A question which remains open is to figure out what simple set of functions can be defined when the assumption that R is $\mathsf{FO}[+, <]$-definable is removed.

This manuscript only consider relation over integers. Note that Theorem 3.2.5 does not directly hold for relation over reals. Indeed, it suffices to consider the following example:

Example 3.5.1. Let $R = \left\{ \frac{1}{n} \mid n \in \mathbb{N}^{>0} \right\}$. The set R of dimension 1 is ultimately periodic, but is not $\mathsf{FO}[+, <]$-definable.

However, methods developed in this chapter are currently adapted in order to give a characterization of the $\mathsf{FO}[+]$-definable sets over real or rationals numbers, using two properties, a local and a recursive one.

Notations used in Chapter 3

$\beta_d(\boldsymbol{x}, \boldsymbol{y}, k)$, 44

$\boldsymbol{c}(R^{\mathcal{S}}, s, t)$, 45
$C_R(\boldsymbol{x}, k)$, 44

$\gamma_d(s, t, k; \boldsymbol{c})$, 46

$\kappa_d(s; K)$, 46
$k(R^{\mathcal{S}}, s)$, 45

μ_d, 46

$\nu_d(x)$, 47

$\sigma_d(\boldsymbol{r}, k, \boldsymbol{x})$, 44
$\varsigma_d(s, k, \boldsymbol{x})$, 44

$\tau_d(t)$, 47
$\theta_{d,m}$, 56
$\text{thres}_m(S)$ for S a relation, 52

Chapter 4

Spectra of logics with successor and a unary function

This chapter deals with spectra of logical formulas. It is proven that some family of sets are $\exists\mathsf{MSO}[+1,\times b]$-spectra and are $\mathsf{FO}[+1,f]$-spectra where $b \geq 2$ and f is a uninterpreted unary function. The set considered in this sections are the b-recognizable sets and some encoding of halting computation of non-deterministic 2-counter automata. This chapter is independent of Chapter 3.

The notion of spectra is now introduced. The result about existential monadic second-order are given in Section 4.2. The results about first-order logic with an uninterpreted function are given in Section 4.3.

Contents

4.1 Introduction 69
4.1.1 Definitions 69
4.1.1.1 Example 70
4.1.1.2 Some properties about spectra 71
4.1.2 Non-deterministic 2-counter automata 72
4.2 Existential monadic second-order logic with arithmetic 74
4.2.1 b-recognizable sets are $\exists\mathsf{MSO}[+1,\times b]$-spectra 74
4.2.2 From spectra of non-deterministic 2-counter automata to $\exists\mathsf{MSO}^2[+1,\times b]$-spectra 76
4.3 First-order logic with successor and an uninterpreted function 81
4.3.1 Boolean combinations of b-recognizable sets are $\mathsf{FO}[+1,f]$-spectra 81
4.3.1.1 Examples 81
4.3.1.2 General case 85
4.3.2 From spectra of Non-deterministic 2-counter automata to $\mathsf{FO}[+1,f]$-spectra . . 90
4.3.3 Defining increasing functions in $\mathsf{FO}[+1,f]$ 90
4.4 Conclusion 92
Notations used in Chapter 4 93

4.1 Introduction

4.1.1 Definitions

Definition 4.1.1 (Spectra)**.** Let ϕ be a formula without free variable. Its spectrum $\mathsf{SP}(\phi)$ is the set of positive numbers n such that ϕ has a model of cardinality n. If $\mathcal{F}$ is a set of formulas then $\mathsf{SP}(\mathcal{F})$ is

defined as the set of spectra of formulas in the set $\mathcal{F}$.

A set $S \subseteq \mathbb{N}^{>0}$ is said to be a $\mathcal{L}[\mathcal{V}]$-spectrum if there exists a $\mathcal{L}[\mathcal{V}]$-formula ϕ such that $\mathsf{SP}(\phi) = S$.

Since the empty universe is not considered, the integer 0 does not belong to any spectrum.

4.1.1.1 Example

In this section, two examples of sets which are spectra are given.

Example 4.1.2. Let us show that $\left\{p^q \mid p \text{ prime }, q \in \mathbb{N}^{>0}\right\}$ is a spectrum of a first-order formula with two uninterpreted binary function symbols.

In order to define this set, field theory is used. Field theory axioms are first-order expressible, using two functions, one as addition, and one as multiplication. Indeed, it is well known that $(\mathbb{Z}/p\mathbb{Z})^q$ with p prime and $q \geq 1$ is a field and that all finite fields are isomorphic to a field $(\mathbb{Z}/p\mathbb{Z})^q$. Hence, all finite fields have cardinality p^q.

This allows to define $\left\{p^q \mid p \text{ prime}, q \in \mathbb{N}^{>0}\right\}$ as the spectrum of the following formula:

$$
\begin{array}{lll}
\exists 0, 1, \forall a, b, c. & 0 \neq 1 & \\
\wedge & a + 0 = a = 0 + a & (0 \text{ is neutral for } +) \\
\wedge & a + b = b + a & (+ \text{ is commutative}) \\
\wedge & a \times 1 = 1 = 1 \times a & (1 \text{ neutral for } \times) \\
\wedge & a \times (b + c) = a \times b + a \times c & (\text{distributive}) \\
\wedge & \exists d. a + d = 0 & (+ \text{ inverse}) \\
\wedge & (a + b) + c = a + (b + c) & (+ \text{ if associative}) \\
\wedge & \exists d. a \times d = 1 & (\times \text{ inverse}) \\
\wedge & (a \times b) \times c = a \times (b \times c) & (\times \text{ is associative})
\end{array}
$$

Example 4.1.3. The set of even integers is now defined as the spectrum of a first-order formula with an uninterpreted unary function symbol. The main idea is to partition the universe into pairs of elements $(e_0^i, e_1^i)_{i \in [n]}$ for $n \in \mathbb{N}^{>0}$. For this, it suffices to state that there exists a unary function f such that $f(e_0^i) = e_1^i$ and $f(e_1^i) = e_0^i$ for all $i \in [n]$, and since $e_0^i \neq e_1^i$, such that $f(x) \neq x$ for all x.

Hence $2\mathbb{N}$ is the spectrum of

$$\forall y. \{f(f(y)) = y \wedge f(y) \neq y\}.$$

When logics with function quantifiers are considered, it is possible to say that $2\mathbb{N}$ is the spectrum of a formula of this logic on the empty vocabulary. More precisely, $2\mathbb{N}$ is the spectrum of:

$$\exists f. \forall y. \{f(f(y)) = y \wedge f(y) \neq y\}.$$

Finally, let us consider spectra such that some symbols admit only one interpretation. For example, some symbols represent arithmetical relations and our universe is an initial segment of $\mathbb{N}$.

Example 4.1.4. In this example, the set $\{2^n + 1 \mid n \in \mathbb{N}\}$ is defined as the spectra of a $\exists\mathsf{MSO}[\times 2, +1]$-formula, that is, of a formula of existential monadic second order with the successor function and the multiplication by 2.

The main idea is to quantify an unary predicate P, which is interpreted by the set of powers of 2, and to state that the last element of the universe belongs to P. This leads to the following formula, whose spectrum is $\{2^n + 1 \mid n \in \mathbb{N}\}$:

$$\exists P. \forall x. \{P(x) \Longleftrightarrow [x \doteq 1 \vee (\exists y. y \times 2 \doteq x \wedge P(y))]\} \wedge P(\text{last}).$$

It is clear that the constant 1 and the last element of the universe, denoted by "last", are expressible in our logic and can be used in this formula.

The spectrum of this formula is then $\{2^n + 1 \mid n \in \mathbb{N}\}$. This set is 2-recognizable. More generally, it is shown in this part that b-recognizable sets, for $b \geq 2$, are spectra.

The preceding formula can be transformed into a formula over binary words, assuming that the ith letter is 1 if $P(i)$ holds, and 0 otherwise. This shows that the set $\{2^n + 1 \mid n \in \mathbb{N}\}$ is also a spectrum over first-order formulas over words.

More generally, existential monadic second order and first-order over words are similar.

4.1.1.2 Some properties about spectra

Four lemmas are given in this section. They help to create $\exists\mathsf{MSO}[+1,\mathcal{V}]$-spectra.

The following lemma states that there is no difference between existentially quantifying a formula and assuming that it belongs to the vocabulary.

Lemma 4.1.5. *Let ψ be a formula, then $\mathsf{SP}(\exists x.\psi) = \mathsf{SP}(\psi)$ and $\mathsf{SP}(\exists R.\psi) = \mathsf{SP}(\psi)$.*

The following lemma states that the set of spectra is closed by adding or removing finitely many integers.

Lemma 4.1.6. *Let $\mathcal{V}$ be a vocabulary which contains $+1$ and $\mathcal{L}[\mathcal{V}]$ be a logical fragment that contains $\Pi_2^2[\mathcal{V}]$. Let S be a spectrum of a $\mathcal{L}[\mathcal{V}]$-formula. Let F and F' be finite disjoint subsets of $\mathbb{N}^{>0}$. Then $(S \cup F) \setminus F'$ is a $\mathcal{L}[\mathcal{V}]$-spectrum.*

Proof. Assume that there exist formulas $\gamma_{n,\Pi} \in \Pi_2^2[+1]$ and $\gamma_{n,\Sigma} \in \Sigma_2^2[+1]$, which hold only on models of cardinality n. Let ϕ_S be the formula whose spectrum is S, then $(S \cup F) \setminus F'$ is the spectrum of:

$$\left(\phi_S \vee \bigvee_{n \in F} \gamma_{n,\Pi}\right) \wedge \bigwedge_{n \in F'} \neg\gamma_{n,\Sigma}.$$

The formulas $\gamma_{n,\Sigma}$ and $\gamma_{n,\Pi}$ must now be defined. Assume that there exist $\gamma_{\geq n,\Pi} \in \Pi_2[+1]$ and $\gamma_{\geq n,\Sigma} \in \Sigma_2[+1]$, which state that universe's cardinality is at least n. Then $\gamma_{n,\Pi}$ can be defined as $\gamma_{\geq n,\Pi} \wedge \neg\gamma_{\geq n+1,\Sigma}$ and $\gamma_{n,\Sigma}$ can be defined as $\gamma_{\geq n,\Sigma} \wedge \neg\gamma_{\geq n+1,\Pi}$.

The formulas $\gamma_{\geq n,\Sigma}$ and $\gamma_{\geq n,\Pi}$ must now be defined. Let $\gamma_{\geq n,\Sigma}$ be $\exists x.x \doteq n - 1$. Assume that there exists a $\Pi_2^2[+1, x]$ formula $suc_n(x)$ which asserts that $x + n \leq$ last. Then let $\gamma_{\geq n,\Pi}$ be $\forall x.x \doteq 0 \Longrightarrow suc_{n-1}(x)$.

Let us now define the formula $suc_n(x)$ by induction over n. This formula is similar to the formula of the proof of Lemma 2.2.14. For $n = 0$, $suc_0(x)$ is defined as the formula "True". For $n > 0$ let $suc_n(x)$ be

$$\{\exists y.x + 1 \doteq y\} \wedge \{\forall y.x + 1 \doteq y \wedge suc_{n-1}(y)\}.$$

□

The following lemma states that spectra are closed by union.

Lemma 4.1.7. *Let $\mathcal{V}$ be a vocabulary and $\mathcal{L}$ a logic. Let $S_0, \ldots, 1_{d-1}$ be a sequence of $\mathcal{L}[\mathcal{V}]$-spectra. Then $S = \bigcup_{i=0}^{d-1} S_i$ is a $\mathcal{L}[\mathcal{V}]$-spectrum.*

Proof. Let $\phi_i \in \mathcal{L}[\mathcal{V}]$ be such that $\mathsf{SP}(\phi_i) = S_i$. Let $\phi = \bigvee_{i=0}^{d-1} \phi_i$. Then $\mathsf{SP}(\phi) = S$. □

The following lemma proves that for any logic that contains the successor relation and Π_2^2, spectra are closed by addition of positive constants.

Lemma 4.1.8. *Let $\mathcal{V}$ be a vocabulary that contains $+1$ and let $\mathcal{L}[\mathcal{V}]$ be a logical fragment that contains $\Pi_2^2[\mathcal{V}]$. Let $S \subseteq \mathbb{N}^{>0}$ be a $\mathcal{L}[\mathcal{V}]$-spectrum. Let $a \in \mathbb{N}$. Then $S + a$ is a $\mathcal{L}[\mathcal{V}]$-spectrum.*

Proof. The result is proven for $a = 1$. The general case is proven by applying the base case a times.

The proof transforms a $\mathcal{V}$-structure $\mathcal{S}$ of cardinality n into a $\mathcal{V}$-structure $\mathcal{S}'$ of cardinality $n+1$ by adding an integer at the end of the structure.

Every quantification is replaced by a relativized quantification: it is ensured that the interpretation of quantified variables is restricted to [last -1]. Then, the last integer of the universe cannot be used.

Up to transforming the subformulas $\forall x.\xi$ into the equivalent formula $\neg\exists x.\neg\xi$, it is assumed that ϕ does not contains universal quantifiers. Let $\phi \in \mathcal{L}[\mathcal{V}]$, then let $\Phi(\phi)$ be the $\mathcal{L}[\mathcal{V}]$-formula obtained from ϕ by replacing each subformula of the form $\exists x.\psi$ by

$$\exists x.\{[\exists y.x+1 \doteq y] \wedge \Phi(\psi)\}.$$

and each subformula of the form $\exists R.\psi$ by

$$\exists R.\{\neg R(\text{last}) \wedge \Phi(\psi)\}.$$

Let ϕ be a $\mathcal{L}[\mathcal{V}]$-formula. By induction over ϕ, for each $n \in \mathbb{N}^{>0}$, $n \in \mathsf{SP}(\phi)$ if and only if $n+1 \in \mathsf{SP}(\Phi(\phi))$. Hence $\mathsf{SP}(\Phi(\phi))\setminus\{1\} = \mathsf{SP}(\phi)+1$. By Lemma 4.1.6, $\mathsf{SP}(\phi)+1$ is also a $\mathcal{L}[\mathcal{V}]$-spectrum. □

4.1.2 Non-deterministic 2-counter automata

The definition of a *non-deterministic 2-counter automaton* is briefly recalled, [Min60].

Definition 4.1.9 (Non-deterministic 2-counter automata)**.** A non-deterministic 2-counter automaton $\mathcal{A}$ consists of a list of instructions. Let $|\mathcal{A}|$ denote the number of instruction of $\mathcal{A}$. The instructions are "incr(h)", "decr(h)", "jmp(i,j)", "jz(h,j)" with $h \in \{0,1\}$, $i,j \in [|\mathcal{A}|-1]$ and "Halt". The j-th instruction is written $\mathcal{A}_j$. Without loss of generality, it is assumed that only one Halt instruction appears in the list and that it appears as the last instruction.

It is then explained how those automata compute.

Definition 4.1.10 (Configuration and Computation)**.** Let $\mathcal{A}$ be a 2-counter automaton. A *configuration* of $\mathcal{A}$ is a 3-tuple of integers (q,n_0,n_1) where q is the next instruction of the automaton and n_j is the value of the j-th counter.

Let (κ,c_0,c_1) be a triplet of lists of the same length l, such that for all $i \in [l-1]$, $(\kappa[i],c_0[i],c_1[i])$ is a configuration. This triplet is a *computation of* $\mathcal{A}$ if the first configuration satisfies $c_0[0] = c_1[0] = \kappa[0] = 0$, the last configuration satisfies $\kappa[l-1] = (|\mathcal{A}|-1)$, and for every $j \in [l-2]$ such that $\mathcal{A}_{\kappa[j]} \neq$ Halt – that is $\kappa[j] < |\mathcal{A}|-1$ – one has :

$$\begin{array}{lllll}
\text{if } \mathcal{A}_{\kappa[j]} = incr\ (i) & \text{then } c_i[j+1] = c_i[j]+1, & c_{1-i}[j+1] = & c_{1-i}[j], & \\
& \text{and } \kappa[j+1] = \kappa[j]+1, & & & \\
\text{if } \mathcal{A}_{\kappa[j]} = decr\ (i) & \text{then } c_i[j+1] = \max(c_i[j]-1,0), & c_{1-i}[j+1] = & c_{1-i}[j], & \\
& \text{and } \kappa[j+1] = \kappa[j]+1, & & & \\
\text{if } \mathcal{A}_{\kappa[j]} = jmp\ (n,m) & \text{then } c_0[j+1] = c_0[j], & c_1[j+1] = & c_1[j] & \\
& \text{and } \kappa[j+1] \in \{n,m\}, & & & \\
\text{if } \mathcal{A}_{\kappa[j]} = jz\ \ (i,m) & \text{then } c_0[j+1] = c_0[j], & c_1[j+1] = & c_1[j] & \\
\text{and, if } c_i[j] = 0 & \text{then } \kappa[j+1] = m & \text{and otherwise } \kappa[j+1] & = \kappa[j]+1. &
\end{array}$$

It should be noted that those automata do not have any input.

The notion of spectra is extended to 2 counter automata.

Definition 4.1.11 ($\mathsf{SP}(\mathcal{A})$)**.** Let $\mathcal{A}$ be a non-deterministic 2-counter automaton. Then $\mathsf{SP}(\mathcal{A}) \subseteq \mathbb{N}$ is defined as the set of integers n such that $n \in \mathsf{SP}(\mathcal{A})$ if there is a computation of $\mathcal{A}$ with n steps.

An example of a non-deterministic 2-counter automaton whose spectrum is not ultimately periodic is now given. This example is useful for the proof of the strict inclusion of b-recognizable sets in $\mathsf{SP}(\exists\mathsf{MSO}[+1,\times b])$ (see Corollary 4.2.11.)

Example 4.1.12. Let $\mathcal{A}$ be the automaton which implements Algorithm 1. Formally, it is

(0) $incr(0)$ (1) $jmp(0,2)$ (2) $decr(0)$ (3) $incr(1)$ (4) $jz(0,2)$ (5) $decr(1)$ (6) $incr(0)$
(7) $jz(1,5)$ (8) $decr(0)$ (9) $jz(0,2)$ (10) $Halt$

This algorithm non-deterministically chooses a positive integer n in the first counter. It transfers the first counter to the second one, then it transfers back the second counter to the first one, and decrements the first counter. It repeats until the first counter equals 0.

Let us prove that $\mathsf{SP}(\mathcal{A}) = \{7n + 3n^2 + 1 \mid n \in \mathbb{N}^{>0}\}$.

Algorithm 1: Example 4.1.12

```
   repeat
 0 |  incr(0)
 1 until non-deterministically chooses when to end; //jmp[0,2]
   repeat
   |  repeat
 2 |  |  decr(0)
 3 |  |  ncr(1)
 4 |  until c0 = 0; //jz[0,2]
   |  repeat
 5 |  |  decr(1)
 6 |  |  incr(0)
 7 |  until c1 = 0; //jz[1,5]
 8 |  decr(0)
 9 until c0 = 0; //jz[0,2]
10 halt
```

An halting computation of this automaton is now studied. The loop of Line 1 is executed n times, for an arbitrary $n \in \mathbb{N}^{>0}$. Each execution of the loop costs 2 steps, hence the entire loops costs $2n$ steps. At the ends of the loops, $c_0 = n$ and $c_1 = 0$.

The outer loop of line 9 is executed n times, the loop variant is that at the end of the i-th execution, $c_0 = n - i$ and $c_1 = 0$. During the ith execution of the outer loop, the first inner loop, at line 4 is repeated $n - i$ times. The loop variant is such that after the jth execution, $c_0 = n - i - j$ and $c_1 = j$. Each execution costs 3 steps, hence the first inner loop costs $3j$ steps. The second inner loop is identical to the first one, with c_0 and c_1 exchanged. Finally the instruction of line 8 decrements the counter 0. Hence the ith execution of the outer loop costs $6(n - i) + 2$ steps. Finally, the Halt instruction costs one step.

Finally, the number of steps of the execution is:

$$2n + \sum_{i=0}^{n-1}[6(n-i)+2] + 1 = 2n + 6\sum_{i=1}^{n} i + 2n + 1 = 4n + 6\frac{n(n+1)}{2} + 1 = 7n + 3n^2 + 1$$

Hence $\mathsf{SP}(\mathcal{A}) = \left\{7n + 3n^2 + 1 \mid n \in \mathbb{N}^{>0}\right\}$.

4.2 Existential monadic second-order logic with arithmetic

Theorems about existential monadic logic with arithmetic relations are proven in this section. More precisely, the logic $\exists\mathsf{MSO}\Pi_2^2[+1,\times b]$ for $b \geq 2$ and $\exists\mathsf{MSO}\Pi_2^2[+1,g]$ for some increasing functions g are now considered.

Section 4.2.1 deals with spectra which are b-recognizable. Then Section 4.2.2 deals with spectra which encode spectra of some non-deterministic 2-counter automaton.

4.2.1 b-recognizable sets are $\exists\mathsf{MSO}[+1,\times b]$-spectra

In this section, it is shown how to represent b-recognizable sets as $\exists\mathsf{MSO}^2[+1,\times b]$-spectra and also as $\forall\mathsf{MSO}^2[+1,\times b]$-spectra.

Theorem 4.2.1. *The following inclusion holds:*

$$b - REC \subseteq \mathsf{SP}\Big(\exists\mathsf{MSO}\Pi_2^2[+1,\times b]\Big).$$

Actually Corollary 4.2.11 states that this inclusion is strict.

To prove this theorem, the following Lemma is needed.

Lemma 4.2.2. *Let $\mathcal{A}$ be an automaton in base b in dimension 1 as in Definition 2.3.6. There exists a $\exists\mathsf{MSO}\Pi_2^2[+1,\times b]$-formula $\phi_{\mathcal{A}}$ which holds on $[n]$ if and only if n is accepted by $\mathcal{A}$.*

Note that $\mathsf{SP}(\phi_{\mathcal{A}}) = \overline{\mathcal{A}}^{\mathbb{N}} + 1$, indeed, the cardinality of $[n]$ is $n+1$. Let us first give an example to illustrate the lemma.

Example 4.2.3. Let $\mathcal{A}$ be the automaton of Figure 4.1. It accepts the language 0^*10^*, hence the set of integers $\{2^i \mid i \in \mathbb{N}\}$.

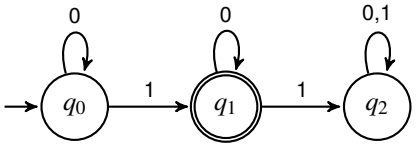


Figure 4.1: Automaton accepting $\{2^i \mid i \in \mathbb{N}\}$

This set is defined by:

$$\exists R.\forall x.\{R(x) \Longleftrightarrow [x \doteq \text{last} \vee R(2x)]\} \wedge R(1). \tag{4.1}$$

This formula holds for the structures $\mathcal{S}$ over the universe $[2^c]$ for $c \in \mathbb{N}$ when the variable R is interpreted by $\{2^i \mid i \in [c]\}$. Intuitively, R is interpreted by the set of integers n such that $\delta(q_0, \underline{n}_b) \in F$.

Lemma 4.2.2 is now proven.

Proof. For $b \in \mathbb{N}$, let $\mathcal{V}_{b,Q}$ be the vocabulary $\{+1, \times b, \left(R_q\right)_{q\in Q}\}$ where each R_q is a unary relation for any state $q \in Q$. Let $n \in \overline{\mathcal{A}}^{\mathbb{N}}$. A $\mathcal{V}_{b,Q}$-structure $\mathcal{S}_n$ is now defined. This structure encodes the computation of $\mathcal{A}$ on the input $w = \underline{n}_b$ of length l. The main idea of the proof is to choose a sequence of integers $c_{n,0}, \ldots, c_{n,l}$ such that $R_q(c_{n,i})$ holds if and only if the ith state of the computation is q. Then the automaton $\mathcal{A}$ accepts w if and only if:

- $R_{q_0}(c_{n,0})$,

- $R_q(c_{n,i})$ implies $R_{\delta(q,w[i])}(c_{n,i+1})$ and
- $R_q(c_{n,l})$ for some $q \in F$.

The precise values for the $c_{n,i}$'s are now given.

For $i \in [l]$, let $w[\geq i]$ be the suffix of w of length $l - i$, that is, w without its i first letters. It is the part of the word that remains to be read after the ith step of the computation of $\mathcal{A}$. Then let $c_{n,i}$ be $\overline{w[\geq i]}^{\mathbb{N}}$. It implies that $c_{n,i+1} = \frac{c_{n,i} - w[i]}{b}$ and $w[i] = c_{n,i} \mod b$. hence, by an easy induction over i, $c_{n,i} = \left\lfloor \frac{n}{b^i} \right\rfloor$, and in particular $c_{n,0} = n$ and $c_{n,l} = 0$.

Similarly, let q_i be the ith step of the computation of the automaton. That is, for all $i < l$:

$$q_{i+1} = \delta(q_i, w[i]) = \delta(q_i, c_{n,i} \mod b).$$

For all $q \in Q$, let $R_q^{\mathcal{S}}$ be $\{c_{n,i} \mid q_i = q\}$. The sets $R_q^{\mathcal{S}}$ can be defined by induction over i as follows: $n \in R_{q_0}^{\mathcal{S}}$ and, for all $c_{n,i} \in R_q^{\mathcal{S}}$, if $c_{n,i} \equiv a \mod b$ then $c_{n,i+1} = \frac{n-a}{b} \in R_{\delta(q,a)}$.

Formally, the formula ψ_δ is introduced. This formula states that two consecutive states encode a correct step of the computation. If x is interpreted by $c_{n,i+1}$ and q by q_i then the formula holds only if a is interpreted by $w[i]$ and $b \times x + a$ by $c_{n,i}$. Hence ψ_δ asserts that $R_{q_i}(c_{n,i})$ implies that $R_{\delta(q_i,w[i])}(c_{n,i+1})$:

$$\psi_\delta = (\forall x. x \neq 0) \bigwedge_{q \in Q} \bigwedge_{a=0}^{b-1} R_q(b \times x + a) \Longrightarrow R_{\delta(q,a)}(x).$$

It must be ensured that $c_{n,0}$ corresponds to an initial state and $c_{n,l}$ corresponds to an accepting state. This can be expressed by the formula $\psi_{0,F}$:

$$\psi_{0,F} = R_{q_0}(\text{last}) \wedge \bigvee_{q \in F} R_q(0).$$

Finally, let ψ_Q be the formula that states that there is at most one state by letter.

$$\psi_Q = \forall x. \bigwedge_{q \neq q' \in Q} \neg\Big[R_q(x) \wedge R_{q'}(x)\Big].$$

The three formulas ψ_δ, $\psi_{0,F}$ and ψ_Q belong to $\Pi_2[+1, \times b, \left(R_q\right)_{q \in Q}]$. Hence their conjunction $\psi = \psi_\delta \wedge \psi_{0,F} \wedge \psi_Q$ also belongs to $\Pi_2[+1, \times b, \left(R_q\right)_{q \in Q}]$. And by construction $\mathsf{SP}(\psi) = \overline{\mathcal{A}}^{\mathbb{N}}$. □

Example 4.2.3 is now resumed.

Example 4.2.4. For the set $\{2^i \mid i \in \mathbb{N}\}$, the formula ψ is:

$$\begin{array}{l}
\exists R_{q_0}, R_{q_1}, R_{q_2}. \wedge R_{q_0}(\text{last}) \wedge R_{q_1}(0) \wedge (\forall x. x \neq 0)\{ \\
R_{q_0}(2 \times x) \Longrightarrow R_{q_0}(x) \wedge R_{q_0}(2 \times x + 1) \Longrightarrow R_{q_1}(x) \wedge \\
R_{q_1}(2 \times x) \Longrightarrow R_{q_2}(x) \wedge R_{q_1}(2 \times x + 1) \Longrightarrow R_{q_2}(x) \wedge \\
R_{q_2}(2 \times x) \Longrightarrow R_{q_2}(x) \wedge R_{q_2}(2 \times x + 1) \Longrightarrow R_{q_2}(x)\} \wedge \\
\forall x. \Big\{\neg\Big[R_{q_0}(x) \wedge R_{q_1}(x)\Big] \wedge \neg\Big[R_{q_0}(x) \wedge R_{q_2}(x)\Big] \wedge \neg\Big[R_{q_2}(x) \wedge R_{q_1}(x)\Big]\Big\}.
\end{array}$$

Theorem 4.2.1 is now proven.

Proof. Let $S \subseteq \mathbb{N}^{>0}$ be a b-recognizable set. By Lemma 4.2.2, it suffices to prove that $S-1$ is accepted by an automaton in base b. Since $S \in b-\mathrm{REC}$, by Theorem 2.3.5, there exists a $\mathsf{FO}[+,V_b]$-formula $\sigma(x)$ that defines S (in $\mathbb{N}$). Then $\sigma(x+1)$ defines $S-1$. Hence $S-1$ is also b-recognizable. By definition of b-recognizable sets, there exists a deterministic automaton $\mathcal{A} = (Q,[b-1],\delta,q_0,F)$ that accepts $\underline{S-1}_b$. □

Example 4.2.5 is now resumed.

Example 4.2.5. Let $S = \{2^i + 1 \mid i \in \mathbb{N}\}$, then $S-1 = \{2^i \mid i \in \mathbb{N}\}$ and S is the spectra of Formula (4.1) of Example 4.2.3.

Theorem 4.2.1 admits the following corollary.

Corollary 4.2.6. *The following inclusion holds:*

$$b-REC \subseteq \mathsf{SP}\Big(\forall\mathsf{MSO}\Sigma_2^2[+1,\times b]\Big).$$

Proof. Let $S \subseteq \mathbb{N}^{>0}$ be a b-recognizable set. The set $\mathbb{N}^{>0} \setminus S$ is also $\mathsf{FO}[+,V_b]$-definable. Hence $\mathbb{N}^{>0} \setminus S$ is b-recognizable. By Theorem 4.2.1, there exists $\psi \in \exists\mathsf{MSO}\Pi_2^2[+1,\times b]$ such that $\psi^{\mathbb{N}} = \mathbb{N}^{>0} \setminus S$. Then $\mathsf{SP}(\neg\psi) = S$ and $\neg\psi \in \forall\mathsf{MSO}\Sigma_2^2[+1,\times b]$. □

It should be noted that, in general, $\mathsf{SP}(\neg\phi)$ is not equal to $\mathbb{N}^{>0} \setminus \mathsf{SP}(\phi)$. In our context, the equality holds because the vocabulary contains only interpreted symbols.

As a corollary of Theorem 4.2.1, the same result is proven over words.

Corollary 4.2.7. *The class $b-REC$ is a subset of the set of $\Pi_2^2[+1,\times b]$-spectra over words over some alphabet.*

That is, $b-\mathrm{REC}$ is a subset of the $\mathsf{FO}^2[+1,\times b]$-spectra.

Proof. Let $S \subseteq \mathbb{N}^{>0}$ be a b-recognizable set. By Theorem 4.2.1 there exists $\phi \in \exists\mathsf{MSO}\Pi_2^2[+1,\times b]$ such that $\mathsf{SP}(\phi) = S$. By construction ϕ is of the form $\exists R_0,\ldots,R_{d-1}.\psi$ with $\psi \in \Pi_2^2[+1,\times b,R_0,\ldots,R_{d-1}]$. By Lemma 4.1.5, $\mathsf{SP}(\psi) = S$.

Let us define the alphabet A as the set of subsets of $[d-1]$. Let ψ' be obtained from ψ by replacing each atomic formula of the form $R_i(t)$ by $\bigvee_{\substack{I \subseteq [d-1] \\ i \in I}} P_I(t)$. Let us prove that $\mathsf{SP}(\psi') = \mathsf{SP}(\psi)$, that is, $\mathsf{SP}(\psi') = S$.

- Assume first that $n \in \mathsf{SP}(\phi)$, then there exists a $\{+1,\times b,(R_i)_{i\in[d-1]}\}$-model $\mathcal{S}$ of ψ. The word $w_{\mathcal{S}}$ of length n with $w_{\mathcal{S}}[j] = \{i \in [d-1] \mid S \models R_i(j)\}$ is clearly a model of ψ'. Hence $n \in \mathsf{SP}(\psi')$.
- Conversely, let $w \in A^0$ be a model of length n of ψ'. Let $\mathcal{S}$ be the $\{[n-1],+1,\times b,(R_i)_{i\in[d-1]}\}$-structure such that $R_i^{\mathcal{S}} = \{j \in [n-1] \mid i \in w[j]\}$. Then $\mathcal{S}$ is a model of ψ, hence $n \in \mathsf{SP}(\phi)$.

□

4.2.2 From spectra of non-deterministic 2-counter automata to $\exists\mathsf{MSO}^2[+1,\times b]$-spectra

This section considers spectra of non-deterministic 2-counter automata, that is, sets of possible halting times of such automata. Those spectra are encoded as $\exists\mathsf{MSO}^2[+1,\times b]$-spectra. More generally, they are encoded as $\exists\mathsf{MSO}^2[+1,g]$ for a class of unary functions g which contains $\times b$ for $b \geq 2$.

In this section, a non-deterministic 2-counter automaton is encoded as a $\{+1, g\}$-structure for g belonging to a large class $\mathbb{I}$ of functions. This implies that the satisfiability problem of this logic is undecidable for any function $g \in \mathbb{I}$.

The following definition introduces the class $\mathbb{I}$ of functions g and some related notations.

Definition 4.2.8. Let $\mathbb{I}$ be the set of increasing functions $g : \mathbb{N} \to \mathbb{N}$ such that $g(1) > 1$ and such that the image of g is not co-finite - that is, for each $n \in \mathbb{N}$, there is $s > n$ such that $g(s+1) > g(s) + 1$.

Let $g \in \mathbb{I}$. Let $\cong^g$ be the equivalence relation such that $n_0 \cong^g n_1$ if and only if $(g^i(n_0) = n_1$ or $g^i(n_1) = n_0)$ for some $i \in \mathbb{N}$, where g^i denotes the function g applied i times.

Then let $E^g(n)$ be the equivalence class of n and $e^g(n)$ be the least integer of $E^g(n)$.

Let $\left(s_n^g\right)_{n\in\mathbb{N}}$ and $\left(p_n^g\right)_{n\in\mathbb{N}}$ be two sequences defined recursively by:

- $s_0^g = 1$.
- for all $i \in \mathbb{N}$ such that s_i^g is defined:
  - p_i^g is the least integer, greater than s_i^g, which has no antecedent by g. Formally:

$$p_i^g = \min\left\{n \in \mathbb{N} \mid n > s_i^g, \neg\exists m.g(m) = n\right\}.$$

  - s_{i+1}^g is the least integer of $E^g(1)$ greatest than p_i^g. Formally

$$s_{i+1}^g = \min\left\{n \in \mathbb{N} \mid n > p_i^g, e^g(n) = 1\right\}.$$

Some examples of functions g's as in the preceding definition are now given.

Example 4.2.9.

- Let g denote the function $\times b$ for $b \geq 3$. The function g belongs to $\mathbb{I}$. One has $e^g(n) = \frac{n}{V_b(n)}$, and the equivalence classes have the form $\{p \times b^n \mid n \in \mathbb{N}\}$ where b does not divide p. Moreover $s_n^g = b^n$ and finally $p_n^g = b^n + 1$.

  The case $b = 2$ is almost identical, except that $s_n^g = 2^{n+1}$ for $n \in \mathbb{N}^{>0}$ and $p_n^g = 2^{n+1} + 1$ for $n \in \mathbb{N}$. The following array gives the first values for $g(n) = 2 \times n$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$g(n)$	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
$e^g(n)$	1	1	3	1	5	3	7	1	9	5	11	3	13	7	15	1	17	9	19	5
	s_0^g		p_0^g	s_1^g	p_1^g			s_2^g	p_2^g							s_3^g	p_3^g			

- Now let $g(n) = n + \left\lfloor \sqrt{n} \right\rfloor$. The first values for this function are:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$g(n)$	2	3	4	6	7	8	9	10	12	13	14	15	16	17	18	20	21	22	23	24
$e^g(n)$	1	1	1	1	5	1	5	1	5	1	11	5	1	11	5	1	11	5	19	1
	s_0^g				p_0^g	s_1^g					p_1^g		s_2^g						p_2^g	s_3^g

  Then the $\cong^g$-classes are $\{0\}$, $\{1,2,3,4,6,8,10,13,16,20,\dots\}$, $\{5,7,9,12,15,18,\dots\}$, $\{11,14,17,\dots\}$, $\{19,\dots\}$, $\dots$. The sequence $\left(p_n^g\right)$ begins by: $(5,11,19,\dots)$ (which is actually equal to $\{n^2+n-1 \mid n \in \mathbb{N}\}$), and the sequence $\left(s_n^g\right)$ begins by $(1,6,10,20,\dots)$.

A relation is now given, between spectra over non-deterministic 2-counter automata and spectra over formulas.

Theorem 4.2.10. *For each non-deterministic 2-counter automaton $\mathcal{A}$, there exists a formula $\phi_{\mathcal{A}} \in \exists\mathsf{MSO}\Pi^2_2[+1, g]$ such that if $g \in \mathbb{I}$ then $\mathsf{SP}(\phi_{\mathcal{A}}) = \{s^g_t + 1 \mid t \in \mathsf{SP}(\mathcal{A})\}$.*

Proof. A computation (κ, c_0, c_1) of a non-deterministic 2-counter automaton $\mathcal{A}$ is encoded with a formula $\phi_{\mathcal{A}}$ in $\exists\mathsf{MSO}\Pi^2_2[+1, g]$ such that $[s^g_t] \models \phi_{\mathcal{A}}$ if and only if $\mathcal{A}$ admits a computation that halts in t steps.

The formula $\phi_{\mathcal{A}}$ will be the conjunction of several formulas which are defined below.

Let us assume that the computation halts after t steps, our finite structure of universe $[s^g_t]$ is then divided in t segments. The ith segment $S_i = [s^g_i, s^g_{i+1} - 1]$ encodes the ith step of the computation.

More precisely, monadic second order variables are used:

- The variable S stands for the set of s^g_i's.
- The variable C_j encodes the jth counter. More precisely, in a segment S_i, a $\cong^g$-class E is either entirely contained in C_j or disjoint from C_j, namely $E \cap S_i \cap C_j \in \{\emptyset, E \cap S_i\}$. And the number of $\cong^g$-classes that intersect $S_i \cap C_j$ is equal to $c_j[i]$. Formally, $|\left\{E^g(n) \mid n \in S_i \cap C_j\right\}| = c_j[i]$.
- The variables $\left(Q_q\right)_{q \in [|\mathcal{A}|-1]}$ stand for the instruction number, that is: Q_q is true on the (whole) segment S_i if and only if $\kappa[i] = q$. In particular, there exists one and only one state by segment, the first state is 0 and the last is $|\mathcal{A}| - 1$. This can be expressed by the formula:

$$\begin{aligned}\phi_Q = \quad & Q_0(1) \wedge Q_{|\mathcal{A}|-1}(\text{last}) \wedge \forall x \neq 0. \\ & \bigvee_{q=0}^{|\mathcal{A}|-1} \Big\{ Q_q(x) \wedge \bigwedge_{q,q' \in Q, |q \neq q'} \neg Q_{q'}(x) \wedge \Big[S(x+1) \vee Q_q(x+1) \Big] \Big\}.\end{aligned}$$

The set S, the counters C_j and the states Q_q cannot be directly defined. Hence auxiliary second order variables are introduced. The intended interpretation of those variables and their formal definitions are then given. Finally, S, C_0, C_1 and the Q_q's are defined using those auxiliary variables.

Defining S The set S cannot be defined directly, since its definition use the order relation, $E^g(1)$ and the sequence $\left(p^g_n\right)$. Hence the following second order variables are used:

- The variable E stands for $E^g(1)$; formally n belongs to E if $n = 1$ or if there exists $n' \in \mathbb{N}$ such that $n' \in E$ and $g(n') = n$. Formally it is characterized by:

$$\phi_E = \forall x. E(x) \Longleftrightarrow \{x \doteq 1 \vee [x \neq 1 \wedge (\exists y. g(y) \doteq x \wedge E(y))]\}.$$

- The variable P stands for the union of the $[s^g_i, p^g_i - 1]$. Formally it is characterized by:

$$\phi_P = \forall x. P(x) \Longleftrightarrow \{E(x) \vee [x \neq 0 \wedge P(x-1) \wedge \exists y. g(y) \doteq x]\}.$$

- Finally S can be characterized by the set of letters of E whose predecessor does not belong to P:

$$\phi_S = \forall x. \{S(x) \Longleftrightarrow [E(x) \wedge \neg P(x-1)]\}.$$

Since it is required that the cardinality of the structure has the form $s^g_t + 1$, it is imposed that last $\in S$. Let

$$\phi_{\text{last}} = S(\text{last}).$$

Counters The main issue with this encoding concerning the counters is that, in order to ensure that two successive segments encode two successive configurations, the cardinality of two sets must be compared. And comparing cardinality does not seem possible in our logic. To overcome this, the properties of the function g are used. If the ith step is a jump or a jz instruction, then $c_j[i] = c_j[i+1]$, and in this case C_j can be chosed in S_{i+1} to be $\{n \in S_{i+1} \mid \exists m \in C_j.g(m) = n\}$. If the ith step is $incr(j)$ then it suffices to add a single position to C_j in S_{i+1}. Such a position exists by construction, and equals p^g_{i+1}. It is a single position since p^g_{i+1} has an antecedent and $g(p^g_{i+1})$ belongs to S_{i+2}. Finally, if the ith step is $decr(j)$ then it suffices to remove the least integer of the image of C_j which belongs to S_i.

More formally:

- If the ith step is $incr(j)$, that is $\kappa[i] = q$ with $\mathcal{A}_q = incr(j)$ and $Q_q\left(s^g_i\right)$, then:
  - $C_j\left(p^g_{i+1}\right)$,
  - $C_{1-j}\left(p^g_{i+1}\right)$ does not hold, and
  - for every $n \in \left[s^g_{i+1}, s^g_{i+2} - 1\right] \setminus \left\{p^g_{i+1}\right\}$, for $k \in \{0,1\}$, the property $C_k(n)$ holds if and only if there exists n' with $g(n') = n$ and $C_j(n')$ holds.

  A new second order variable R^+_j states that the jth counter should be incremented. It is true on $[s^g_{i+1}, p^g_{i+1} - 1]$:

  $$\phi_{R^+_j,q} = \forall x.R^+_j(x) \Longleftrightarrow \left\{[S(x) \wedge Q_q(x-1)] \vee \left[\exists y.g(y) = x \wedge R^+_j(x-1)\right]\right\}$$

  It should be noted that the formula is correct because $p^g_{i+1} > s^g_{i+1}$.

- If the ith step is $decr(j)$, let r be the least integer of S_i such that $C_j(r)$ holds if it exists, and be s^g_{i+1} otherwise. Then:
  - for every $n \in \left[s^g_{i+1}, s^g_{i+2} - 1\right]$, $C_j(n)$ holds if and only if there exists n' with $g(n') = n$ such that $C_j(n')$ holds and $n \neq r$.
  - for every $n \in \left[s^g_{i+1}, s^g_{i+2} - 1\right]$, $C_{1-j}(n)$ holds if and only if there exists n' with $g(n') = n$ such that $C_{1-j}(n')$ holds.

  The value of r must now be defined: for this, a new second order variable R^-_j is introduced, this variable holds only for integers of the segment $\left[s^g_{i+1}, r - 1\right]$:

  $$\begin{aligned}\phi_{R^-_j,q} = \quad & \forall x.R^-_j(x) \Longleftrightarrow \\ & \left\{\left[S(x) \wedge Q_q(x-1)\right] \vee \left[\neg S(x) \wedge R^-_j(x-1) \wedge \neg(\exists y.g(y) \doteq x \wedge C_i(y))\right]\right\}.\end{aligned}$$

- In every other case, $n \in \left[s^g_{i+1}, s^g_{i+2} - 1\right]$, $C_j(n)$ holds if and only if there exists n' with $g(n') = n$ and $C_j(n')$ holds.

The C_j are finally defined by

$$\begin{aligned}\phi_{C_j} = \quad & \forall x.C_j(x) \Longleftrightarrow \\ & \left\{\left[R^+_j(x-1) \wedge \neg\exists y.g(y) = x\right] \vee \left[\neg R^-_j(x-1) \wedge \exists y.g(y) \doteq x \wedge C_j(y)\right]\right\}\end{aligned}$$

Let us prove that $C_k(n)$ does not hold for any $n \in E^g(1)$. Let (*) denote this statement. For the sake of contradiction, let $n \cong^g 1$ be the least integer such that $C_k(n)$ holds. If $n = 1$, the property (*) does not hold since $c_k[0] = 0$. If $n > 1$ then either $n = p^g_i$ or there exists n' such that $g(n') = n$ and $C_k(n')$. The first case is impossible since $p^g_i \not\cong^g 1$ by definition on p^g_i, and the second case contradicts the minimality of n.

States Finally, the formula states that the different states appear in the correct order. The formula ϕ_Q already states that the initial state is 0 and that the last state is $|\mathcal{A}| - 1$. It remains to encode that two successive segments encode a step of the computation.

Let $i \in [t-1]$ be a step, such that at the ith step of the computation the state of the automaton is q.

- If $\mathcal{A}_q = jmp(q_0, q_1)$, then either $Q_{q_0}\left(s^g_{i+1}\right)$ or $Q_{q_1}\left(s^g_{i+1}\right)$. This transition can be defined by:

$$\phi_q = \forall x. \Big[S(x) \wedge Q_q(x-1)\Big] \Longrightarrow \Big\{Q_{q_0}(x) \vee Q_{q_1}(x)\Big\}.$$

- If $\mathcal{A}_q = jz(j, q')$, then if there exists a position $z_{i,j} \in \left[s^g_i, s^g_{i+1} - 1\right]$ such that $C_j\left(z_{i,j}\right)$ then $Q_{q+1}(s^g_{i+1})$, otherwise $Q_{q'}(s^g_{i+1})$.

  This condition cannot be stated directly, as it uses the order relation. Hence an auxiliary variable Z_j determines whether the value of the jth counter equals 0 or not in the segment. More precisely, Z_j is such that $Z_j \cap S_i = \left[s^g_i, z_{i,j} - 1\right]$ for the minimal value of $z_{i,j}$, if such a value exists, and $Z_j \cap S_i = S_i$ otherwise. Formally:

$$\phi_{Z_j} = \forall x. Z_j(x) \Longleftrightarrow \{S(x) \vee \Big[Z_j(x-1) \wedge \neg C_j(x)\Big]\}.$$

  Then the transition can be defined by:

$$\phi_q = \forall x. \Big[S(x) \wedge Q_q(x-1)\Big] \Longrightarrow \Big\{\Big[Z_j(x-1) \wedge Q_{q'}(x)\Big] \vee \Big[\neg Z_j(x-1) \wedge Q_{q+1}(x)\Big]\Big\}$$

- If $\mathcal{A}_q = incr(j)$ or $decr(j)$, that is $Q_q\left(s^g_i\right)$ with $\kappa(q)$ being $incr(j)$ or $decr(j)$, then $Q_{q+1}\left(s^g_{i+1}\right)$.

$$\phi_q = \forall x. \Big[S(x) \wedge Q_q(x-1)\Big] \Longrightarrow Q_{q+1}(x)$$

Finally $\phi_{\mathcal{A}}$ is defined by the $\exists \mathsf{MSO}\Pi_2[+1, g]$-formula:

$$\begin{aligned}\exists C_0, C_1, R_0^+, R_1^+, R_0^-, R_1^-, Z_0, Z_1, E, S, P, \left(Q_q\right)_{q \in [|\mathcal{A}|-1]}. \phi_Q \wedge \phi_{\text{last}} \wedge \\ \left(\bigwedge_{q \in [|\mathcal{A}|-1]} \phi_q\right) \wedge \phi_E \wedge \phi_P \wedge \phi_S \wedge \Big[\phi_{C_j} \wedge \phi_{Z_j} \wedge \\ \bigwedge_{j=0}^{1} \left(\bigwedge_{\mathcal{A}_{[q]} = incr(j)} \phi_{R_j^+, q}\right) \wedge \left(\bigwedge_{\mathcal{A}_{[q]} = decr(j)} \phi_{R_j^-, q}\right)\Big].\end{aligned}$$

An incrementation step is represented in Figure 4.2. □

Combining the above theorem with Lemma 5.1.1 yields the following corollary.

Corollary 4.2.11. *The class $b-REC$ is a strict subset of* $\mathsf{SP}\left(\exists \mathsf{MSO}\Pi_2^2[+1, \times b]\right)$.

Proof. The inclusion is proven in Theorem 4.2.1. Let us prove the strictness, that is

$$\mathsf{SP}\left(\exists \mathsf{MSO}\Pi_2^2[+1, \times b]\right) \not\subseteq b - \text{REC}.$$

Theorem 4.2.10 is used with $g(n) = b \times n$. This function is studied in Example 4.2.9. If $\mathcal{A}$ is a non-deterministic 2-counter automaton whose spectrum is S, then the spectrum of $\phi_{\mathcal{A}}$ is $\{b^n + 1 \mid n \in S\}$. Hence $\underline{\mathsf{SP}(\phi_{\mathcal{A}})}_b$ is equal to $\left\{10^{n-1}1 \mid n \in S\right\}$. Thus $\mathsf{SP}(\phi_{\mathcal{A}})$ is b-recognizable if and only if S is ultimately periodic. Now, by Example 4.1.12, there exists a non-deterministic 2-counter automaton whose spectra is not ultimately periodic. □

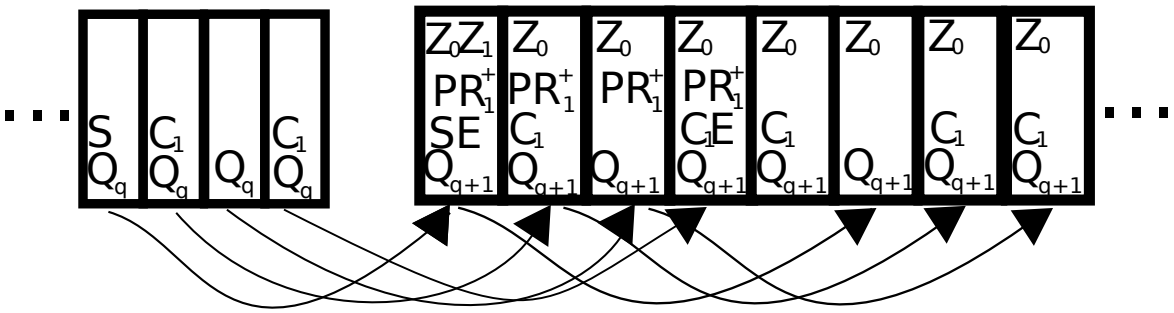


Figure 4.2: Example of a computation of $incr(1)$ in a non-deterministic 2-counter automaton

4.3 First-order logic with successor and an uninterpreted function

The results of this section are similar to the results of the previous section, but deal with the first-order logic with the successor function and an uninterpreted unary function symbol.

Section 4.3.1 is about spectra which are Boolean combination of b-recognizable sets for different values of b. Section 4.3.2 is about spectra which encodes spectra of non-deterministic 2-counter automata. Finally, Section 4.3.3 deals with encodings of some extremely quickly increasing functions in $\mathsf{FO}[+1, f]$.

4.3.1 Boolean combinations of b-recognizable sets are $\mathsf{FO}[+1, f]$-spectra

A theorem similar to Theorem 4.2.1 is proven in this section, for a logic with an uninterpreted function.

Theorem 4.3.1. *Every Boolean combinations of b-recognizable sets (for possibly distinct b's) is a* $\Pi_2[+1, f]$*-spectrum where* f *is a uninterpreted unary function symbol.*

Let us emphasize the main differences between Theorem 4.2.1 and Theorem 4.3.1. Theorem 4.2.1 considers the vocabulary $\{+1, \times b\}$ while Theorem 4.3.1 considers $\{+1, f\}$. The former theorem considers monadic second-order logic with two first-order variables, while the latter considers first-order logic with any number of variables.

Uninterpreted function and two-variable logic are not considered together, because almost no restriction to the function can be expressed in two-variable logic. For example, if one wants to restrict f to be the multiplication by 2, then it is naturally defined by $f(0) \doteq 0 \wedge \forall x. f(x) + 2 \doteq f(x + 1)$, but $f(x) + 2 \doteq f(x + 1)$ does not seem to be expressible in two-variable logic.

4.3.1.1 Examples

Two examples of 2-recognizable sets are given in this section. It is then show how to represent them as $\Pi_2[+1, f]$-spectra.

Example 4.2.5 is first resumed. This example shows how a formula can restrict the interpretation of f.

Example 4.3.2. Let $S = \{2^i + 1 \mid i \in \mathbb{N}\}$. A $\{+1, f\}$-formula ϕ whose spectrum is S is first constructed. Let $\mathcal{S}$ be a $\{+1, f\}$-structure of universe $[c]$. If $\mathcal{S} \models \phi$ then $c = 2^i$ for some $i \in \mathbb{N}$. Reciprocally, for all $i \in \mathbb{N}$, there exists a $\{+1, f\}$-structure $\mathcal{S}$ of universe $[2^i]$ such that $\mathcal{S} \models \phi$. For the sake of simplicity, consider that $c \geq 5$.

m	4
b_0	3
S_0	$\{3i+2 \mid i \in \mathbb{N}\}$
ξ_0	$x \equiv 2 \mod 3 \wedge x \geq 8$
S_0^k	$\{12 \times n + 8 - 3 \times k \mid n \in \mathbb{N}\}$ for $k \in [4]$
T_0^k	$\{12 \times n + 8 - 4 \times k \mid n \in \mathbb{N}\}$ for $k \in [4]$
U_0^k	$\{3 \times n + 2 - k \mid n \in \mathbb{N}\}$ for $k \in [4]$
ζ_0^k	$\exists (R_i)_{i \in [11]}. R_0(0) \wedge \forall x \neq \text{last}.$ $\bigwedge_{i=0}^{11} [R_i(x) \Longleftrightarrow R_{i+1 \mod 12}(x+1)]$ $\wedge R_{16-3k \mod 12}(\text{last})$
b_1	2
S_1	$\{2^i + 1 \mid i \in \mathbb{N}\}$
S_1^1	$\{2^i + 1 \mid i \in \mathbb{N}\}$
T_1^1	$\{2^i + 1 \mid i \in \mathbb{N}\}$
U_1^1	$\{2^i + 1 \mid i \in \mathbb{N}^{>0}\}$
ζ_1^1	$\exists R_{q_0}. R_{q_0}(\text{last}) \wedge \neg R_{q_0}(0) \wedge \forall n, n'.$ $\Big[n \neq 0 \wedge R_{q_0}(n) \wedge 2 \times n' \doteq n\Big] \Longrightarrow R_{q_0}(n')$
S_1^k	$\emptyset$ for k being 0, 2, 3
T_1^k	$\emptyset$ for k being 0, 2, 3
U_1^k	$\emptyset$ for k being 0, 2, 3
ζ_1^k	False for k being 0, 2, 3
S	$S_0 \cap S_1 = \{2^{2i} + 1 \mid i > 1\}$
S^1	$\{2^{2i} + 1 \mid i > 1\}$
T^1	$\{2^{2i} + 1 \mid i \in \mathbb{N}\}$
S^k	$\emptyset$ for k being 0, 2, 3
T^k	$\emptyset$ for k being 0, 2, 3

Table 4.1: Variables for a fixed set $S = S_0 \cap S_1$ of Proof of Theorem 4.3.1

The formula ϕ ensures that f encodes the set of powers of 2, as well as multiplication by 2. The multiplication is encoded over even numbers, and the set of powers of 2 is encoded over odd numbers.

Consider the function $g : [c] \to [c]$ defined as follows:

$$g(n) = \begin{cases} 2n & \text{if } n \text{ is even and } 2n \leq c \\ 1 & \text{if } n \text{ is even and } 2n > c \\ 3 & \text{if } n = 2^i - 1 \text{ for } i > 0 \\ 5 & \text{otherwise.} \end{cases}$$

Observe that c is a power of 2, namely $c = 2^i$ for $i \in \mathbb{N}$, if and only if $g(\text{last} - 1) = 1$ (for $i > 0$) or last $= 1$ (for $i = 0$).

The formula ϕ which ensures that the symbol f is interpreted as g is now constructed. The first part assert that for all $n > 0$, $f(n) \in \{3, 5\}$ if and only if $f(n-1) \notin \{3, 5\}$.

$$\forall x \neq 0. \big[f \doteq 3 \vee f \doteq 5\big] \Longleftrightarrow \{\neg \big[f(x-1) \doteq 3 \vee f(x-1) \doteq 5\big]\}.$$

The second part assert that the interpretation of f over even numbers is correct. This holds if the following conditions hold:

- $f(0) = 0$.
- For each x such that $f(x) \notin \{1,3,5\}$ and $f(x)+4 \leq c$, then $f(x+2) = f(x)+4$. Indeed, in this case, x is even, then $x+2$ is also even, and $f(x+2)$ should be $2\times(x+2) = 2\times x+4 = f(x)+4$. It can be asserted by:

$$\begin{aligned}\xi_{\leq \frac{c}{2}} = \forall x\{ \quad & f(x) \neq 1 \wedge f(x) \neq 3 \wedge f(x) \neq 5\} \Longrightarrow \\ \{ \quad & [(\exists z.z \doteq f(x)+4) \quad \Longrightarrow f(x+2) \doteq f(x)+4] \\ & \wedge [(\neg \exists z.z \doteq f(x)+4) \Longrightarrow f(x+2) \doteq 1]\}.\end{aligned}$$

- For each x such that $f(x) = 1$ then $f(x+2) = 1$.

$$\xi_{> \frac{c}{2}} = \forall x.f(x) \doteq 1 \Longrightarrow f(x+2) \doteq 1$$

Let ψ_{even} be the conjunction $f(0) \doteq 0 \wedge \xi_{\leq \frac{c}{2}} \wedge \xi_{> \frac{c}{2}}$.

Then $2 \times x \doteq y$ is considered as an abbreviation for

$$y \neq 1 \wedge y \neq 3 \wedge y \neq 5 \wedge \{f(x) \doteq y \vee f(x-1) \doteq y-2\}.$$

The interpretation of f over odd numbers is correct if: $f(x) = 3$ is equivalent to $\{x = 1$ or $f(\frac{x-1}{2}) = 3\}$. Indeed $2^1 - 1 = 1$ and $f(\frac{x-1}{2}) = 1$ implies that $\frac{x-1}{2} = 2^i - 1$ for some $i \in \mathbb{N}$, hence that $x = 2^{i+1} - 1$. It is asserted as follows:

$$\psi_{\text{odd}} = \forall x.f(x) \doteq 1 \Longleftrightarrow \{x \doteq 3 \vee \exists y.[2y+1 \doteq x \wedge f(y) \doteq 3]\}.$$

Finally S is the spectrum of the fDeeowing formula:

$$\{f(\text{last}-1) \doteq 1 \vee \text{last} \doteq 1\} \wedge \psi_{\text{even}} \wedge \psi_{\text{odd}}.$$

The following example is more involved. Let the basis b be 2. Let us start from a 2-recognizable set S. Let $\mathcal{A}$ be an automaton which accepts S. A formula ϕ of spectrum $3S$ is then given. The $\Pi_2[+1, f]$-formula ϕ asserts that the model of universe $[3c]$ encodes a computation of $\mathcal{A}$ over $\underline{c}_b$ using the uninterpreted function.

Example 4.3.3. Let S be the set of numbers n such that the word $\underline{n}_b$ has an even number of 1.

The set S is accepted by the automaton $\mathcal{A} = (\mathbb{Z}/2\mathbb{Z}, \{0,1\}, +, 0, \{0\})$.

A $\Pi_2[+1, f]$-formula ϕ whose spectra is $3S$ is now given. The formula ϕ asserts that, over the different equivalence classes modulo 3, the formula f encodes respectively:

- the equivalence classes modulo 3,
- the multiplication by 2 and
- the computation of the automaton $\mathcal{A}$.

Let $\mathcal{S}$ be a $\{+1, f\}$-structure of cardinality c and let $w = \underline{c}_b$. For technical reasons, it is assumed that $c \geq 3$. Let Q_i be the ith state of the computation of $\mathcal{A}$ on c. That is Q_i is the number of 1 in the first i letters of w.

Let $g : [c] \to [c]$ be the function defined as follows.:

- $g(3n) = 0$,

- $g(3n+1) = \begin{cases} Q_i + 1 & \text{if } n = \left\lfloor \frac{c}{2^i} \right\rfloor, i \in \mathbb{N}, \\ 3 & \text{otherwise,} \end{cases}$
- $g(3n+2) = \begin{cases} 6 \times n & \text{if } n \leq \frac{c}{6} \\ 5 & \text{otherwise} \end{cases}$.

The formula ϕ is now introduced, this formula states that the symbol f is interpreted as g.

The interpretation of f over multiples of 3 is correct if and only if the two following conditions hold: $f(0) = 0$ and for each $x \neq 2$, $f(x) = 0$ if and only if $f(x+3) = 0$.

It is formalized by ψ_0:

$$f(0) \doteq 0 \wedge (\forall x. x \not\equiv 2)[f(x) \doteq 0 \Longleftrightarrow f(x+3) \doteq 0].$$

Using this characterization, $n \equiv i \mod 3$ can be expressed as $f(n-i) \doteq 0 \wedge n - i \not\equiv 2$.

The interpretation of f over $3\mathbb{N} + 2 \cap [\frac{c}{6}]$ is correct if and only if the two following conditions hold: $f(2) = 0$ and for each $n \equiv 2 \mod 3$, $f(n+3)$ is equal to $f(n) + 6$ if it exists and to 5 otherwise. It is formalized by ξ_0:

$$f(2) \doteq 0 \wedge \forall x \equiv 2 \mod 3.\{ \quad [(\exists y \doteq f(x) + 6) \Longrightarrow f(x+3) \doteq f(x) + 6] \\ \wedge \quad [(\neg \exists y. y \doteq f(x) + 6) \Longrightarrow f(x+3) \doteq 5]\}.$$

Then $2 \times x = y$ can be expressed as $\bigvee_{i=0}^{2} x \equiv i \mod 3 \wedge f(x - i + 2) = y - 2 \times i$.

The interpretation of f over $3\mathbb{N} + 2 \setminus [\frac{c}{6}]$ is formalized by ξ_1:

$$\forall n. f(n) \doteq 5 \Longrightarrow f(n+3) \doteq 5.$$

Then the interpretation of f over $3\mathbb{N} + 2$ is formalized by $\psi_1 = \xi_0 \wedge \xi_1$.

The interpretation of f over $3\mathbb{N} + 1$ is correct if and only if the two following conditions hold:

- $f(\text{last}) \doteq 1$, indeed: $f(\text{last}) = f(c) = f(\left\lfloor \frac{c}{2^0} \right\rfloor) = Q_0 + 1 = 0 + 1 = 1$.
- the value of $f(3n+1)$ is 1, 2 or 3. It is formalized by χ_0:

$$\forall x \equiv 1 \mod 3. \bigvee_{i=1}^{3} f(x) \doteq i$$

- if $f(3n+1) = 1$ and n is even then $f(3\frac{n}{2} + 1) = 1$. Indeed, it implies that $n = \left\lfloor \frac{c}{2^i} \right\rfloor$ and $Q_i = 0$ for some $i \in \mathbb{N}$. Since n_i is even, the $(i+1)$th read letter is a 0, hence $Q_{i+1} = 0$, and finally one has $f(3\frac{n}{2} + 1) = f(3\left\lfloor \frac{c}{2^{i+1}} \right\rfloor + 1) = 1$.

  More generally, if $f(3n+1)$ is 1 or 2, if n is even then $f(3\frac{n}{2} + 1) = f(3n+1)$ and if n is odd then $f(3\frac{n-1}{2} + 1) = 3 - f(3n+1)$.

  It is formalized by the formula χ_1:

$$\forall x \equiv 0 \mod 3 \bigwedge_{i=1}^{2} \{f(x+1) \doteq i\} \Longrightarrow \\ \{\exists y. [2 \times y \doteq x \wedge f(y+1) \doteq i] \vee [2 \times y + 1 \doteq x \wedge f(y+1) \doteq 3 - i]\}$$

Then let ψ_2 be the formula $f(\text{last}) \doteq 1 \wedge \chi_0 \wedge \chi_1$.

The computation is accepting if the last state is 0, that is $f(1) = 1$.

Finally, $3S$ is the spectrum of the formula ϕ defined as follows

$$\psi_0 \wedge \psi_1 \wedge \psi_2 \wedge f(1) \doteq 1.$$

It is shown in the next section that, using properties of b-recognizable sets, the spectrum $3S$ can be replaced by S.

4.3.1.2 General case

It is now explained how to encode a Boolean combination of b-recognizable sets as a $\Pi_2[+1, f]$-spectrum.

Two classes of function are now introduced. A class of functions $\Xi_{m,d,e}$ from $\{+1, \times 2, \ldots, \times(m-1)\}$-structures to $\{+1, f\}$-structures and a function $\Phi_{m,d,e}$ from $\exists\mathsf{MSO}[+1, (\times 2, \ldots, \times(m-1))]$-formulas to $\mathsf{FO}[+1, f]$-formulas. The function $\Xi_{m,d,e}$ multiplies the cardinality by m. Moreover those functions are chosen such that $\mathcal{S} \models \phi$ if and only if $\Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}(\phi)$. Hence, if ϕ has a model, then $\Phi_{m,d,e}(\phi)$ also has a model. Conversely, if $\Phi_{m,d,e}(\phi)$ has a model and this model belongs to the image of $\Xi_{m,d,e}$ then ϕ also has a model. This properties impose to choose $\Xi_{m,d,e}$ such that there exists a $\mathsf{FO}[+1, f]$-formula which characterizes its image.

The function $\Phi_{m,d,e}$ is defined by induction over the $\exists\mathsf{MSO}[+1, (\times 2, \ldots, \times(m-1))]$-formulas. Let $\phi \in \exists\mathsf{MSO}[+1, \times b]$ be of the form $\exists R.\psi$, then $\psi \in \exists\mathsf{MSO}[+1, \times b, R]$, hence $\Phi_{m,d,e}$ and $\Xi_{m,d,e}$ must be defined on vocabularies which extends $\{+1, \times b\}$ with a finite number of first and second order variables.

The formal definition is now given.

Definition 4.3.4. Let $m > 1$ and let $d, e \in \mathbb{N}$. Let :

$$\mathcal{V}_{m,d,e} = \left\{+1, \times 2, \ldots, \times(m-1), (R_i)_{i \in [d-1]}, (x_i)_{i \in [e-1]}\right\},$$

and let

$$\mathcal{V}'_e = \left\{+1, f, (x_i)_{i \in [e-1]}\right\}.$$

The function $\Xi_{m,d,e}$ from $\mathcal{V}_{m,d,e}$ to $\mathcal{V}'_e$ must now be defined.

Semantically, $\Xi_{m,d,e}$ multiplies every value by m, and encodes every relation, apart from $+1$, with the unary function f. The image by f of each equivalence class modulo m encodes either the set of second order variables, or a multiplication, or the modular classes.

Definition 4.3.5. The function $\Xi_{m,d,e}$ sends each $\mathcal{V}_{m,d,e}$-structure $\mathcal{S}$ of cardinality κ to a $\mathcal{V}'_e$-structure $\Xi_{m,d,e}(\mathcal{S})$ of cardinality $m \times \kappa$, defined as follows:

- For $i \in [e-1]$, let $x_i^{\Xi_{m,d,e}(\mathcal{S})} = m \times x_i^{\mathcal{S}}$.
- The function $f^{\Xi_{m,d,e}(\mathcal{S})}$ is defined as follows:
  - $f^{\Xi_{m,d,e}(\mathcal{S})}(m \times n) = 0$ (to encode the congruence classes)
  - $f^{\Xi_{m,d,e}(\mathcal{S})}(m \times n + 1) = \left(\sum_{\substack{i \in [d-1] \\ R_i^{\mathcal{S}}(n)}} 2^{i+1}\right) + 1$ (to encode the value of all unary relations over n)

– for every $b \in [2, m-1]$:

$$f^{\Xi_{m,d,e}(\mathcal{S})}(m \times n + b) = \begin{cases} m \times n \times b & \text{if } m \times n \times b \text{ belongs to } [n \times \kappa - 1] \\ 1 & \text{otherwise} \end{cases}$$

(to encode the multiplication by b).

The value of $f^{\Xi_{m,d,e}(\mathcal{S})}(m \times n + 1)$ encodes the set of second order variables whose interpretation in $\mathcal{S}$ hold on n. This is the only value of $\Xi_{m,d,e}(\mathcal{S})$ which depends on $\mathcal{S}$.

It should be noted that the antecedent of 0 by $f^{\Xi_{m,d,e}(\mathcal{S})}$ is $(m \times [\kappa - 1]) \cup [2, m-1]$. Hence $x \equiv 0 \mod m$ if and only if $\Xi_{m,d,e}(\mathcal{S}) \models \mathrm{Mul}_m(x)$ where:

$$\mathrm{Mul}_m(x) = f(x) \doteq 0 \wedge \bigwedge_{i=2}^{m-1} x \neq i.$$

In the following examples, Example 4.2.5 is resumed. The exact result of the application of those functions is shown, with $m = 4$. Note that Example 4.3.2 is not an application of the functions $\Phi_{m,d,e}$ and $\Xi_{m,d,e}$; some properties used in the general case are omitted in Example 4.3.2 to simplify the formula.

Example 4.3.6. Let $m = 4$, $d = 1$ and $e = 1$, then $\mathcal{V}_{4,1,1} = \{+1, \times 2, \times 3, R_0, x_0\}$ and $\mathcal{V}'_1 = \{+1, f, x_0\}$.

Let $\mathcal{S}$ be a $\mathcal{V}_{m,d,e}$-structure of cardinality $2^c + 1$ for $c \in \mathbb{N}$ such that: $x_0^{\mathcal{S}} = \mathrm{last}^{\mathcal{S}} = 2^c$ and $R_0^{\mathcal{S}} = \{2^i \mid i \in [c] \setminus \{0\}\}$.

Then $\Xi_{m,d,e}(\mathcal{S})$ is the structure of cardinality $4 \times \left(2^i + 1\right) = 2^{i+2} + 4$ such that:

- $x_0^{\Xi_{m,d,e}(\mathcal{S})} = 2^{c+2} = \left(2^{c+2} + 3\right) - 3 = \mathrm{last}^{\Xi_{m,d,e}(\mathcal{S})} - 3$,
- The function $f^{\Xi_{m,d,e}(\mathcal{S})}$ is defined as:
  - $f^{\Xi_{m,d,e}(\mathcal{S})}(4 \times n) = 0$ for $n \in [2^c]$,
  - $f^{\Xi_{m,d,e}(\mathcal{S})}(4 \times n + 1) = \begin{cases} 3 & \text{if } n \text{ is of the form } 2^j \\ 1 & \text{otherwise} \end{cases}$
  - $f^{\Xi_{m,d,e}(\mathcal{S})}(4 \times n + 2) = 8 \times n$ if $n \in \left[2^{c-3}\right]$, and is undefined otherwise,
  - $f^{\Xi_{m,d,e}(\mathcal{S})}(4 \times n + 3) = 12 \times n$ if $n \in \left[\left\lfloor \frac{2^{c-2}}{3} \right\rfloor\right]$ and is undefined otherwise,

Finally, the function $\Phi_{m,d,e}$ from $\mathsf{FO}[\mathcal{V}_{m,d,e}]$ to $\mathsf{FO}[\mathcal{V}'_e]$ is introduced. Intuitively, this function translates the formulas such that the properties introduced in Definition 4.3.5 are satisfied.

Definition 4.3.7 ($\Phi_{m,d,e}$)**.** The function $\Phi_{m,d,e}$ is defined recursively as follows:

ϕ	$\Phi_{m,d,e}(\phi)$	ϕ	$\Phi_{m,d,e}(\phi)$
$\chi \vee \psi$	$\Phi_{m,d,e}(\chi) \vee \Phi_{m,d,e}(\psi)$	$\neg\psi$	$\neg\Phi_{m,d,e}(\psi)$
$x + 1 \doteq y$	$x + m \doteq y$	$b \times x \doteq y$	$f(x + b) \doteq y$
$\exists x.\psi$	$\exists x.\mathrm{Mul}_m(x) \wedge \Phi_{m,d,e+1}(\psi)$	$x \doteq y$	$x \doteq y$
$R_i(x)$	$\bigvee_{\substack{I \subseteq [d] \\ i \in I}} \left[f(x+1) \doteq \sum_{j \in I} 2^{j+1} + 1\right]$		

Example 4.3.6 is resumed in order to give an example of the application of $\Phi_{m,d,e}$ to the formula of Example 4.2.5.

Example 4.3.8. The formula ϕ of Example 4.2.5 and the formula $\Phi_{m,d,e}(\phi)$ are:

$$\begin{array}{rlll} \phi = & \exists R_{q_0}.\, R_{q_0}(\mathrm{last}) & \wedge \quad \neg R_{q_0}(0) & \wedge \\ & \forall x. & \{x \neq 0 \wedge R_{q_0}(2 \times x) & \}\wedge R_{q_0}(n') \\ \Phi_{m,d,e}(\phi) = & f(\mathrm{last} - 2) \doteq 3 \wedge & \neg f(1) \doteq 3 & \wedge \\ & \forall x.\mathrm{Mul}_4(x) & \Longrightarrow \{x \neq 0 \wedge f(f(x+2)+1) \doteq 3\} & \wedge f(n'+1) \doteq 3. \end{array}$$

The following lemma states that the functions $\Xi_{m,d,e}$ and $\Phi_{m,d,e}$ preserve satisfiability.

Lemma 4.3.9. *Let $m, d, e \in \mathbb{N}$. Let $\phi \in \mathsf{FO}[\mathcal{V}_{m,d,e}]$ and $\mathcal{S}$ be a $\mathcal{V}_{m,d,e}$-structure. Then $\mathcal{S} \models \phi$ if and only if $\Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}(\phi)$.*

Proof. By induction over ϕ:

- If ϕ is $x_i \doteq x_j$, then the following statements are equivalent:

$$
\begin{aligned}
&\mathcal{S} \models && x_i \doteq x_j && && \\
\iff & && x_i^{\mathcal{S}} = x_j^{\mathcal{S}} && && \text{(using the definition of } \models) \\
\iff & && m \times x_i^{\mathcal{S}} = m \times x_j^{\mathcal{S}} && && \text{(multiplication)} \\
\iff & && x_i^{\Xi_{m,d,e}(\mathcal{S})} = x_j^{\Xi_{m,d,e}(\mathcal{S})} && && \text{(using the definition of } \Xi_{m,d,e}) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models && x_i \doteq x_j && && \text{(using the definition of } \models) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}(&& x_i \doteq x_j &&) && \text{(using the definition of } \Phi_{m,d,e}).
\end{aligned}
$$

- If ϕ is $x_i + 1 \doteq x_j$, then the following statements are equivalent:

$$
\begin{aligned}
&\mathcal{S} \models && x_i + 1 \doteq x_j && && \\
\iff & && x_i^{\mathcal{S}} + 1 = x_j^{\mathcal{S}} && && \text{(using the definition of } \models) \\
\iff & && m \times x_i^{\mathcal{S}} + m = m \times x_j^{\mathcal{S}} && && \text{(multiplication)} \\
\iff & && x_i^{\Xi_{m,d,e}(\mathcal{S})} + m = x_j^{\Xi_{m,d,e}(\mathcal{S})} && && \text{(using the definition of } \Xi_{m,d,e}) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models && x_i + m \doteq x_j && && \text{(using the definition of } \models) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}(&& x_i + 1 \doteq x_j &&). && \text{(using the definition of } \Phi_{m,d,e})
\end{aligned}
$$

- If ϕ is $x_i \times b \doteq x_j$, then two cases must be considered, depending on the value of $x_i^{\mathcal{S}}$. Assume that $x_i^{\mathcal{S}} \geq \frac{|\mathcal{S}|}{b}$. Then $x_i^{\mathcal{S}} \times b \geq |\mathcal{S}|$, hence $x_i^{\mathcal{S}} \times b$ does not belong to the universe, which implies that $f\left(m \times x_i^{\mathcal{S}} + b\right) = 1$, which is not a multiple of m. Hence $\mathcal{S} \not\models f(x_i + b) \doteq x_j$. Hence $\mathcal{S} \models \phi$ is trivially equivalent to $\Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}\left(x_i \times b \doteq x_j\right)$ since both statements are false.

  Now, assume that $x_i^{\mathcal{S}} < \frac{|\mathcal{S}|}{b}$, then the following statements are equivalent:

$$
\begin{aligned}
&\mathcal{S} \models && b \times x_i && \doteq && x_j && \\
\iff & && b \times x_i^{\mathcal{S}} && = && x_j^{\mathcal{S}} && \text{(using the definition of } \models) \\
\iff & && b \times m \times x_i^{\mathcal{S}} && = && m \times x_j^{\mathcal{S}} && \text{(multiplication)} \\
\iff & && b \times x_i^{\Xi_{m,d,e}(\mathcal{S})} && = && x_j^{\Xi_{m,d,e}(\mathcal{S})} && \text{(using the definition of } \Xi_{m,d,e}) \\
\iff & && f^{\Xi_{m,d,e}(\mathcal{S})}(x_i^{\Xi_{m,d,e}(\mathcal{S})} + b) && = && x_j^{\Xi_{m,d,e}(\mathcal{S})} && \left(\text{using the definition of } f^{\Xi_{m,d,e}}\right) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models && f(x_i + b) && \doteq && x_j && \text{(using the definition of } \Xi_{m,d,e}) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}(&& b \times x_i && \doteq && x_j &&). \quad \text{(using the definition of } \Phi_{m,d,e})
\end{aligned}
$$

- If ϕ is $R_i\left(x_j\right)$, then the following statements are equivalent:

$$
\begin{aligned}
&\mathcal{S} \models R_i\left(x_j\right) && \\
\iff & \text{there exists } I \subseteq [d],\ j \in I \text{ such that} && \\
& f^{\Xi_{m,d,e}(\mathcal{S})}\left(x_j^{\Xi_{m,d,e}(\mathcal{S})}\right) = \textstyle\sum_{k \in I} 2^{k+1} + 1 && \left(\text{using the definition of } f^{\Xi_{m,d,e}}\right) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models \bigvee_{\substack{I \subseteq [d] \\ i \in I}} f(x) = \textstyle\sum_{j \in I} 2^{j+1} + 1 && \text{(using the definition of } \models) \\
\iff & \Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}\left(R_i\left(x_j\right)\right). && \text{(using the definition of } \Phi_{m,d,e})
\end{aligned}
$$

- If ϕ is $\exists x.\psi$, then it should be noted that $f^{\Xi_{m,d,e}(\mathcal{S})}(n) = 0$ if and only if ($n = p \times m + q$ with $q \in [m-1]$ and $q = 0$) or ($p = 0$ and $q > 1$). Then the following statements are equivalent:

$$\begin{array}{lll}
\mathcal{S} & \models \exists x.\psi & \\
\Longleftrightarrow \text{there exists } c \in [s-1] & \text{such that} & \\
\mathcal{S}\ [x/c] & \models \psi & \text{(using the definition of } \models) \\
\Longleftrightarrow \text{there exists } c \in [s-1] & \text{such that} & \\
\Xi_{m,d,e}(\mathcal{S}\ [x/c]) & \models \Phi_{m,d,e}(\psi) & \text{(using induction)} \\
\Longleftrightarrow \text{there exists } c \in [s-1] & \text{such that} & \\
\Xi_{m,d,e}(\mathcal{S})[x/m \times c] & \models \Phi_{m,d,e}(\psi) & \text{(using the definition of } \Xi_{m,d,e}) \\
\Longleftrightarrow \text{there exists } c' \in [m \times s - 1] \cap m\mathbb{N}, & \text{such that} & \\
\Xi_{m,d,e}(\mathcal{S})[x/c'] & \models \Phi_{m,d,e}(\psi) & \\
\Longleftrightarrow \text{there exists } c' \in [m \times s - 1] & \text{such that} & \\
\Xi_{m,d,e}(\mathcal{S})[x/c'] & \models \Phi_{m,d,e}(\psi) \wedge \mathrm{Mul}_m(x) & \text{(using the definition of } \mathrm{Mul}_m) \\
\Longleftrightarrow \Xi_{m,d,e}(\mathcal{S}) & \models \Phi_{m,d,e}(\phi). & \text{(using the definition of } \Phi_{m,d,e})
\end{array}$$

- Finally if ϕ is a negation or a disjunction, then the proof is a straightforward consequence of the induction hypothesis.

□

As explained in the introduction of this section, the image of $\Xi_{m,d,e}$ must be characterized. This is done in the following lemma.

Lemma 4.3.10. *Let $m, d, e \in \mathbb{N}$. There exists a $\Pi_2[+1, f]$-formula $\theta_{m,d,e}$ which holds over the $\mathcal{V}'_e$-structures belonging to the image of $\Xi_{m,d,e}$.*

Proof. A list of properties is given, which characterizes the image of $\Xi_{m,d,e}$, together with $\Pi_2[+1, f]$-formulas which express those properties.

- Let ψ_0 be the formula which states that the cardinality of the structure is at least 2^{d+1}, using the formula introduced in Lemma 4.1.6:

$$\gamma_{\geq 2^{d+1}}.$$

- Let ψ_1 be the formula which states that all constants belong to $m\mathbb{N}$:

$$\bigwedge_{i=0}^{e-1} \mathrm{Mul}_m(c_i)$$

- Let ψ_2 be the formula which states that the cardinality of the structure is a multiple of m:

$$\mathrm{Mul}_m(\mathrm{last} - m + 1)$$

- For each $n \in m \times \mathbb{N}$:
  - Let ξ_0 be the formula which states that $f^{\Xi_{m,d,e}(\mathcal{S})}(n+m) = 0$:

$$f(n+m) \doteq 0.$$

  - Let ξ_1 be the formula which states that $f^{\Xi_{m,d,e}(\mathcal{S})}(n+1)$ is an odd integer between 1 and $2^{d+2} - 1$:

$$\bigvee_{i=0}^{2^d} f(n) \doteq 2i + 1.$$

– For $q \in [2, m-1]$, let $\xi_{2,q}$ be the formula which states that $f^{\Xi_{m,d,e}(\mathcal{S})}(n+q)$ is $c \times n$ if cn belongs to the universe, and equals 1 otherwise. Recall that the notation $\langle \cdot \mid \cdot \mid \cdot \rangle$ is introduced in Notation 2.2.11. The formula $\xi_{2,q}$ is:

$$f(q) \doteq 0 \wedge \langle [\exists y. y \doteq m \times q + f(n+q-m)] \mid f(n+q) \doteq m \times q + f(n+q-m) \mid f(n+q) \doteq 1 \rangle.$$

It should be noted that $m \times q$ and $q - m$ are constants, hence it is indeed a $\Pi_2[+1, f]$-formula.

– Let ξ_3 be the formula which states that if $f^{\Xi_{m,d,e}(\mathcal{S})}(n+q) = 1$ for $q > 1$, then $f^{\Xi_{m,d,e}(\mathcal{S})}(n+q+m) = 1$:

$$\{f(n+q) \doteq 1\} \Longrightarrow \{f(n+m+q) \doteq 1\}.$$

Let ψ_3 be the formula

$$\forall n. \left(f(n) \doteq 0 \wedge \bigwedge_{i=2}^{m-1} n \neq i \right) \Longrightarrow \{\xi_0 \wedge \xi_1 \wedge \xi_{2,q} \wedge \xi_3\}$$

The image of $\Xi_{m,d,e}$ is then defined by the formula $\theta_{m,d,e} = \psi_0 \wedge \psi_1 \wedge \psi_2 \wedge \psi_3$. □

Combining the formulas $\theta_{m,d,e}$ and $\Phi_{m,d,e}$, $\exists \mathsf{MSO}[+1, \times 2, \ldots, \times(m-1)]$-spectrum S can be transformed into a $\mathsf{FO}[+1, f]$-spectrum $m \times S$.

Lemma 4.3.11. *Let $m \geq 2$, $d, e \in \mathbb{N}$, and $k < m$. Let $\phi \in \mathsf{FO}[+1, (\times b)_{b \in [m-1]}, (R_i)_{i \in [d-1]}, (x_i)_{i \in [e-1]}]$. Let $\psi = \theta_{m,d,e} \wedge \Phi_{m,d,e}(\phi)$. Then $\mathsf{SP}(\psi) = (m \times \mathsf{SP}(\phi)) \setminus [2^{d+1} - 1]$.*

Proof. Let us prove that $\mathsf{SP}(\psi) \subseteq (m \times \mathsf{SP}(\phi)) \setminus [2^{d+1} - 1]$.

Let $n \in \mathsf{SP}(\psi)$. Then there exists a $\mathcal{V}'_e$-structure $\mathcal{S}'$ with cardinality n such that $\mathcal{S}' \models \psi$. If follows from the definition of ψ and Lemma 4.3.10 that the structure $\mathcal{S}'$ belongs to the image of $\Xi_{m,d,e}$. Hence n is of the form $m \times n'$, with $n \geq 2^{d+1}$ and there exists a $\mathcal{V}_{m,d,e}$-structure $\mathcal{S}$ of cardinality n' such that $\Xi_{m,d,e}(\mathcal{S}) = \mathcal{S}'$. Since $\mathcal{S}' \models \Phi_{m,d,e}(\phi)$, by Lemma 4.3.9, $\mathcal{S} \models \phi$, hence $n' \in \mathsf{SP}(\phi)$, thus $n \in m \times \mathsf{SP}(\phi)$.

Let us prove that $\mathsf{SP}(\psi) \subseteq (m \times \mathsf{SP}(\phi)) \setminus [2^{d+1} - 1]$.

Let $n \in (m \times \mathsf{SP}(\phi)) \setminus [2^{d+1} - 1]$, then $n = m \times n'$ and $n \geq 2^{d+1}$ with $n' \in \mathsf{SP}(\phi)$. It must be proved that $n \in \mathsf{SP}(\psi)$. There exists a $\mathcal{V}_{m,d,e}$-model $\mathcal{S}$ of cardinality n' such that $\mathcal{S} \models \phi$. Hence by Lemma 4.3.9 $\Xi_{m,d,e}(\mathcal{S}) \models \Phi_{m,d,e}(\phi)$. Furthermore, by Lemma 4.3.10, $\Xi_{m,d,e}(\mathcal{S}) \models \theta_{m,d,e}$. Hence $\Xi_{m,d,e}(\mathcal{S})$ is also a model of $\Phi_{m,d,e}(\phi) \wedge \theta_{m,d,e}$, that is, a model of ψ. Moreover, by definition, the cardinality of $\Xi_{m,d,e}(\mathcal{S})$ is n. Hence $n \in \mathsf{SP}(\psi)$. □

The proof of Theorem 4.3.1 is finally given.

Table 4.1 gives examples of values for the variables of the first part of the proof. It describes different ways to see the set $S = S_0 \cap S_1$. The formulas ζ_i^k are not the ones given by Lemma 4.1.6, but some smaller equivalent ones. This simplifies the example without loss of generality. Indeed this proof is correct for any formula, and not only for the one generated by Lemma 4.1.6.

Proof of Theorem 4.3.1. Let S be a Boolean combining of b-recognizable set. Since b-recognizable sets are closed under complementing, it can be assumed that S is a positive Boolean combination of $b_{i,j}$-recognizable sets, that is, $S = \bigcup_i \bigcap_j S_{i,j}$ where every $S_{i,j}$ is $b_{i,j}$-recognizable for some $b_{i,j} \geq 2$. Let $m = \max\left(b_{i,j}\right) + 1$.

Some intermediate sets are then introduced, and it is proven that all such sets are $\mathsf{FO}[+, (V_b)_{b<m}]$-definable. The problem is then reduced to proving that those sets are $\Pi_2[+1, f]$-spectra.

By Lemma 4.1.7, spectra are closed by union, thus, in order to prove that S is a $\Pi_2[+1, f]$-spectrum, it is sufficient to prove that every $S_i = \bigcap_j S_{i,j}$ is a $\Pi_2[+1, f]$-spectrum. Let i be fixed in the remaining of this proof. Let $\chi_{i,j}(x) \in \mathsf{FO}[+, V_{b_{i,j}}]$ be a formula which defines $S_{i,j}$.

Let us prove that $S_i = \bigcap_j S_{i,j}$ is a $\Pi_2[+1, f]$-spectrum.

Since the function $\Xi_{m,d,e}$ multiplies the size of models by m, the set S is partitioned into m parts, one part for each congruence class. For $k \in [m-1]$, let $S^k_{i,j} = S_{i,j} \cap (m\mathbb{N} + k)$ and $S^k_i = S_i \cap (m\mathbb{N} + k)$. The set $S^k_{i,j}$ is b-recognizable as it is defined by $\chi^k_{i,j}(x) = \chi_{i,j}(x) \wedge x \equiv k \mod m$ and the modular relations are $\mathsf{FO}[+]$-definable.

Then $S_i = \bigcup_{k\in[m-1]} S^k_i$. By Lemma 4.1.7 it is enough to prove that S^k_i is a $\Pi_2[+1, f]$-spectrum. Let $k \in [m-1]$ be fixed for the remainder of the proof.

Let $T^k_{i,j} = S^k_{i,j} - k$, it is $b-$regular since it is defined by $\tau^k_{i,j}(x) = \chi^k_{i,j}(x + k)$.

Let $T^k_i = \cap_j T^k_{i,j}$. By Lemma 4.1.8, it is enough to prove that T^k_i is a $\Pi_2[+1, f]$-spectrum. Let $U^k_{i,j} = \frac{T^k_{i,j}}{m}$. This set is also $b_{i,j}$-recognizable as it is defined by $\beta^k_{i,j}(x) = \tau^k_{i,j}(m \times x)$. By Theorem 4.2.1 there exist $d \in \mathbb{N}$ and an $\exists\mathsf{MSO}\Pi_2[+1, \times b_{i,j}]$-formula $\zeta^k_{i,j}$ of the form $\exists R_0, \ldots, R_{d-1}.\xi^k_{i,j}$ such that $\mathsf{SP}\left(\zeta^k_{i,j}\right) = U^k_{i,j}$. Without loss of generality, it can be assumed that no second order variable is used in two distinct formulas $\zeta^k_{i,j}$ and $\zeta^{k'}_{i',j'}$. Hence the formulas $\exists R_0, \ldots, R_{d-1}. \bigwedge_j \zeta^k_{i,j}$ and $\bigwedge_j \exists R_0, \ldots, R_{d-1}.\zeta^k_{i,j}$ are equivalent.

Let $\psi^k_i = \theta_{m,d,e} \wedge \Phi_{m,d,0}\left(\bigwedge_j \zeta^k_{i,j}\right)$, then by Lemma 4.3.11,

$$\begin{aligned}\mathsf{SP}\left(\psi^k_i\right) &= m\times\mathsf{SP}\left(\textstyle\bigwedge_j \zeta^k_{i,j}\right)\setminus[2^{d+1}-1] = m\times[\textstyle\bigcap_j \mathsf{SP}\left(\zeta^k_{i,j}\right)]\setminus[2^{d+1}-1] = \\ &m\times\ [\textstyle\bigcap_j U^k_{i,j}]\ \setminus[2^{d+1}-1] = m\times\ \ U^k_i\ \ \setminus[2^{d+1}-1] = T^k_{i,j}\setminus[2^{d+1}-1].\end{aligned}$$

Hence $T^k_i \setminus [2^{d+1}-1]$ is a $\Pi_2[+1, f]$-spectrum, and by Lemma 4.1.6, T^k_i is a $\Pi_2[+1, f]$-spectrum. □

4.3.2 From spectra of Non-deterministic 2-counter automata to $\mathsf{FO}[+1, f]$-spectra

The following theorem is similar to Theorem 4.2.10, for the logic $\mathsf{FO}[+1, f]$.

Theorem 4.3.12. *For each non-deterministic 2-counter automaton $\mathcal{A}$, there exists a formula $\chi_{\mathcal{A}} \in \Pi_2[+1, f]$ such that $\mathsf{SP}(\chi_{\mathcal{A}}) = \left\{2^{t+3} + 4 \mid t \in \mathsf{SP}(\mathcal{A})\right\}$.*

Proof. Let $\mathcal{A}$ be a non-deterministic 2-counter automaton. Theorem 4.2.10 is used with $g(x) = x \times 2$, hence with $s^g_t = 2^{t+1}$. By this theorem, there exists $\phi_{\mathcal{A}} \in \exists\mathsf{MSO}\Pi_2[+1, \times 2]$ such that $\mathsf{SP}(\phi_{\mathcal{A}}) = \{2^{t+1} + 1 \mid t \in \mathsf{SP}(\mathcal{A})\}$. The formula $\phi_{\mathcal{A}}$ is of the form $\exists X_0, \ldots, X_{d-1}.\psi_{\mathcal{A}}$ with $\psi_{\mathcal{A}} \in \Pi_2[+1, \times 2, X_0, \ldots, X_{d-1}]$. By Lemma 4.1.5, $\mathsf{SP}(\phi_{\mathcal{A}}) = \mathsf{SP}(\psi_{\mathcal{A}})$.

Let $\chi_{\mathcal{A}} = \theta_{4,d,0} \wedge \Phi_{4,d,0}(\psi_{\mathcal{A}})$, where $\theta_{4,d,0}$ is the $\Pi_1[+1, f]$-formula of Lemma 4.3.10, and $\Phi_{4,d,0}$ is the function of Definition 4.3.7. By Lemma 4.3.11:

$$\begin{aligned}\mathsf{SP}(\chi_{\mathcal{A}}) &= \{4 \times n \mid n \in \mathsf{SP}(\psi_{\mathcal{A}})\} \setminus \left[2^{d+1} - 1\right] \\ &= \left\{4 \times \left(2^{t+1} + 1\right) \mid t \in \mathsf{SP}(\mathcal{A})\right\} \setminus \left[2^{d+1} - 1\right] \\ &= \left\{2^{t+3} + 4 \mid t \in \mathsf{SP}(\mathcal{A})\right\} \setminus \left[2^{d+1} - 1\right].\end{aligned}$$

By Lemma 4.1.6, $\left\{2^{t+3} + 4 \mid t \in \mathsf{SP}(\mathcal{A})\right\}$ is also a spectrum. □

4.3.3 Defining increasing functions in $\mathsf{FO}[+1, f]$

Another way to assert the expressivity of a logic is to exhibit some sets that it can define. It is proven that $\Pi_2[+1, f(x)]$ — with $f(x)$ uninterpreted — can encode in $\mathbb{N}$ some functions which are increasing extremely quickly such as $n \mapsto c \uparrow^d n$, the Knuth's up-arrow notation, as defined in [Knu76] .

The induction operator $\iota : ((\mathbb{N} \to \mathbb{N}) \times \mathbb{N}) \to (\mathbb{N} \to \mathbb{N})$ is now introduced. For $f : \mathbb{N} \to \mathbb{N}$, $c, n \in \mathbb{N}$, let $\iota(f,c)$ be the function defined by recursion on c such that $\iota(f,c)(0) = c$ and $\iota(f,c)(n+1) = f(\iota(f,c)(n))$.

Definition 4.3.13 ($\mathbb{F}$)**.** Let $\mathbb{F}$ be the smallest set of functions containing:

- the constant function 0,
- the function successor "+1",
- the function $f \circ g$ for each function f and g of $\mathbb{F}$ and
- the function $\iota(f,c)$ for each function f of $\mathbb{F}$ and $c \in \mathbb{N}$.

Some examples of functions in $\mathbb{F}$ are now given:

Example 4.3.14.

- the function $+1 \circ +(c-1)$ equals the function $+c$,
- the function $+c \circ 0$ equals the constant function c,
- the function $\iota(+c, 1)$ equals the multiplication by a constant $\times c$,
- the function $\iota(\times c, 1)$ equals the exponentiation in base c, $n \mapsto c^n$ and
- the function $\iota\left(c \uparrow^d n, c\right)$ equals the function $c \uparrow^{d+1} n$.

Hence, $\mathbb{F}$ contains functions that are known to increase quickly. On the other hand, it does not seem to contain functions such as $\log(n)$ or n^2.

Theorem 4.3.15. *For each $g \in \mathbb{F}$ there exists a formula $\phi(x,y) \in \Pi_2[+1, f]$ such that for any $\{+1, f\}$-structure over the universe $\mathbb{N}$, $\mathcal{S} \models \phi(x,y)$ if and only if $g\left(x^{\mathcal{S}}\right) = y^{\mathcal{S}}$.*

Proof. The function g is defined by induction, using a finite number m of functions. Let $(g_i)_{i \in [m-1]}$ be a list of those functions, with $g = g_m$. Let $M = m + 2$. Each function g_i will be defined in the equivalence class $i + 2$ modulo M. Hence the set of multiples of M must also be defined. For technical reasons, the last equivalence class defines the multiplication by M.

It is now stated that the function $f^{\mathcal{S}}$ is such that $f^{\mathcal{S}}(M \times n) = 0$ for $n \in \mathbb{N}$, and $f^{\mathcal{S}}(M \times n + a) \neq 0$ for all $a \in [M-1] \setminus \{0\}$. This can be express by the formula ϕ_{mod}, equal to:

$$\bigwedge_{a=1}^{M-2} f(a) \not\doteq 0 \wedge f(0) \doteq 0 \wedge \forall x. f(x) \doteq 0 \Longleftrightarrow f(x+M) \doteq 0.$$

By this requirement, $x \equiv a \mod (m+2)$ can be expressed by $f(x-a) \doteq 0$.

It is now stated that $f^{\mathcal{S}}(n \times M + 1) = M^2 \times n + 1$, which can be expressed by the following formula ϕ_{mul}, equal to:

$$f(1) \doteq 1 \wedge \forall x. (x \equiv 1 \mod M) \Longrightarrow f(x+M) \doteq f(x) + M^2.$$

Hence $x \times M \doteq y$ can be expressed by:

$$\bigvee_{a=0}^{m+1} (x \equiv a \mod M \wedge f(x+1-a) + a \times M - 1 \doteq y),$$

Finally, for $a \in [m-1]$, for $n \in \mathbb{N}$, $f(n \times M + a + 2) = g_a(n) + 1$. Hence $g_a(x)$ can be defined as $f(x \times M + a + 2) - 1$ by the formula ϕ_{g_a} defined as follows:

- if g_a is the constant function 0, let ϕ_{g_a} be $\forall x. f(x \times M + a + 2) \doteq 1$,
- if g_a is the function $+1$, let ϕ_{g_a} be $\forall x. f(x \times M + a + 2) \doteq x + 2$,
- if g_a is the function $g_b \circ g_c$, let ϕ_{g_a} be $\forall x. f(x \times M + a + 2) \doteq g_b(g_c(x))$,
- and finally, if g_a is the function $\iota(g_b, c)$, let ϕ_{g_a} be

$$f(a) \doteq c + 1 \wedge \forall x.\{x \equiv a \mod M\} \Longrightarrow f(x + m + 2) \doteq g_b(f(x) - 1).$$

Then the formula ϕ defined as

$$\phi_{\text{mod}} \wedge \phi_{mul} \wedge \bigwedge_{i=0}^{m-1} \phi_{g_i}.$$

asserts that g is interpreted as required above.

Hence $g\left(x^{\mathcal{S}}\right) = y^{\mathcal{S}}$ can be expressed as $\phi \wedge g_m(x) \doteq y$, that is as

$$\phi \wedge f(Mx + m + 2) - 1 \doteq y.$$

□

4.4 Conclusion

In this chapter, it is proven that, contrary to what may intuitively be expected, first-order logic with only the successor and an uninterpreted function is quite expressive. In particular the spectra of those logics are complex, even when there is only one alternation of quantifiers.

Note that the spectrum of $\phi_{\mathcal{A}}$ for the non-deterministic 2-counter automaton $\mathcal{A}$ of Example 4.1.12 is equal to

$$\left\{2^{7n+3n^2+1} + 1 \mid n \in \mathbb{N}^{>0}\right\}.$$

More natural than $\left\{2^{7n+3n^2+1} + 1 \mid n \in \mathbb{N}^{>0}\right\}$ could be generated, such as $\left\{2^{n^2} + 1 \mid n \in \mathbb{N}^{>0}\right\}$. Indeed, the encoding of spectra used in Theorem 4.2.10 is robust. In order to give more flexibility to generate the desired spectra, the following modifications in the definition of the non-deterministic 2-counter automata could easily be encoded in a similar fashion:

- adding any finite number of counters,
- adding an instruction that copies a counter into another one,
- assigning 0 to a counter.

More generally, it remains to find more classes of sets which are spectra of those logics. In particular, we are currently studying how to encode the image of polynomials as $\mathsf{FO}[+1, f]$-spectra with f uninterpreted.

Notations used in Chapter 4

$E^g(n)$, 79
$e^g(n)$, 79

$\mathbb{F}$, 93

$\gamma_{\geq n,\Sigma}$, 73
$\gamma_{\geq n,\Pi}$, 73
$\gamma_{n,\Pi}$, 73
$\gamma_{n,\Sigma}$, 73

$\iota(f,c)$, 93

$\Phi_{m,d,e}$, 88

s_n^g, 79

$\theta_{m,d,e}$, 90

$\mathcal{V}'_e$, 87
$\mathcal{V}_{m,d,e}$, 87

$\Xi_{m,d,e}$, 87

Chapter 5

Undecidability of satisfiability of some logics

In this chapter, it is proven that satisfiability problems for several related logics are undecidable. The first two logics considered are the one studied in Chapter 4: $\exists\mathsf{MSO}[+1, g(n)]$ where g is not bounded by any function of the form $n \mapsto n+c$, and $\mathsf{FO}[+1, f]$ with f uninterpreted, as in Chapter 4. It is also proven that $\mathsf{FO}[<, R]$ is undecidable, where R is $\mathsf{FO}[<,+]$-definable, but not $\mathsf{FO}[<, \mathrm{mod}]$-definable, as in Section 3.4.

Contents

5.1 From finite models to $\mathbb{N}$ **95**

5.2 The results **96**

5.3 Conclusion **96**

5.1 From finite models to $\mathbb{N}$

The next lemma extends undecidability of the finite satisfiability problem to undecidability over $\mathbb{N}$. This will allow to prove theorems about finite universes only.

Lemma 5.1.1. *Let $\mathcal{L}[\mathcal{V}]$ be a first-order logic with universal and existential quantifiers, and at least two first-order variables, such that finite satisfiability of the logic $\exists\mathsf{MSO}\mathcal{L}[\mathcal{V}]$ is undecidable. Then satisfiability of $\exists\mathsf{MSO}\mathcal{L}[\mathcal{V} \cup \{+1\}]$ is undecidable over $\mathbb{N}$.*

Proof. Let $\phi \in \mathcal{L}[\mathcal{V}]$ and $\mathcal{S}$ be a $\mathcal{V}-$structure of cardinality n. Let M be a second-order variable not in $\mathcal{V}$, and let $\mathcal{S}'$ be the $(\mathcal{V} \cup \{M\})$-structure over $\mathbb{N}$, where $M^{\mathcal{S}'} = [n-1]$, $+1$ has its usual interpretation, and $\varsigma^{\mathcal{S}} = \varsigma^{\mathcal{S}'}$ for every symbol ς of $\mathcal{V}$.

Let ϕ' be obtained from ϕ by replacing each quantification $\exists x.\psi$ by $\exists x.(M(x) \wedge \psi)$ and $\forall x.\psi$ by $\forall x.(M(x) \Longrightarrow \psi)$. By an easy induction over ϕ, $\mathcal{S} \models \phi$ is equivalent to $\mathcal{S}' \models \phi'$, and in particular, ϕ has a finite model if and only if the formula

$$\exists M.\{[\forall x \neq 0.M(x) \Longrightarrow M(x-1)] \wedge [\exists y.\neg M(y)] \wedge M(0) \wedge \phi'\}$$

has a model of universe $\mathbb{N}$. □

5.2 The results

Recall that non-deterministic 2-counter automata are introduced in Definition 4.1.9. The undecidability of the halting problem for non-deterministic 2-counter automata is used to prove the undecidability of the satisfiability problem of the logics studied in this manuscript.

The next theorem states the undecidability result:

Theorem 5.2.1. *For $g \in \mathbb{I}$, the finite satisfiability of $\exists\mathsf{MSO}\Pi_2^2[+1, g]$, and the satisfiability of $\exists\mathsf{MSO}\Pi_2^2[+1, g]$ over $\mathbb{N}$, are undecidable.*

Proof. By Lemma 5.1.1 it suffices to prove the first claim. By Theorem 4.2.10, there exists a $\exists\mathsf{MSO}\Pi_2^2[+1, g]$-formula $\phi_{\mathcal{A}}$ such that $\mathsf{SP}(\phi_{\mathcal{A}}) \neq \mathsf{SP}(A)$. Hence $\mathsf{SP}(\phi_{\mathcal{A}}) \neq \emptyset$ if and only if $\mathcal{A}$ halts, which is undecidable [Min60]. □

This theorem admits the following corollary.

Corollary 5.2.2. *For every $g \in \mathbb{I}$, satisfiability of $\Pi_2^2[+1, g]$ over words is undecidable.*

The proof is exactly the same as the one of Corollary 4.2.7, hence it is not repeated.

Using the ideas of the reduction from Corollary 5.2.2 to Theorem 4.3.12 leads to the following theorem:

Theorem 5.2.3. *The finite satisfiability and the satisfiability over $\mathbb{N}$ of $\Pi_2[+1, f]$ are undecidable.*

Finally, using results of Chapters 3 and 4, the following result is obtained.

Theorem 5.2.4. *Let $d \in \mathbb{N}^{>0}$ and let R be a relation symbol with arity d. Let $\mathcal{S}$ be a $\{\mathbb{N}, <, +\mathbb{N}, R\}$-structure such that $R^{\mathcal{S}}$ is $\mathsf{FO}[+]$-definable and not $\mathsf{FO}[<, \mathrm{mod}]$-definable. The finite satisfiability of the logics $\exists\mathsf{MSO}\Pi_3[\mathbb{N}, <, +\mathbb{N}, R]$, as well as the satisfiability of $\exists\mathsf{MSO}\Pi_3[\mathbb{N}, <, +\mathbb{N}, R]$ over $\mathbb{N}$, are undecidable in $\mathcal{S}$.*

Proof. By Lemma 5.1.1, it suffices to consider the finite case.

As in the proof of Theorem 5.2.1, the undecidability of the satisfiability of the logic $\exists\mathsf{MSO}\Pi_3[\mathbb{N}, <, +\mathbb{N}, R]$ is proven by reducing the halting problem for non-deterministic 2-counter automata to this problem. By [Min60], the halting problem for non-deterministic 2-counter automata is undecidable.

Since $R^{\mathcal{S}}$ is $\mathsf{FO}[+]$-definable but not $\mathsf{FO}[<, \mathrm{mod}]$-definable, by Theorem 3.4.1 there exists an increasing $\Pi_2[<, +\mathbb{N}, R]$-definable function g with slope greater than 1.

Let $\mathcal{A}$ be a non-deterministic 2-counter automaton. By Theorem 4.2.10, there exists a $\exists\mathsf{MSO}\Pi_2[+1, g]$-formula $\phi_{\mathcal{A}}$ whose spectrum is $\mathsf{SP}(\mathcal{A})$; hence, which is finitely satisfiable if and only if $\mathsf{SP}(\mathcal{A})$ is non empty. Let $\psi_{\mathcal{A}}$ be $\phi_{\mathcal{A}}$ where $g(x; y)$ is replaced by its $\Pi_2[<, +\mathbb{N}, R]$-definition. Then the formula $\psi_{\mathcal{A}}$ belongs to $\exists\mathsf{MSO}\Pi_3[+1, g]$ and is finitely satisfiable if and only if $\mathcal{A}$ admits an halting computation. □

5.3 Conclusion

It is proven in this chapter that (finite) satisfiability of $\mathsf{FO}[<, R, (P_a)_{a\in A}]$ is undecidable for every set R which is $\mathsf{FO}[+]$-definable and not $\mathsf{FO}[<, \mathrm{mod}]$-definable. Similarly, (finite) satisfiability of $\mathsf{FO}[+1, f, (P_a)_{a\in A}]$ is undecidable if f is not bounded by any function of the form $n \mapsto n + c$, or if f is uninterpreted.

We see many directions for further research. We may want to minimize the number of alternations of quantifiers needed to get undecidability, and conversely to find an algorithm to decide those logics with one or two alternations.

Note that, in Part II, a new proof of Corollary 3.3.9 is given, with a polynomial-time algorithm.

Part II

Logic and automata

In this part, it is shown how to decide whether a set R given as a minimal automaton is definable in the logics $\mathsf{FO}[<,-,\mathrm{mod}]$, $\mathsf{FO}[<,\mathrm{mod}]$ or $\mathsf{FO}[+1,\mathrm{mod}]$. When the automata accepts non-negative numbers, the existence of a formula can be decided in time $O(n)$ where n is the number of states of the automaton. When the automaton accepts subsets of $\mathbb{Z}^d$, the complexity time is $O(n\log(n))$ (because some automata must then be minimized). This part is independent of Part I.

This problem can naively be solved, for automata accepting sets of non-negative integers, by combining algorithms already given in the literature, but with a greater computation time. Indeed idea similar to the one in [Muc03], but using the characterization of $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$ given in Theorem 3.3.1 instead of the one of $\mathsf{FO}[\mathbb{N},+]$, yields an algorithm for deciding whether the set is $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$-definable in time 4-EXP.

On the other hand a formula $\phi_{\mathcal{A}} \in \mathsf{FO}[\mathbb{N},+]$ of length $|Q|^{O(1)}$ which defines R can be computed by the algorithm of [Ler06]. Then it can be decided whether R is definable in a less expressive logic such as $\mathsf{FO}[\mathbb{N},<,\mathrm{mod}]$, $\mathsf{FO}[\mathbb{N},+1,\mathrm{mod}]$ or $\mathsf{FO}[\mathbb{N},<]$ using the algorithm of [Cho08, Theorem 10]. The whole algorithm runs in time 2-EXP.

The main results are obtained as follows. The problem is first reduced from integers to non-negative integers. For a formula ϕ in a logic studied in this part, its minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$ is described. A sequence of properties is given, which are satisfied by $\mathcal{A}_{\phi,\mathbb{N}}$. It is then proven that those properties characterize the set of deterministic minimal automata which accept a $\mathsf{FO}[<,\mathrm{mod}]$-definable set or a set definable in a less expressive logic considered in this part. Each of those properties can be checked in time $O(n)$. Then it is explained how those properties can be used to obtain a formula in this logic, and for some of those logics, it is shown that the formula's length is $O\left(n^3\log(n)\right)$.

An automaton accepting a set defined by a $\mathsf{FO}[<,\mathrm{mod}]$-definable set is given in Chapter 7. Its minimal automaton is then constructed in Chapter 8. The algorithm which accepts automata accepting $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable sets is given in Chapter 9. The algorithms which returns an existential formula of polynomial size which defines the set accepted by the automaton is given in Chapter 10.

Table of Contents

6 Introduction **105**

6.1 Logics . . . 105

6.1.1 Vocabularies . . . 105

6.2 A note about the algorithm . . . 106

6.2.1 Time Analysis . . . 106

7 From Formula to Automaton **107**

7.1 From $\mathbb{Z}$ to $\mathbb{N}$ . . . 107

7.1.1 Integers . . . 107

7.1.2 Formulas . . . 108

7.1.3 Languages . . . 112

7.1.4 Automata . . . 112

7.1.4.1 The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ . . . 115

7.1.4.2 The Algorithm $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$ . . . 116

7.2 Restricting the Logic . . . 117

7.2.1 The Automaton $\mathcal{A}$ and the Automata $\mathcal{A}_q$ . . . 117

7.2.1.1 From a Formula for $\overline{\mathcal{A}}^{\mathbb{N}}$ to Formulas for $\overline{\mathcal{A}_q}^{\mathbb{N}}$ . . . 118

7.2.1.2 From formulas for $\overline{\mathcal{A}_q}^{\mathbb{N}}$ to a formula for $\overline{\mathcal{A}}^{\mathbb{N}}$ . . . 120

7.2.2 Initially-Cyclic Automata . . . 125

7.2.2.1 The Fragment $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}(e,a,M)\right]/\nu$ . . . 125

7.2.2.2 The Fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$ . . . 128

7.2.3 Defining the Automaton $\mathcal{A}'_{\phi,\nu}$ . . . 132

7.3 Totally Ordered Partitions . . . 132

7.3.1 Totally Ordered Partitions . . . 133

7.3.1.1 Definition . . . 133

7.3.1.2 Image of $\tau\mathrm{op}^m_{\nu,\mathcal{V}_\iota'}$ . . . 136

7.3.1.3 $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$'s Product . . . 141

7.3.1.4 Adding ζ and β . . . 144
7.3.2 $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ . . . 148
7.3.2.1 Interpretation . . . 148
7.3.2.2 Quotients and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ . . . 150
7.3.3 Automata . . . 151
7.3.3.1 Examples . . . 151

8 The Minimal Automaton $\mathcal{A}_{\phi,\mathbb{N}}$ 155
8.1 Definitions . . . 155
8.1.1 Partially-Ordered Partition . . . 155
8.1.2 Relations over $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ . . . 156
8.1.3 Axiom and orders . . . 158
8.1.4 Relation between $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ . . . 159
8.1.5 Syntactically Equivalent States. . . . 160
8.2 Minimal element of each syntactical equivalence classes. . . . 162
8.2.1 $\sim_\phi$ and $\overset{\mathbb{OESB}}{\preccurlyeq}$ . . . 163
8.2.2 $\sim_\phi$ and $\overset{\mathbb{L}}{\preccurlyeq}$ . . . 170
8.2.3 $\sim_\phi$ and $\sqsubseteq$ . . . 190
8.3 The minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$ . . . 191
8.3.1 Examples . . . 192

9 The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ 195
9.1 New symbols . . . 196
9.1.1 The set of symbols $\mathbb{P}^d$ . . . 196
9.1.2 The left-inverse symbols . . . 197
9.1.3 The set of symbols $\mathbb{C}^d$ . . . 201
9.2 Characterization of states . . . 202
9.2.1 Studying loops. . . . 202
9.2.2 Studying $\mathbb{C}^d$-cycles and modular values . . . 208
9.3 From $\left(A_b^d\right)^*$ to $\mathcal{L}$-words . . . 210
9.3.1 From A_b^d to $\mathcal{L}$-words . . . 210
9.3.2 From $\left(A_b^d\right)^*$ to $\mathcal{L}$-words . . . 217
9.3.2.1 Moving symbols of the form $[\emptyset,K]$ . . . 220
9.3.2.2 Moving symbols of the form $[K;\emptyset]$ . . . 224
9.3.2.3 Partitioning the J_i's . . . 225
9.3.2.4 $\left(A_b^d\right)^*$ to $\mathcal{L}^*$ . . . 233
9.3.2.5 Proving Proposition 9.3.17 . . . 243
9.4 The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ . . . 243
9.4.1 The algorithm . . . 245

10 The algorithm *CEF'*($\mathcal{V}_\iota^{\mathbb{N}}$) **247**
10.1 A polynomial-time algorithm for a fixed dimension d. 247
10.1.1 The algorithm 247
10.1.2 Reducing the set of consider states 248
10.2 Considering $\mathbb{O}$, $\mathbb{E}$, $\mathbb{S}$ and $\mathbb{B}$ 249
10.2.1 The $\mathbb{E}_P$ and $\mathbb{S}_P$ 249
10.2.2 Strongly connected component 249
10.2.3 Encoding of $\mathbb{L}$: $\leq$ or $<$ 251
10.3 The modular part 252
10.3.1 $[I;\emptyset]$-cycles and LoopSize(C,E) 253
10.3.2 Set of modular parts 256
10.3.3 Computing the modular part 258
10.3.4 Defining $\Downarrow_{\phi,C}$ 261
10.4 The algorithm 263
10.4.1 Associating a language to a state 263
10.4.2 The algorithm 264

11 Conclusion **267**
11.0.3 Considering other vocabularies 267
11.0.4 The algorithm 268
11.1 Open questions 269
11.1.1 Deciding other classes of set 269
11.1.2 Writing a polynomial-size $\Sigma_0[\mathbb{N},<,+\mathbb{N},\mathrm{mod}\,\mathbb{N}]/\nu$-formula 270
11.1.3 Sequential automaton 270
11.1.4 Automaton over reals 270
Index of Part II 271

Chapter 6

Introduction

The logics considered in this part are given in Section 6.1. The presentation of the algorithm is discussed in Section 6.2.

6.1 Logics

The logics studied in this part and the relations between them are introduced in this section. No new result is presented in this section.

In this part, the minimal automaton which accepts the set defined by a logical formula is characterized. For this, the set of formulas is restricted, hence a sequence of reductions is applied to formulas. Let ϕ be an arbitrary $\mathsf{FO}[\mathcal{V}]$-formula where $\mathcal{V}$ is a vocabulary studied in this part.

- In Section 2.2.2, Definition 2.2.17 explains how to eliminate the quantifiers.
- In Section 7.1, Lemma 7.1.4 transforms formulas interpreted over $\mathbb{Z}$ into formulas interpreted over $\mathbb{N}$.
- In Section 7.2, Corollary 7.2.21 explains how to reduce the problem to a special form of formulas, with a finite number of non-modular relations.
- Finally, in the same Section, Proposition 7.2.31 adds a syntactical restriction to the set of formulas that must be considered, such that the minimal automaton accepting a set defined by such a formula is initially-cyclic.

It should be noted that quantifier elimination adds relations to the vocabulary. On the other hand every other result mentioned in the previous paragraph restricts the vocabulary and the set of formulas. The first and the last considered logics use the same vocabulary. But those operations do not cancel each other, and the formula obtained after all those transformations is not similar to the former one.

6.1.1 Vocabularies

The next definition gives the exhaustive set of vocabularies that are studied in this part.

Definition 6.1.1. Let $\mathbb{V}$ be the set of vocabularies $\mathcal{V}$ given in Table 6.1.

Let $\mathbb{V}^{\mathbb{Z}}$ (respectively, $\mathbb{V}^{\mathbb{N}}$) be the set of vocabularies of $\mathbb{V}$ which contain (respectively, do not contain) $\mathbb{Z}$>.

Name	Over $\mathbb{Z}$	Name	Over $\mathbb{N}$
$\mathcal{V}_0^{\mathbb{Z}}$	$\{\doteq\mathbb{Z}, \doteq, <, +\mathbb{N}, \mathbb{Z}-, \mathbb{Z}>, <-, \mathrm{mod}\}$		
$\mathcal{V}_1^{\mathbb{Z}}$	$\{\doteq\mathbb{Z}, \doteq, <, +\mathbb{N}, \quad \mathbb{Z}>, \quad \mathrm{mod}\}$	$\mathcal{V}_1^{\mathbb{N}}$	$\{\doteq\mathbb{N}, \doteq, <, +\mathbb{N}, \mathrm{mod}\}$
$\mathcal{V}_2^{\mathbb{Z}}$	$\{\doteq\mathbb{Z}, \doteq, \quad +\mathbb{N}, \quad \mathbb{Z}>, \quad \mathrm{mod}\}$	$\mathcal{V}_2^{\mathbb{N}}$	$\{\doteq\mathbb{N}, \doteq, \quad +\mathbb{N}, \mathrm{mod}\}$

Table 6.1: Vocabularies

The set of vocabularies of $\mathbb{V}^{\mathbb{Z}}$ and of $\mathbb{V}^{\mathbb{N}}$ are given in the second and fourth columns of Table 6.1 respectively. When $\mathcal{V}_\iota^{\mathbb{N}} \in \mathbb{V}^{\mathbb{N}}$ and $\mathcal{V}_\iota^{\mathbb{Z}} = \mathcal{V}_\iota^{\mathbb{N}} \cup \{\mathbb{Z}>\} \in \mathbb{V}^{\mathbb{Z}}$, those two vocabularies appear on the same line. In this case, they also have the same index assigned to them.

6.2 A note about the algorithm

The proof of the algorithm is longer than the algorithm itself. Let us say a word about which part of the part is about the algorithm and which part is about its proof. Readers whose only interest is the algorithm may skip the part about the proof.

The definitions used in the algorithm are preceded by a star. The main algorithms of the part are clearly marked as algorithms. Some easy subroutines are given in lemmas, where the algorithm is simultaneously given and proven. Those lemmas are also preceded by a star. Section 11.1.4 contains the list of definitions and lemmas needed by the algorithm, and the list of algorithms.

6.2.1 Time Analysis

In this section the notion of time complexity are discussed. For the sake of simplicity, it is assumed that:

- all basic arithmetic operations, such as addition, multiplication, subtraction, comparison of integers, can be computed in constant time,
- creating an array, accessing to an element of the array and changing it takes constant time,
- for any automaton $A = (Q, A, \delta, q_0, F)$, the transition function δ returns in time $O(d)$,
- for $n \in \mathbb{N}$ and $I, J \subseteq [n-1]$, computing the subsets of $[n-1]$ which are Boolean combinations of I and J runs in time $O(n)$.

Chapter 7

From Formula to Automaton

In this part, an automaton $\mathcal{A}'_{\phi,\nu}$ is described, which accepts the same language as a formula ϕ belonging to a logic considered in this part.

The problem is reduced from $\mathbb{Z}$ to $\mathbb{N}$ in Section 7.1. The set of considered formulas is restricted to a simpler set in Section 7.2. An automaton $\mathcal{A}'_{\phi,\nu}$ which accepts ϕ is constructed in Section 7.3.

7.1 From $\mathbb{Z}$ to $\mathbb{N}$

Automata accepting sets of integers are considered in this section. It is easier to study automata reading non negative integers than automata reading integers. Hence, the first step of our algorithm is to reduce the problem over $\mathbb{Z}$ to a finite number of instances of a similar problem over $\mathbb{N}$. The number of instances is linear in the size of the alphabet.

More precisely, the computation problems considered over $\mathbb{Z}$ is reduced to more general ones over $\mathbb{N}$. Those new problems over $\mathbb{N}$ also take as input a parameter ν which is a subset of $[d-1]$. The values of ν correspond to the indices of negative components of a tuple of variables interpreted in $\mathbb{Z}^d$.

Hence, every algorithm given in the following sections are correct over $\mathbb{N}$ when ν is assumed to be the empty set, as there are no negative components. For the same reason, the "positive quantifier" and "negative quantifier" introduced in Definition 7.1.2 $\exists^-$ can be ignored. It suffices to replace $\exists^+$ by $\exists$. Note that no $\exists^-$ appears in formula when $\nu \neq \emptyset$.

Apart from $\exists^-$ and ν, the following sections do not uses any notion introduced in this section, hence those sections can be read independently from this section. In particular the algorithms of the following sections are independent of the algorithms of this section.

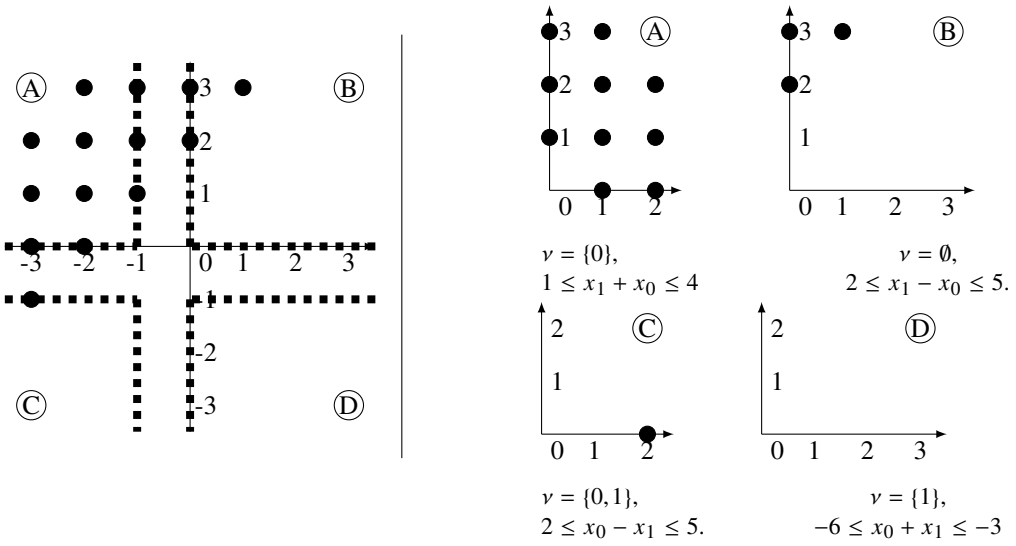
7.1.1 Integers

In this section, it is explained how to reduce sets of tuples of integers to sets of tuples of non-negative integers.

The set $\mathbb{Z}$ is naturally partitioned into $\mathbb{N} = \{0, 1, 2, \dots\}$ and $\mathbb{Z}^{<0} = \{-1, -2, -3, \dots\}$. More generally $\mathbb{Z}^d$ can be partitioned into 2^d sets $(\mathbb{N}_\nu)_{\nu \subseteq [d-1]}$ with

$$\mathbb{N}_\nu = \Big\{ \boldsymbol{n} \in \mathbb{Z}^d \mid n_i < 0 \Longleftrightarrow i \in \nu, \text{ for each } i \in [d-1] \Big\}.$$

The tuples $\boldsymbol{x}$ considered later in this part are such that $x_i < 0$ if and only if $i \in \nu$, hence ν represents the set of indices of the negative integers of the tuple. More generally, each set $R \subseteq \mathbb{Z}^d$ is partitioned into 2^d sets, $R \cap \mathbb{N}_\nu$.



(a) $R \subseteq \mathbb{Z}^2$, $2 \leq x_1 - x_0 \leq 5$ (b) The R_ν's.

Figure 7.1: Set of integers and of non-negative integers.

***Definition 7.1.1** ($\overline{f}_\nu$)**.** Let $\overline{f}_\nu : \mathbb{Z}^d \to \mathbb{Z}^d$ be such that for $\boldsymbol{n} \in \mathbb{Z}^d$, $\overline{f}_\nu(n)$ is the d-tuple whose i-th component is n_i if $i \notin \nu$ and $-1 - n_i$ otherwise.

The function $\overline{f}_\nu$ is its own inverse. For $R \subseteq \mathbb{Z}^d$, let $R_\nu = \left\{\boldsymbol{n} \in \mathbb{N}^d \mid \overline{f}_\nu(\boldsymbol{n}) \in R\right\}$. For example, Figure 7.1a shows a set $R \subseteq \mathbb{Z}^2$, the dashed lines represent the boundary of the $\mathbb{N}_\nu$. Then Figure 7.1b represents the sets $R_\nu \subseteq \mathbb{N}^2$ for all $\nu \subseteq \{0,1\}$.

7.1.2 Formulas

The relation between formulas which define sets of tuples of integers and formulas which define the sets of non-negative integers as defined in Section 7.1.1 are studied in this section.

Let $R \subseteq \mathbb{Z}^d$. Let (*) denote the property "each R_ν is $\mathsf{FO}[\doteq 0, <, \mathrm{mod}]$-definable". Lemma 7.1.4 below proves that (*) is a characterization of "R is $\mathsf{FO}[\doteq 0, <, -, \mathrm{mod}]$-definable"; note that the symbol $-$ is added. In order to characterize "R is $\mathsf{FO}[\doteq 0, <, \mathrm{mod}]$-definable", without the symbol $-$, a restriction is added to the logic $\mathsf{FO}[\doteq 0, <, \mathrm{mod}]$. This restriction is introduced in Definition 7.1.2.

An example is first given. Let $R \subseteq \mathbb{Z}^2$ be defined by the formula $x_0 \doteq -x_1$, then R_ν for $\nu = \{1\}$ is defined by the formula $x_0 \doteq x_1 + 1$. Reciprocally if an equality relation occurs between x_0 and x_1 in the definition of R_ν, with $0 \notin \nu$ and $1 \in \nu$, this equality is an indication that a symbol "$-$" should occur in the formula defining R. Hence, to consider vocabularies without the minus function, the usage of the symbol "$\doteq$" is forbidden between x_i and x_j when $i \in \nu \Longleftrightarrow j \notin \nu$. And more generally, no binary relation can have both of those variables as arguments.

***Definition 7.1.2** (Polarity)**.** Let $\nu \subseteq [d-1]$ be fixed. The *polarity* of a variable x_i is now introduced. The polarity of the variable x_i is *positive* (respectively, *negative*) if $i \notin \nu$, (respectively, $i \in \nu$). Then $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ is the restriction of the set of $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]$-formulas where $x_i < x_j$ and $x_i + c \doteq x_j$ can occur only if x_i and x_j have the same polarity.

The class of formula $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ for an integer $p \geq 1$ is defined similarly, but there are two existential quantifiers, $\exists^+$ and $\exists^-$. The first (respectively, second) quantifier introduces positive (respectively,

negative) variables.

A notation is now introduced for quantification of d-tuples of positive and negative variables.

***Definition 7.1.3** ($\exists^\nu$)**.** Let $\exists^\nu \boldsymbol{y}$ be an abbreviation for $\exists^{\pm(0)} y_0, \ldots, \exists^{\pm(d-1)} y_{d-1}$ where $\pm(i)$ is $-$ if $i \in \nu$ and is $+$ otherwise.

The two following statements are not used in this manuscript, hence not proved. Note that Proposition 2.2.19 also holds for $\mathsf{FO}\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, the proof is similar.

The class of $\mathsf{FO}[<, \mathrm{mod}\, m]/\nu$-definable sets admits a characterization similar to the characterization of the class of $\mathsf{FO}[<, \mathrm{mod}\, m]/$-definable sets given in Theorem 3.3.1: it suffices to reformulate the Condition b. of Theorem 3.3.1 in "Let $\boldsymbol{p}, \boldsymbol{p'} \in \mathbb{N}^d$ be such that $p_i = 0$ and $p'_i = m$ if $i \notin \nu$ and $p_i = m$ and $p'_i = 0$ otherwise. There exists $t \in \mathbb{N}$ such that R is $\boldsymbol{p}$- and $\boldsymbol{p'}$-periodic in $(\mathbb{N}^{\geq t})^d$."

It should be noted that the set of $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]$-formulas is exactly the set of $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\emptyset$-formulas, hence results about the fragment $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ holds if and only this result holds on $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]$ with $\nu = \emptyset$.

Two lemmas are now given, which explain formally the relation between the formula which defines R and the ones which define R_ν for $\nu \subseteq [d-1]$.

Lemma 7.1.4. *Let $R \subseteq \mathbb{Z}^d$ be a set. If R is defined by a $\Sigma_0\left[\mathcal{V}_0^{\mathbb{Z}}\right]$-formula, then for all $\nu \subseteq [d-1]$, the set R_ν is defined by a $\Sigma_0\left[\mathcal{V}_1^{\mathbb{N}}\right]$-formula.*

If R is defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula for ι being 1 or 2, then for all $\nu \subseteq [d-1]$, R_ν is defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula.

The main difference between the two cases is that the "$/\nu$" is used only in the second case, when the symbol $-$ does not belong to the vocabulary.

An example of the result is given before proving the general case.

Example 7.1.5. Let ϕ be $x_0 + 1 \doteq x_1$ and consider the base $b = 2$. For every $\nu \subseteq \{0,1\}$, we give the formula $\phi_\nu(x_0, x_1)$, the automaton $\mathcal{A}_{\phi_\nu(x_0,x_1)}$ that accepts the set defined by this formula and the language accepted by this automaton.

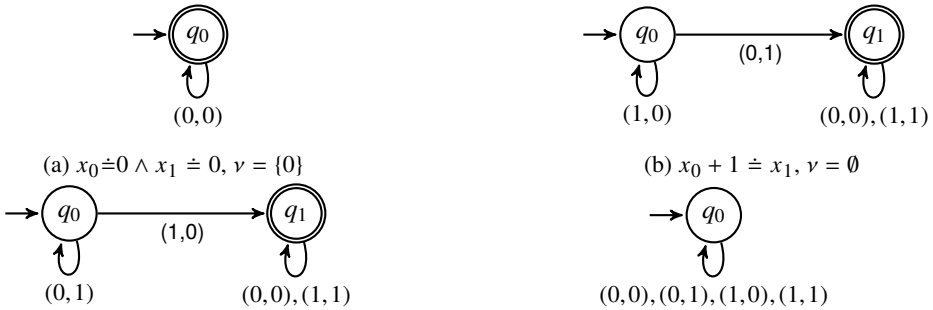
- For $\nu = \{0\}$, the formula ϕ_ν is $x_0 \doteq 0 \wedge x_1 \doteq 0$. Then $\underline{\phi_\nu}_{\mathbb{N}}$ is described by $(0,0)^*$ and is accepted by the automaton pictured in Figure 7.2a.
- For $\nu = \emptyset$, the formula ϕ_ν is $x_0 \doteq x_1 + 1$. Then $\underline{\phi_\nu}_{\mathbb{N}}$ is described by

  $$(1,0)^*(0,1)[(0,0) + (1,1)]^*$$

  and is accepted by the automaton pictured in Figure 7.2b.
- For $\nu = \{0,1\}$, the formula ϕ_ν is $x_0 \doteq x_1 - 1$. Its language and automaton are the same than the preceding but with the pairs $(0,1)$ and $(1,0)$ switched. That is, $\underline{\phi_\nu}_{\mathbb{N}}$ is described by

  $$(0,1)^*(1,0)[(1,1) + (0,0)]^*$$

  and is accepted by the automaton pictured in Figure 7.2c.
- Finally, for $\nu = \{1\}$, the formula ϕ_ν is False, and its language is accepted by the automaton pictured in Figure 7.2d.



(a) $x_0 \doteq 0 \wedge x_1 \doteq 0$, $\nu = \{0\}$ (b) $x_0 + 1 \doteq x_1$, $\nu = \emptyset$

(c) $x_0 \doteq x_1 + 1$, $\nu = \{0,1\}$ (d) false, $\nu = \{1\}$

Figure 7.2: $(x_0 + 1 \doteq x_1)_\nu$ for every $\nu \subseteq \{0,1\}$

Proof. Let $\mathcal{V}_\iota^{\mathbb{Z}} \in \mathbb{V}^{\mathbb{Z}}$ with $\iota > 0$. Let $R \subseteq \mathbb{Z}^d$ be a set defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula $\phi(\boldsymbol{x})$. Then R_ν is defined by $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ with $\overline{f}_\nu$ as in Definition 7.1.1. That is: $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ is obtained from $\phi(\boldsymbol{x})$ by replacing each occurrence of x_i by $-1 - x_i$ for all $i \in \nu$.

It must be checked that $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ is a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ formula. Formally, $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ is obtained from ϕ by rewriting the atomic formulas of ϕ as in Table 7.1. The formula $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ belongs to $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, as

if		$\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$, for x_i positive, is	$\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ for x_i negative, is
ϕ is $x_i \doteq c$	for $c \in \mathbb{Z}$	$x_i \doteq c$,	$x_i \doteq -c - 1$,
ϕ is $x_i \doteq x_j + c$	for $c \in \mathbb{N}$ and x_j positive	$x_i \doteq x_j + c$,	false,
ϕ is $x_i \doteq x_j + c$	for $c \in \mathbb{N}$ and x_j negative	$\bigvee_{e=0}^{c-1}\left(x_j \doteq d \wedge x_i \doteq c - 1 + e\right)$,	$x_i \doteq x_j - c$,
ϕ is $x_i \equiv c \mod m$	for $m \in \mathbb{N}$ and $c \in [m-1]$	$x_i \equiv c \mod m$,	$x_i \equiv -c - 1 \mod m$,
ϕ is $x_i < x_j$,	for x_j positive	$x_i < x_j$,	true,
ϕ is $x_i < x_j$,	for x_j negative	false,	$x_i > x_j$,
ϕ is $x_i < c$	for $c \in \mathbb{Z}$	$\bigvee_{j=0}^{c-1} x_i \doteq j$,	$\bigvee_{j=-c}^{-1} x_i \doteq j$,
ϕ is $x_i \doteq c - x_j$	for $c \in \mathbb{Z}$ and x_j positive	$\bigvee_{h=0}^{c} x_j \doteq h \wedge x_i \doteq c - h$,	$x_i \doteq x_j - c - 1$,
ϕ is $x_i \doteq c - x_j$	for $c \in \mathbb{Z}$ and x_j negative	$x_i \doteq x_j + c + 1$,	false

Table 7.1: $\phi(\overline{f}_\nu(\boldsymbol{x}))$

in Definition 7.1.2.

- For $i \in \nu \Longleftrightarrow j \notin \nu$, the formulas $x_i < x_j$ and $x_i \doteq x_j + c$ occur in $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ only if $-$ belongs to the vocabulary, that is if $\mathcal{V}_\iota^{\mathbb{Z}} = \mathcal{V}_0^{\mathbb{Z}}$.
- And the formula $x_i < x_j$ occurs in $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ only if $x_i < x_j$ or $x_i > x_j$ occur in ϕ.

The proof for $\mathcal{V}_0^{\mathbb{Z}}$ is similar, but does not require the restrictions on ν to be satisfied.

□

The previous lemma computes a definition of the sets R_ν, from the definition of any set $R \subseteq \mathbb{Z}^d$. The converse result, computing a definition of R given the definitions of R_ν, is done in the following lemma.

More precisely, the next lemma is about any logic Σ_p for $p \in \mathbb{N}$ and not only Σ_0. Indeed, on the one hand, Lemma 7.1.4 is used to characterize the minimal automaton $\mathcal{A}_{\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)}$ for ϕ a formula. By

Proposition 2.2.21, there is no loss of generality in assuming that ϕ is quantifier-free. On the other hand, Lemma 7.1.6 is used to construct a formula ϕ from the formulas $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$, and the algorithms of this part generate quantifier-free formulas whose length are not not polynomially-bounded, and formulas the size of which is polynomially-bounded, which are not quantifier-free.

***Lemma 7.1.6** (From $\mathbb{N}$ to $\mathbb{Z}$)**.** Let $p \in \mathbb{N}$, $R \subseteq \mathbb{Z}^d$ and ι be 1 or 2.

If R_ν is defined by a $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula of length s for all $\nu \subseteq [d-1]$, then the set R is defined by a $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula of length $O\left(2^d(s+d)\right)$ and computable in time $O\left(2^d(s+d)\right)$.

If R_ν is defined by a $\Sigma_p\left[\mathcal{V}_1^{\mathbb{N}}\right]$-formula of length s for all $\nu \subseteq [d-1]$, then the set R is defined by a $\Sigma_p\left[\mathcal{V}_0^{\mathbb{Z}}\right]$-formula of length $O\left(2^d(s+d)\right)$.

An example of the result is given before proving the general case.

Example 7.1.7 (Resuming Example 7.1.5)**.** Using the formulas $\phi\left(\overline{f}_\nu(\boldsymbol{x})\right)$ of Example 7.1.5, by Lemma 7.1.6, the set R is defined by:

$$\begin{array}{l}\{x_0 < 0 \wedge x_1 \geq 0 \wedge \quad x_0 \doteq -1 \wedge x_1 \doteq 0\ \} \vee \{x_0 \geq 0 \wedge x_1 \geq 0 \wedge x_0 \doteq x_1 + 1\} \vee \\ \{x_0 < 0 \wedge x_1 < 0 \wedge -x_0 - 1 \doteq -x_1 - 1 + 1\} \vee \{x_0 \geq 0 \wedge x_1 < 0 \wedge \quad \text{False} \quad\}.\end{array}$$

Lemma 7.1.6 is now proved.

Proof. Let $R \subseteq \mathbb{Z}^d$. Let us assume that R_ν is defined by a $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula $\phi(\boldsymbol{x})$ of length s for ι being 1 or 2 and $\nu \subseteq [d-1]$.

Then the set accepted by the automaton is defined by the $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula of length $O\left(2^d(s+d)\right)$:

$$\bigwedge_{\nu \subseteq [d-1]} \left[\left(\bigwedge_{i \in \nu} x_i \geq 0 \wedge \bigwedge_{i \notin \nu} x_i < 0 \right) \Longrightarrow \phi_\nu\left(\overline{f}_\nu(\boldsymbol{x})\right) \right]$$

It remains to show that the formula $\phi_\nu(\overline{f}_\nu(x))$ belongs to $\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$. For this it is enough to study how the different atomic formulas are replaced. The recursive algorithm is given in Table 7.2.

		$\phi_\nu\left(\overline{f}_\nu(\boldsymbol{x})\right)$ is	
if		and if x_i is positive	and if x_i is negative
ϕ is $x_i \doteq c$	for $c \in \mathbb{N}$	$x_i \doteq c$,	$x_i \doteq -c-1$
ϕ is $x_i \equiv c \mod m$	for $m \in \mathbb{N}$ and $c \in [m-1]$	$x_i \equiv -c-1 \mod m$	$x_i \equiv c \mod m$,
ϕ is $x_i < x_j$	for x_j positive	$x_i < x_j$	$x_i \geq -x_j$,
ϕ is $x_i < x_j$	for x_j negative	$x_i \leq -x_j$	$x_i > x_j$
ϕ is $x_i \doteq x_j + c$	for $c \in \mathbb{N}$ and x_j positive	$x_i \doteq x_j + c$,	$x_i \doteq -c-1-x_j$
ϕ is $x_i \doteq x_j + c$	for $c \in \mathbb{N}$ and x_j negative	$x_i \doteq c-1-x_j$,	$x_i \doteq x_j - c$,
ϕ is $x_i \doteq c - x_j$	for $c \in \mathbb{N}$ and x_j positive	$x_i \doteq c - x_j$,	$x_i \doteq -c-1+x_j$
ϕ is $x_i \doteq c - x_j$	for $c \in \mathbb{N}$ and x_j negative	$x_i \doteq x_j + c + 1$,	$x_i \doteq c - x_j$

Table 7.2: $\phi_\nu(\overline{f}_\nu(\boldsymbol{x}))$

If $\mathcal{V}_\iota^{\mathbb{Z}}$ is different from $\mathcal{V}_0^{\mathbb{Z}}$ then there is no atomic formula $x_i < x_j$ or $x_i \doteq x_j + c$, when x_i and x_j have the same polarity, so the symbol $-$ does not occur in $\phi_\nu\left(\overline{f}_\nu((\boldsymbol{x})\right)$.

Checking the computation time is trivial, as it is linear in the length of the formulas and consists in the application of simple rewriting rules.

The other case, where R_ν is defined by a $\Sigma_p\left[\mathcal{V}_1^{\mathbb{N}}\right]$-formula, is similar. Indeed,

$$\bigwedge_{\nu\subseteq[d-1]}\left[\left(\bigwedge_{i\in\nu}x_i\geq 0\wedge\bigwedge_{i\notin\nu}x_i<0\right)\Longrightarrow\phi_\nu\left(\overline{f}_\nu(\boldsymbol{x})\right)\right]$$

is a $\Sigma_p\left[\mathcal{V}_0^{\mathbb{Z}}\right]$-formula. □

7.1.3 Languages

The relation between the base b representation of two integers of the form n and $-1-n$ is studied in this section. More generally, the base b representation of $\boldsymbol{n}$, and the one of $\overline{f}_\nu(\boldsymbol{n})$ for $\nu\subseteq[d-1]$ and $\boldsymbol{n}\in\mathbb{Z}^d$, are studied.

The function that sends the representation of n to the representation of $-1-n$ in base b is now introduced.

***Definition 7.1.8** ($\underline{f}$ and $\underline{f}_\nu$)**.** Let $\underline{f}:[b-1]^*\to[b-1]^*$ be the morphism that sends the letter $a\in[b-1]$ to the letter $b-1-a\in[b-1]$.

Let $\underline{f}_\nu:\left(A_b^d\right)^*\to\left(A_b^d\right)^*$ be the morphism such that, for each $\boldsymbol{a}\in A_b^d$ and for $i\in[d-1]$, then $\boldsymbol{c}=\underline{f}_\nu(\boldsymbol{a})$ is such that c_i is $\underline{f}(a_i)$ if $i\in\nu$ and a_i otherwise.

Note that $\underline{f}_\nu$ sends sign letters to sign letters. The function $\underline{f}$ corresponds to a basic property in b-complement notation:

Lemma 7.1.9 ([CSRL01])**.** *Let* $\boldsymbol{w}\in[b-1]^*\cdot\{0,b-1\}$*, then* $\overline{\underline{f}(w)}^{\mathbb{Z}}=-\overline{w}^{\mathbb{Z}}-1$.

Hence, $\overline{\underline{f}_\nu(\boldsymbol{w})}^{\mathbb{Z}}=\overline{f}_\nu\left(\overline{\boldsymbol{w}}^{\mathbb{Z}}\right)$ for $\boldsymbol{w}\in\left(A_b^d\right)^*\{0,b-1\}^d$. Equivalently, $\underline{\overline{f}_\nu(\boldsymbol{n})_{\mathbb{Z}}}=\underline{f}_\nu\left(\underline{\boldsymbol{n}}_{\mathbb{Z}}\right)$ for all $\boldsymbol{n}\in\mathbb{Z}^d$.

Hence, similarly to Lemma 7.1.6, if $\underline{R_{\nu_{\mathbb{N}}}}$ is described by the regular expression ρ_ν, then $\underline{R}_{\mathbb{Z}}$ is described by $\sum_{\nu\subseteq[d-1]}\underline{f}_\nu(\rho_\nu\mathbf{0})$ where $\underline{f}_\nu(\rho)$ is the regular expression ρ where $\underline{f}_\nu$ is applied to each letter. Example 7.1.5 is now resumed, giving the regular expression and an automaton which accepts the set of this example.

Example 7.1.10 (Example 7.1.5)**.** Let $R=\{(x,y)\mid x+1\doteq y\}$, and consider the base $b=2$, as in Example 7.1.5. For all $\nu\subseteq\{0,1\}$, a regular expression and an automaton which accepts $\underline{R_\nu}$ are given in Example 7.1.5. Using those expressions for $\underline{\phi_\nu}_{\mathbb{Z}}$, the set $\underline{R}_{\mathbb{Z}}$ is described by the following regular expression:

$$\begin{aligned}
\underline{R}_{\mathbb{Z}} = {} & \underline{f}_{\{0\}}((0,0)^*\cdot(0,0)) && + \underline{f}_{\emptyset}((1,0)^*\cdot(0,1)\cdot[(0,0)+(1,1)]^*\cdot(0,0))\\
& +\underline{f}_{\{0,1\}}((0,1)^*\cdot(1,0)\cdot[(1,1)+(0,0)]^*\cdot(0,0)) && +\underline{f}_{\{1\}}(\emptyset\cdot(0,0))\\
= {} & ((1,0)^*\cdot(1,0)) && + ((1,0)^*\cdot(0,1)\cdot[(0,0)+(1,1)]^*\cdot(0,0))\\
& + ((1,0)^*\cdot(0,1)\cdot[(0,0)+(1,1)]^*\cdot(1,1)) && + (\emptyset\cdot(0,1))\\
= {} & (1,0)^*\cdot\{(0,1)\cdot[(0,0)+(1,1)]^+ && + (1,0)\}
\end{aligned}$$

This language is described by the automaton of Figure 7.3.

7.1.4 Automata

This section considers the relation between an automaton over $\mathbb{Z}$ which accepts a language representing a set R of tuples of integers, and the automata over $\mathbb{N}$ which accept the different sets R_ν of tuples of non-negative numbers.

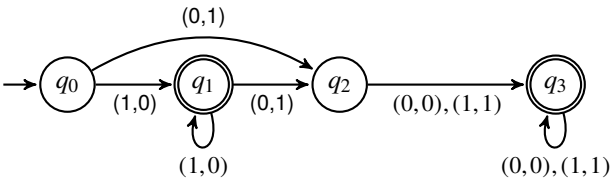


Figure 7.3: $x_0 + 1 \doteq x_1$ over $\mathbb{Z}$

***Lemma 7.1.11** (Automaton over $\mathbb{Z}$ to automata over $\mathbb{N}$)**.** Let $\mathcal{A}$ be an automaton over $\mathbb{Z}$ with n states. Let $\nu \subseteq [d-1]$. The set $(\overline{\mathcal{A}}^{\mathbb{Z}})_\nu$ is accepted by a automaton $\mathcal{A}_\nu$ with n states. Moreover the automaton $\mathcal{A}_\nu$ is computable from $\mathcal{A}$ in linear time.

Proof. Let $R \subseteq \mathbb{Z}^d$ be a set accepted by an automaton $\mathcal{A} = (Q, A, \delta, q_0, F)$. Let $\nu \subseteq [d-1]$. Let us construct an automaton $\mathcal{A}_\nu = \left(Q, A_b^d, \delta_\nu, q_0, F_\nu\right)$ with n states such that $\overline{\mathcal{A}_\nu}^{\mathbb{N}} = R_\nu$.

For each $q \in Q$, $a \in A_b^d$, let $\delta_\nu(q, \boldsymbol{a}) = \delta(q, \underline{f}_\nu(\boldsymbol{a}))$. Let (*) denote the property: for each $w \in \left(A_b^d\right)^*$, $\delta_\nu(q, \boldsymbol{w}) = \delta(q, \underline{f}_\nu(\boldsymbol{w}))$. It is proven by an easy induction on $|\boldsymbol{w}|$. Let

$$F_\nu = \left\{q \in Q \mid \delta(q, \underline{f}_\nu(\mathbf{0})) \in F\right\}.$$

It is now proven that $\mathcal{A}_\nu$ is an automaton over $\mathbb{N}$ as in Definition 2.3.6, that is $q \in F$ is equivalent to $\delta(q, \mathbf{0}) \in F$ for all states q. It should be noted that, since $\mathcal{A}$ is an automaton over $\mathbb{Z}$, that is $\delta(q, \boldsymbol{a}) \in F$ is equivalent to $\delta(q, \boldsymbol{aa}) \in F$ for every $q \in Q$ and for every sign letter $\boldsymbol{a} \in \{0, b-1\}^d$.

Let $q \in Q$, then:

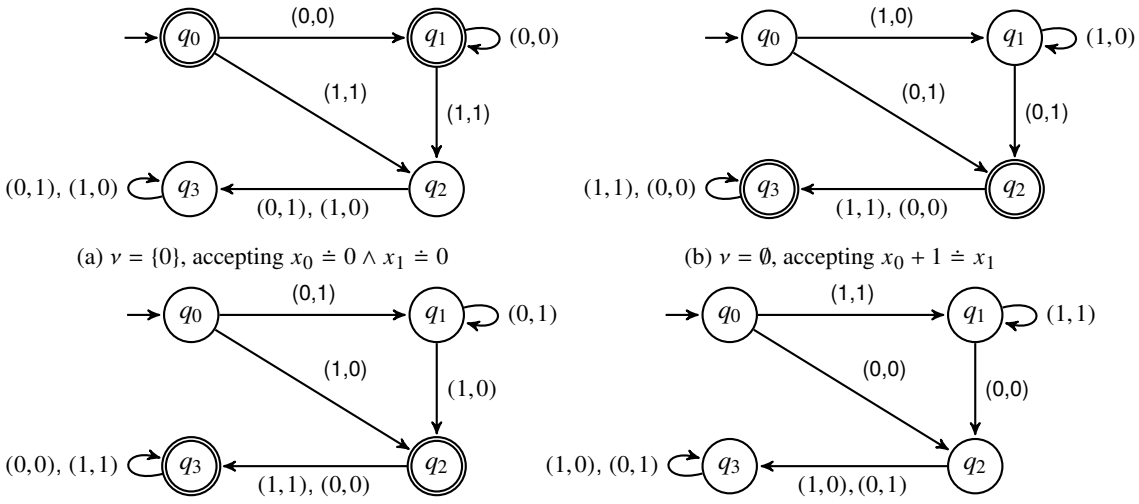
$$\begin{aligned}
q \in F_\nu &\iff \delta(q, \underline{f}_\nu(\mathbf{0})) &&\in F && \text{(using the definition of } F_\nu\text{)} \\
&\iff \delta(q, \underline{f}_\nu(\mathbf{0})\underline{f}_\nu(\mathbf{0})) &&\in F && \text{(using Definition 2.3.6)} \\
&\iff \delta(q, \mathbf{0}) &&\in F && \text{(using the definition of } F_\nu\text{)}
\end{aligned}$$

Let us prove that $\overline{\mathcal{A}_\nu}^{\mathbb{N}} = \left(\overline{\mathcal{A}}^{\mathbb{Z}}\right)_\nu$. Let $\boldsymbol{w} \in \left(A_b^d\right)^*$, It is now proven that $\boldsymbol{w}$ is accepted by $\mathcal{A}_\nu$ if and only if $\overline{\boldsymbol{w}}^{\mathbb{N}}$ belongs to $\left(\overline{\mathcal{A}}^{\mathbb{Z}}\right)_\nu$. Then:

$$\begin{aligned}
\overline{\boldsymbol{w}}^{\mathbb{N}} \in \overline{\mathcal{A}_\nu}^{\mathbb{N}} &\iff \delta_\nu(q_0, \boldsymbol{w}) \in F_\nu && \text{(using Definition 2.3.6)} \\
&\iff \delta(q_0, \underline{f}_\nu(\boldsymbol{w})) \in F_\nu && \text{(Using property } (*)\text{)} \\
&\iff \delta(q_0, \underline{f}_\nu(\boldsymbol{w}\mathbf{0})) \in F && \text{(using the definition of } F_\nu\text{)} \\
&\iff \overline{\underline{f}_\nu(\boldsymbol{w}\mathbf{0})}^{\mathbb{Z}} \in \left(\overline{\mathcal{A}}^{\mathbb{Z}}\right) && \\
&\iff \overline{f}_\nu\left(\overline{\boldsymbol{w}\mathbf{0}}^{\mathbb{Z}}\right) \in \left(\overline{\mathcal{A}}^{\mathbb{Z}}\right) && \text{(using Lemma 7.1.9)} \\
&\iff \overline{\boldsymbol{w}\mathbf{0}}^{\mathbb{Z}} \in \left(\overline{\mathcal{A}}^{\mathbb{Z}}\right)_\nu && \left(\text{using the definition of } \left(\overline{\mathcal{A}}^{\mathbb{Z}}\right)_\nu\right) \\
&\iff \overline{\boldsymbol{w}}^{\mathbb{N}} \in \left(\overline{\mathcal{A}}^{\mathbb{Z}}\right)_\nu. &&
\end{aligned}$$

□

Example 7.1.12 (Example 7.1.5)**.** Let $\mathcal{A}$ be the automaton of Figure 7.3. For all $\nu \subseteq \{0, 1\}$, the automata $\mathcal{A}_\nu$ are represented in Figure 7.4. Note that this example shows that $\mathcal{A}$ being minimal does not imply that the $\mathcal{A}_\nu$ are minimal.



(a) $\nu = \{0\}$, accepting $x_0 \doteq 0 \wedge x_1 \doteq 0$

(b) $\nu = \emptyset$, accepting $x_0 + 1 \doteq x_1$

(c) $\nu = \{0,1\}$, accepting $x_1 + 1 \doteq x_0$

(d) $\nu = \{1\}$, accepting False

Figure 7.4: The automata $\mathcal{A}_\nu$ for the automaton $\mathcal{A}$ of Figure 7.3

The converse statement partly holds. If, for every ν, there exists an automaton $\mathcal{A}_\nu$ over $\mathbb{N}$ with n states which defines R_ν, then there exists an automaton $\mathcal{A}$ over $\mathbb{Z}$ which accepts R. But as far as we know, there is no linear size automaton. The best algorithm known by the author creates an automaton with n^{2^d} states. Intuitively, the construction is similar to the Cartesian product of the 2^d automata $\mathcal{A}_\nu$.

The automaton $\mathcal{A}$ is not used in this part, hence the correctness of this statement is not formally proved.

The main theorems of this part are now stated. They both state the existence of a polynomial-time algorithm:

- The first theorem (Theorem 7.1.14) gives the proof of correctness of algorithm $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ (Algorithm 7.1.13). The notation $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ stands for "there *E*xists a *Q*uantifier-*F*ree $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula". This algorithm takes as input an automaton $\mathcal{A}$ over $\mathbb{Z}$ and decides in quasi-linear times whether there exists a quantifier-free $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula $\phi_{0,\mathbb{Z}}^{\mathcal{A}}$ that defines $\overline{\mathcal{A}}^{\mathbb{Z}}$.

  On the one hand, the algorithm $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ does not compute the quantifier-free formula. On the other hand the proof of the algorithm is constructive and yields an algorithm $CQF(\mathcal{V}_\iota^{\mathbb{Z}})$ which construct a quantifier-free formula $\phi_{0,\mathbb{Z}}^{\mathcal{A}}$. The notation $CQF(\mathcal{V}_\iota^{\mathbb{Z}})$ stands for "*C*onstruct a *Q*uantifier-*F*ree $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula". The $CQF(\mathcal{V}_\iota^{\mathbb{Z}})$ algorithm runs in exponential time, hence can not be used for $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$.

- The notation $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$ stands for "*Construct* an *E*xistential *F*ormula, Algorithm 7.1.15". The second theorem (Theorem 7.1.16) gives the proof of correctness of algorithm $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$. It states that if an automaton $\mathcal{A}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable set, then there exists a polynomial-length $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula $\phi_{1,\mathbb{Z}}^{\mathcal{A}}$ which defines $\overline{\mathcal{A}}^{\mathbb{Z}}$. The algorithm which computes the existential-formula $\phi_{1,\mathbb{Z}}^{\mathcal{A}}$ is denoted $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$ and runs in polynomial time.

7.1.4.1 The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$

The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ is now given. It is then proven that it accepts exactly the $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable set. This algorithm uses algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$, given as Algorithm 9.4.6.

***Algorithm 7.1.13** ($EQF(\mathcal{V}_\iota^{\mathbb{Z}})$)**.** Let $\mathcal{V}_\iota^{\mathbb{Z}} \in \mathbb{V}^{\mathbb{Z}}$. The cases where ι is 1 or 2 is first considered.

Let $\mathcal{A}$ be an automaton. The algorithm runs on each set $\nu \subseteq [d-1]$. For each ν the algorithm computes the automaton $\mathcal{A}_\nu$, as in Lemma 7.1.11. The algorithm then runs $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ on the automaton $\mathcal{A}_\nu$ and the logic $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$. The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ is given as Algorithm 9.4.6. If $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ rejects, then the algorithm rejects. If the algorithm has not rejected, it accepts.

The case $\mathcal{V}_0^{\mathbb{Z}}$ is similar. The only difference is that $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ is called with the logic $\Sigma_0\left[\mathcal{V}_1^{\mathbb{N}}\right]$.

It is now proven that $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ accepts exactly the automata accepting $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable set. The proof of the following theorem uses Theorem 9.4.8, which is the equivalent theorem for automata and logics over $\mathbb{N}$.

Theorem 7.1.14. *Let $\mathcal{V}_\iota^{\mathbb{Z}} \in \mathbb{V}$. Let $\mathcal{A}$ be an automaton with n states. It is decidable in time*

$$O\left(2^d n b^d (\log(n) + 3^d d)\right)$$

whether $\overline{\mathcal{A}}^{\mathbb{Z}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable.

The time formula uses three distinct parameters, the number of states n, the basis $b \geq 2$[1] and the dimension $d \geq 1$. If b and d are assumed to be fixed, then the time complexity of the algorithm is $O(n \log(n))$.

Since the alphabet size is b^d and $b \geq 2$, then $2^d \leq \left(b^d\right)$, that is, the expression 6^d is still polynomial in the size of the automaton. The same remarks apply for every analysis of time complexity of this part.

Proof. Let $\mathcal{V}_\iota^{\mathbb{Z}} \in \mathbb{V}_{\text{mod}}^{\mathbb{Z}}$. The cases where ι is 1 or 2 are first considered.

Let us first prove that, $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ accepts $\mathcal{A}$ if and only if $\overline{\mathcal{A}}^{\mathbb{Z}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable. By definition, the algorithm $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$ accepts $\mathcal{A}$ if and only if $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ accepts $\mathcal{A}_\nu$ for all $\nu \subseteq [d-1]$. By 9.4.8 it is equivalent to the fact that $\overline{\mathcal{A}_\nu}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable for all $\nu \subseteq [d-1]$. By Lemma 7.1.11, $\overline{\mathcal{A}_\nu}^{\mathbb{N}} = (\mathcal{A})_\nu$, hence it is equivalent to the fact that the set $(\mathcal{A})_\nu$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable for all $\nu \subseteq [d-1]$. By Lemmas 7.1.4 and 7.1.6, it is equivalent to the fact that $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable.

The case $\mathcal{V}_0^{\mathbb{Z}}$ is similar. The only difference is that the formulas over $\mathbb{N}$ are $\Sigma_0\left[\mathcal{V}_1^{\mathbb{N}}\right]$-formulas and not $\Sigma_0\left[\mathcal{V}_0^{\mathbb{N}}\right]/\nu$-formulas

[1] A technical note must be given for the case where the basis b is fixed to 2 or to 3. In those two cases, the computation time is similar to the one mentioned in the theorem, except that b is replaced by b^2, that is by 4 and 9 respectively. This note apply to all time complexity given in this part.

Computation time There are $O\left(2^d\right)$ sets $\nu \subseteq [d-1]$. By Lemma 7.1.11, computing the automata $\mathcal{A}_\nu$'s is done in time $O\left(nb^d\right)$, and $\mathcal{A}_\nu$ has $O(n)$ states. By Theorem 9.4.8, the algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ runs in time

$$O\left(nb^d(\log(n) + 3^d d)\right)$$

Hence the whole algorithm runs in time

$$O\left(2^d nb^d(\log(n) + 3^d d)\right).$$

□

7.1.4.2 The Algorithm *CEF*$(\mathcal{V}_\iota^{\mathbb{Z}})$

In this section, let us assume that $\mathcal{V}_\iota^{\mathbb{Z}}$ belongs to $\mathbb{V}_+$. The algorithm $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$ is now given, it uses algorithm $CEF(\mathcal{V}_\iota^{\mathbb{N}})$, given as Algorithm 7.2.13.

***Algorithm 7.1.15** ($CEF(\mathcal{V}_\iota^{\mathbb{Z}})$)**.** Let $\mathcal{A}$ be an automaton which accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable set. Let $\mathcal{V}_\iota^{\mathbb{Z}} \in \mathbb{V}_{\text{mod}}^{\mathbb{Z}}$. The cases where ι is 1 or 2 is first considered.

The algorithm runs on each set $\nu \subseteq [d-1]$. For each ν the algorithm computes the automaton $\mathcal{A}_\nu$, as in Lemma 7.1.11. The algorithm then runs $CEF(\mathcal{V}_\iota^{\mathbb{N}})$ on the automaton $\mathcal{A}_\nu$ and the logic $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ in order to construct a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula $\phi_{1,\mathbb{N}}^{\mathcal{A}_\nu}$ which defines $\overline{\mathcal{A}_\nu}^{\mathbb{N}}$. The algorithm $CEF(\mathcal{V}_\iota^{\mathbb{N}})$ is given as Algorithm 7.2.13.

The algorithm returns the $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula $\phi_{1,\mathbb{Z}}^{\mathcal{A}}$ returned by the application of the algorithm given in Lemma 7.1.6 with the formulas $\phi_{1,\mathbb{N}}^{\mathcal{A}_\nu}$'s.

The case $\mathcal{V}_0^{\mathbb{Z}}$ is similar. The only difference is that $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ is called with the logic $\Sigma_0\left[\mathcal{V}_1^{\mathbb{N}}\right]$.

It is now proven that $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$ returns a formula which defines $\overline{\mathcal{A}}^{\mathbb{Z}}$. The proof of the theorem use Theorems 7.2.14, which is the equivalent theorem for automata and logics over $\mathbb{N}$.

Theorem 7.1.16. *Let $\mathcal{V}_\iota^{\mathbb{Z}}$ be a vocabulary belonging to $\mathbb{V}_+$. Let $\mathcal{A}$ be an automaton with n states which accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-definable set. The algorithm* CEF$(\mathcal{V}_\iota^{\mathbb{Z}})$ *returns in time:*

$$O\left(n^3 \log(b) 2^{2d} d\left(\log(n) + d^2\right)\right)$$

a formula of length:

$$O\left(n^3 2^d \log(b)\left(\log(n) d^2 + 2^d\right)\right)$$

which defines $\overline{\mathcal{A}}^{\mathbb{Z}}$.

If the basis b and the dimension d are assumed to be constant, then the time complexity of the algorithm is $O\left(n^3 \log(n)\right)$.

Proof. Let $\mathcal{V}_\iota^{\mathbb{Z}}$ be a vocabulary of $\mathbb{V}_+$. Let $\mathcal{A}$ be an automaton over $\mathbb{Z}$ with n states. The cases where ι is 1 or 2 are first considered. The existence of the $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula $\phi_{\iota,\mathbb{Z}}^{\mathcal{A}}$ that defines $\overline{\mathcal{A}}^{\mathbb{Z}}$ is first proven.

By Lemma 7.1.4 all automata $\mathcal{A}_\nu$ have n states and are computable in time $O\big(nb^d\big)$. By Theorem 7.2.14, the formulas $\phi^{\mathcal{A}_\nu}_{1,\mathbb{N}}$ are computable in time:

$$O\Big(n^3 2^d\, d \log(b)\Big(\log(n) + d^2\Big)\Big),$$

and their length are:

$$O\Big(n^3 \log(b)\Big(\log(n)d^2 + 2^d\Big)\Big).$$

By Lemma 7.1.6, if the sets $\left(\overline{\mathcal{A}}^{\mathbb{Z}}\right)_\nu$ are defined by $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formulas of length $O(s)$, then $\overline{\mathcal{A}}^{\mathbb{Z}}$ is defined by a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]$-formula computable in time $O\Big(2^d(s+d)\Big)$. Hence the algorithm $CQF(\mathcal{V}_\iota^{\mathbb{Z}})$ returns a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{Z}}\right]$-formula $\phi^{\mathcal{A}}_{1,\mathbb{Z}}$ that defines $\overline{\mathcal{A}}^{\mathbb{Z}}$ in time:

$$O\Big(2^d\Big(nb^d(\log(n) + 3^d d)\Big)\Big),$$

and its length is:

$$O\Big(2^d\Big(n^3 \log(b)\Big(\log(n)d^2 + 2^d\Big)\Big)\Big),$$

The case $\mathcal{V}_0^{\mathbb{Z}}$ is similar. The only difference is that the formulas over $\mathbb{N}$ are $\Sigma_1\left[\mathcal{V}_1^{\mathbb{N}}\right]$-formulas and not $\Sigma_1\left[\mathcal{V}_0^{\mathbb{N}}\right]/\nu$-formulas □

7.2 Restricting the Logic

Let us recall that the problem studied in this part is to decide whether a given automaton accepts a set of integers defined in some fragment of $\mathsf{FO}[<,\mathrm{mod}]$. The problem has been reduced from $\mathbb{Z}$ to $\mathbb{N}$ in Section 7.1. In this section, it is reduced again to automata having a special form. These automata are characterized by another fragment of $\mathsf{FO}[<,\mathrm{mod}]$ denoted by $\Sigma_0[\mathcal{V}_\iota']/\cdot,\cdot,\nu$ which is introduced in Section 7.2.2.

More precisely, the problem studied in this part is reduced to the problem of deciding whether an initially-cyclic automaton accepts a set of integers defined in some fragment of $\mathsf{FO}[<,\mathrm{mod}]$. The reduction from the first problem to the second one is studied in Section 7.2.1. A characterization of the $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable sets accepted by an initially-cyclic automaton is given in Section 7.2.2.

The reader is reminded that the symbol ν has been defined in Section 7.1 to study relations over $\mathbb{Z}$. To study relations over $\mathbb{N}$, it suffices to assume that $\nu = \emptyset$. Let $\nu \subseteq [d-1]$ be fixed for the rest of the part.

7.2.1 The Automaton $\mathcal{A}$ and the Automata $\mathcal{A}_q$

The main result of this section is Proposition 7.2.10. It states that, for an automaton $\mathcal{A}$, the set $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable if and only if for all cyclic states q of $\mathcal{A}$, the sets $\overline{\mathcal{A}_q}^{\mathbb{N}}$ are $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

To obtain this result, this section considers how a formula defining the set accepted by an automaton $\mathcal{A}$ relates to formulas defining the sets accepted by $\mathcal{A}_q$, for q a state of $\mathcal{A}$.

In the first section, formulas defining $\overline{\mathcal{A}_q}^{\mathbb{N}}$ are computed from a formula which defines $\overline{\mathcal{A}}^{\mathbb{N}}$. In the second section a formula defining $\overline{\mathcal{A}}^{\mathbb{N}}$ is computed from the formulas which define $\overline{\mathcal{A}_q}^{\mathbb{N}}$ for some states q.

7.2.1.1 From a Formula for $\overline{\mathcal{A}}^{\mathbb{N}}$ to Formulas for $\overline{\mathcal{A}_q}^{\mathbb{N}}$

The notions of left-quotient of languages and its relation to automata have already been introduced in Section 2.3.2. Similarly to the left quotient of languages, the following definition introduces the notion of *left-quotient of formulas*. This notion has already been introduced in [BC96, Section 2][2] and in [WB00, Section 3] for FO[+]-formulas. The left-quotient of a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula by a long-enough word, belongs to the fragment $\Sigma_0[\mathcal{V}_\iota']/\cdot,\cdot,\nu$ of the logic $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, introduced in the next section.

Intuitively, the left quotient of ϕ by $\boldsymbol{w}$, denoted by $\boldsymbol{w}^{-1}\phi(\boldsymbol{x})$, is defined as $\phi\left(b^{|\boldsymbol{w}|}\boldsymbol{x}+\overline{\boldsymbol{w}}^{\mathbb{N}}\right)$ where all atomic formulas which cannot hold over integers are replaced by false.

***Definition 7.2.1** (Left quotient of formulas)**.** Let $\phi\in\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ and let $\boldsymbol{w}\in\left(A_b^d\right)^*$.

Let $\boldsymbol{w}^{-1}\phi\in\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ be the formula defined by induction over ϕ as follows:

ϕ	if	then $\boldsymbol{w}^{-1}\phi$ is	otherwise it is
$x_i \doteq c$	$\overline{w_i}^{\mathbb{N}} \equiv c \mod b^{\lvert\boldsymbol{w}\rvert}$	$x_i \doteq \frac{c-\overline{w_i}^{\mathbb{N}}}{b^{\lvert\boldsymbol{w}\rvert}}$	False
$x_i \doteq x_j + c$	$\overline{w_i}^{\mathbb{N}} \equiv \overline{w_j}^{\mathbb{N}} + c \mod b^{\lvert\boldsymbol{w}\rvert}$	$x_i \doteq x_j + \frac{c-\overline{w_i}^{\mathbb{N}}+\overline{w_j}^{\mathbb{N}}}{b^{\lvert\boldsymbol{w}\rvert}}$	False
$x_i < x_j$	$\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$	$\neg\left(x_j < x_i\right)$	$x_i < x_j$
$x_i \equiv c \bmod m$ $\left(\text{Let} g = \gcd\left(b^{\lvert\boldsymbol{w}\rvert}, m\right)\right)$	g divides $c - \overline{w_i}^{\mathbb{N}}$	$x_i \equiv \frac{c-\overline{w_i}^{\mathbb{N}}}{g}\left(\frac{b^{\lvert\boldsymbol{w}\rvert}}{g}\right)^{-1} \mod \frac{m}{g}$	False
$\xi \vee \psi$		$\boldsymbol{w}^{-1}\xi \vee \boldsymbol{w}^{-1}\psi$	
$\neg\psi$		$\neg\boldsymbol{w}^{-1}\psi$	

An example of application of this lemma is now given.

Example 7.2.2. Consider the basis $b=2$. Let ϕ be $x_0 \doteq 2 \vee x_0 \doteq 1 \vee x_0 < x_1$. Then

$$(1,0)^{-1}\left\{(0,1)^{-1}\phi\right\} = (1,0)^{-1}\{x_0 \doteq 1 \vee \text{False} \vee \neg(x_1 < x_0)\} = x_0 \doteq 0 \vee \text{False} \vee \neg\neg(x_0 < x_1).$$

Since the double negations and the False formulas are removed, $(1,0)^{-1}\left\{(0,1)^{-1}\phi\right\}$ is equal to $x_0 \doteq 0 \vee x_0 < x_1$.

The case of the left quotient of order relation needs an explanation. If $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$ then $\boldsymbol{w}^{-1}\left(x_i < x_j\right)$ is $\neg\left(x_j < x_i\right)$. This formula is equivalent to the more readable formula $x_i \leq x_j$. One could intuitively have preferred this formula. But $\leq$ does not belong to our vocabulary, and taking $x_i \leq x_j$ as an abbreviation for $x_i < x_j \vee x_i \doteq x_j$ would introduce the $\doteq$ predicate in the formula.

We want to avoid to introduce new predicates in left quotient for two reasons: the use of the $\doteq$ predicate is restricted in Section 7.2.2.2. Hence $x_i \doteq x_j$ would cause technical problems that $\neg\left(x_j < x_i\right)$ avoids. Furthermore, introducing the $\doteq$ predicates implies that $\left(\boldsymbol{w}'^{-1}\boldsymbol{w}^{-1}\right)\phi$ may be different from $\boldsymbol{w}'^{-1}\left(\boldsymbol{w}^{-1}\phi\right)$. Namely, the left quotient would not be a right action. It is now proved that it is a right action.

Lemma 7.2.3. *The function $\cdot^{-1}$ is a right action of $\left(A_b^d\right)^*$ over $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$.*

Proof. Let $\boldsymbol{w},\boldsymbol{w}'\in\left(A_b^d\right)^*$. Let $\phi\in\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$. The fact that $\boldsymbol{w}^{-1}\phi\in\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ is straightforward from the definition. It must be proven that $(\boldsymbol{w}\boldsymbol{w}')^{-1}\phi$ and $\boldsymbol{w}'^{-1}(\boldsymbol{w}^{-1}\phi)$ are equal. The proof is by induction on ϕ. The induction cases are trivial. The base cases consist in a straightforward case study. The only special case is the order relation, which may create two successive negations. But successive negations are removed, and the equality of the formulas follows. □

[2] For e a formula and $\boldsymbol{b}$ a tuple of digit, they note $e(b_0,\ldots,b_{d-1})$ what we note $\boldsymbol{b}^{-1}e$.

The following lemma states that this definition is consistent, namely, that the set defined by the quotient of a formula ϕ is the quotient of the set defined by the formula ϕ. A similar lemma for $\Sigma_0[+,<,\mathrm{mod}]$ has been proved in [BC96] and in [WB00]. The proof is almost the same, but it is given here for the sake of completeness.

Lemma 7.2.4. *Let $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ and $\boldsymbol{w} \in \left(A_b^d\right)^*$. One has $\overline{\boldsymbol{w}^{-1}\phi}^{\mathbb{N}} = \boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}}$.*

Proof. Let us prove that $\overline{\boldsymbol{w}^{-1}\phi}^{\mathbb{N}} = \boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}}$. Namely, it is proven that for all $\boldsymbol{n} \in \mathbb{N}^d$, $\boldsymbol{n} \in \overline{\boldsymbol{w}^{-1}\phi}^{\mathbb{N}}$ if and only if $\boldsymbol{n} \in \boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}}$.

Let us claim that $\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})$ if and only if $\phi(\boldsymbol{w}\cdot\boldsymbol{n})$. It implies that $\boldsymbol{n} \in \overline{\boldsymbol{w}^{-1}\phi}^{\mathbb{N}}$ if and only if $\boldsymbol{w}\cdot\boldsymbol{n} \in \overline{\phi}^{\mathbb{N}}$. Since $\boldsymbol{w}\cdot\boldsymbol{n} \in \overline{\phi}^{\mathbb{N}}$ if and only if $\boldsymbol{n} \in \boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}}$, by transitivity, it implies that $\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})$ if and only if $\boldsymbol{n} \in \boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}}$.

It remains to prove, by induction on ϕ, that $\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})$ if and only if $\phi(\boldsymbol{w}\cdot\boldsymbol{n})$.

The induction cases are trivial. The base cases are now proven:

- Let us assume that ϕ is $x_i \doteq c$. Two cases must be considered, depending on whether $\overline{w_i}^{\mathbb{N}} \equiv c \mod b^{|\boldsymbol{w}|}$ or not. If $\overline{w_i}^{\mathbb{N}} \not\equiv c \mod b^{|\boldsymbol{w}|}$ then $\boldsymbol{w}^{-1}\phi$ is the formula False and $w_i\cdot n_i \neq c$. Hence $\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})$ and $\phi(\boldsymbol{w}\cdot\boldsymbol{n})$ are equivalent since they are both false.

  If $\overline{w_i}^{\mathbb{N}} \equiv c \mod b^{|\boldsymbol{w}|}$, then $\boldsymbol{w}^{-1}\phi$ is $x_i \doteq \frac{c-\overline{w_i}^{\mathbb{N}}}{b^{|\boldsymbol{w}|}}$. Hence:

$$\left(\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})\right)\Longleftrightarrow\left(n_i = \frac{c-\overline{w_i}^{\mathbb{N}}}{b^{|\boldsymbol{w}|}}\right)\Longleftrightarrow\left(\overline{w_i}^{\mathbb{N}} + b^{|\boldsymbol{w}|}n_i = c\right)\Longleftrightarrow(w_i\cdot n_i = c)\Longleftrightarrow(\phi(\boldsymbol{w}\cdot\boldsymbol{n})).$$

- The proof is similar for $x_i \doteq x_j + c$.

- Let us assume that ϕ is $x_i < x_j$. Two cases must be considered: if $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$ then $\boldsymbol{w}^{-1}\phi$ is $\neg\left(x_j < x_i\right)$, in this case:

$$\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})\Longleftrightarrow\neg\left(n_j < n_i\right)\Longleftrightarrow n_j \leq n_j\Longleftrightarrow w_i\cdot n_i < w_j\cdot n_j\Longleftrightarrow\phi(\boldsymbol{w}\cdot\boldsymbol{n}).$$

  Otherwise $\overline{w_i}^{\mathbb{N}} \geq \overline{w_j}^{\mathbb{N}}$ then $\boldsymbol{w}^{-1}\phi$ is $x_i < x_j$, in this case:

$$\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})\Longleftrightarrow n_i < n_j\Longleftrightarrow w_i\cdot n_i < w_j\cdot n_j\Longleftrightarrow\phi(\boldsymbol{w}\cdot\boldsymbol{n}).$$

- Finally, let us assume that ϕ is $x_i \equiv c \mod m$. Let $g = \gcd(b^{|\boldsymbol{w}|}, m)$. Two cases must be considered: if g does not divide $c - w_i$, then $\boldsymbol{w}^{-1}\phi$ is the formula False and $w_i\cdot n_i \not\equiv c \mod m$. Hence $\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})$ and $\phi(\boldsymbol{w}\cdot\boldsymbol{n})$ are equivalent since they are both false.

  Otherwise, let us assume that g divides $c - w_i$. Then $\boldsymbol{w}^{-1}\phi$ is $x_i \equiv \frac{c-w_i}{g}\times\left(\frac{b^{|\boldsymbol{w}|}}{g}\right)^{-1} \mod \frac{m}{g}$. Hence:

$$\begin{aligned}
\left(\left(\boldsymbol{w}^{-1}\phi\right)(\boldsymbol{n})\right)\Longleftrightarrow(&\quad n_i \equiv \tfrac{c-w_i}{g}\times\left(\tfrac{b^{|\boldsymbol{w}|}}{g}\right)^{-1} &&\mod \tfrac{m}{g})\\
\Longleftrightarrow(&\quad \tfrac{b^{|\boldsymbol{w}|}}{g}n_i \equiv \tfrac{c-w_i}{g} &&\mod \tfrac{m}{g})\\
\Longleftrightarrow(&\quad b^{|\boldsymbol{w}|}n_i \equiv c - \overline{w_i}^{\mathbb{N}} &&\mod m)\\
\Longleftrightarrow(&\quad \overline{w_i}^{\mathbb{N}} + b^{|\boldsymbol{w}|}n_i \equiv c &&\mod m)\\
\Longleftrightarrow(&\quad w_i\cdot n_i \equiv c &&\mod m)\\
\Longleftrightarrow(&\quad \phi(\boldsymbol{w}\cdot\boldsymbol{n}))
\end{aligned}$$

□

The previous lemma leads to the following corollary when the set $\overline{\phi}^{\mathbb{N}}$ is accepted by an automaton.

Corollary 7.2.5. *Let $\mathcal{A} = (Q, A, \delta, q_0, F)$ be an automaton accepting a set defined by a formula ϕ. Then for each $\boldsymbol{w} \in A_b^d$, $\overline{\mathcal{A}_{\delta(q_0,\boldsymbol{w})}}^{\mathbb{N}} = \overline{\boldsymbol{w}^{-1}\phi}^{\mathbb{N}}$.*

Proof. One has $\overline{\mathcal{A}_{\delta(q_0,\boldsymbol{w})}}^{\mathbb{N}} = \boldsymbol{w}^{-1}\overline{\mathcal{A}}^{\mathbb{N}} = \boldsymbol{w}^{-1}\overline{\phi}^{\mathbb{N}} = \overline{\boldsymbol{w}^{-1}\phi}^{\mathbb{N}}$. □

For a given state q there may be distinct words $\boldsymbol{w}$ and $\boldsymbol{w'}$ such that $\delta(q_0, \boldsymbol{w}) = q$ and $\delta(q_0, \boldsymbol{w'}) = q$. The automaton $\mathcal{A}_q$ accepts the set defined by the formulas $\boldsymbol{w}^{-1}\phi$ and $\boldsymbol{w'}^{-1}\phi$. Those formulas may be distinct formulas, but are equivalent.

An example of how this result applies to an automaton is now given. This example is based on Example 2.3.3.

Example 7.2.6. Consider the basis be $b = 2$, the dimension $d = 2$. Let $\mathcal{A}$ be the automaton of Figure 7.5. It accepts the set defined by the formula ϕ which is equal to $x_0 - 1 \equiv x_1 \mod 6 \wedge x_0 < x_1$. Let us recall that $x_0 - 1 \equiv x_1 \mod 6$ is an abbreviation for $\bigwedge_{i=0}^{5} x_0 \equiv i + 1 \mod 6 \wedge x_1 \equiv i \mod 6$.

Since $q_2 = \delta(q_0, (0,1))$, by the previous lemma, the automaton $\mathcal{A}_{q_2}$ accepts the set defined by $(0,1)^{-1}\phi$, which is equal to $x_0 - 1 \equiv x_1 \mod 3 \wedge \neg(x_1 < x_0)$. Since $q_2 = \delta(q_0, (1,0)(1,0)(1,0))$, then the automaton $\mathcal{A}_{q_2}$ also accepts the set defined by $[(1,0)(1,0)(1,0)]^{-1}\phi$ which is equal to $x_0 - 1 \equiv x_1 \mod 3 \wedge \neg(x_1 \leq x_0)$.

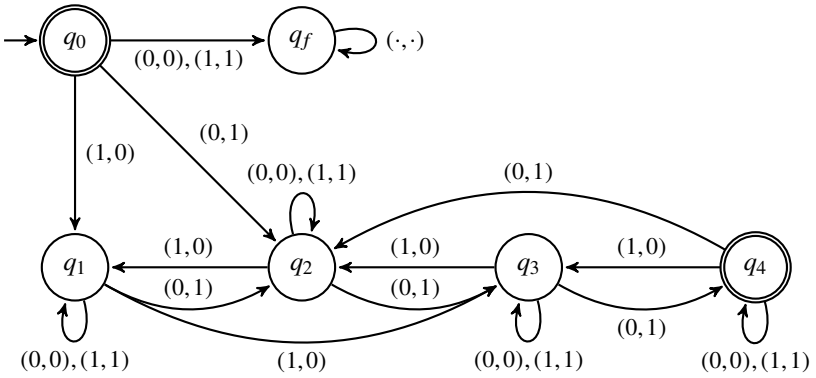


Figure 7.5: $x_0 - 1 \equiv x_1 \mod 6 \wedge x_0 \geq x_1$ in $\mathbb{N}^2$

7.2.1.2 From formulas for $\overline{\mathcal{A}_q}^{\mathbb{N}}$ to a formula for $\overline{\mathcal{A}}^{\mathbb{N}}$

It is explained, in the previous section, how one could compute a formula defining $\overline{\mathcal{A}_q}^{\mathbb{N}}$ from a formula defining $\overline{\mathcal{A}}^{\mathbb{N}}$. The inverse construction is explained in this section. For some set S of states it is now explained how a formula defining $\overline{\mathcal{A}}^{\mathbb{N}}$ can be computed from the formulas defining $\overline{\mathcal{A}_q}^{\mathbb{N}}$ for $q \in S$.

The main proposition of this section yields the computation of a formula defining $\mathcal{A}$ when S is the set of cyclic states.

The following lemma proves that a set is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable if and only if all of its quotients by a letter, or by every word of a fixed length, are $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

Lemma 7.2.7. *Let R be a subset of $\mathbb{N}^d$ and let $l \in \mathbb{N}$. If for all $\boldsymbol{w} \in \left(A_b^d\right)^l$, the left-quotient $\boldsymbol{w}^{-1}R$ is defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula then R is defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula.*

Proof. A function $\Phi_{\boldsymbol{w}}$ from formulas to formulas must first be defined. This function is applied to $\phi_{\boldsymbol{w}}$ in the definition of ϕ. This function $\Phi_{\boldsymbol{w}}$ transforms $\psi(\boldsymbol{x})$ into $\psi(\frac{\boldsymbol{x}-\boldsymbol{w}}{b^l})$. For example if the length l is 1, the basis b is 2 and ψ is $x_0 \doteq 4$ then $\Phi_1(\psi)$ is $2 \times x_0 + 1 \doteq 4$, which is equivalent to $x_0 \doteq 9$.

The formula $\Phi_{\boldsymbol{w}}$ is defined by induction on ψ as follows:

ψ	$\Phi_{\boldsymbol{w}}(\psi)$	ψ	$\Phi_{\boldsymbol{w}}(\psi)$
$\psi \vee \xi$	$\Phi_{\boldsymbol{w}}(\psi) \vee \Phi_{\boldsymbol{w}}(\xi)$	$\neg\psi$	$\neg\Phi_{\boldsymbol{w}}(\psi)$
$x_i \doteq c$	$x \doteq b^l \times c + w_i$	$x_i + c \doteq x_j$	$x_i + \left(b^l \times c - w_i + w_j\right) \doteq x_j$
$x_i < x_j$	$x_i - w_j + w_i < x_j$	$x_i \equiv c \mod m$	$x_i \equiv b^l \times c + w_i \mod b^l \times m$
False	False		

It must be proven that $\overline{\Phi_{\boldsymbol{w}}(\psi)}^{\mathbb{N}} \cap \left(b^l\mathbb{N}^d + \overline{\boldsymbol{w}}^{\mathbb{N}}\right) = b^l \times \overline{\psi}^{\mathbb{N}} + \overline{\boldsymbol{w}}^{\mathbb{N}}$. Namely, it must be proven that for all $\boldsymbol{n} \in \mathbb{N}^d$, $\boldsymbol{n} \in \left(\overline{\Phi_{\boldsymbol{w}}(\psi)}^{\mathbb{N}} \cap \left(b^l\mathbb{N}^d + \overline{\boldsymbol{w}}^{\mathbb{N}}\right)\right)$ if and only if $\boldsymbol{n} \in \left(b^l \times \overline{\psi}^{\mathbb{N}} + \overline{\boldsymbol{w}}^{\mathbb{N}}\right)$. If $\boldsymbol{n} \not\equiv \boldsymbol{w} \mod b^l$ then $\boldsymbol{n}$ does not belong to any of those two sets, hence the equivalence holds. Let us assume that $\boldsymbol{n} \equiv \boldsymbol{w} \mod b^l$.

Let us first assume that $(\Phi_{\boldsymbol{w}}(\psi))(\boldsymbol{n})$ if and only if $\psi\left(\frac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l}\right)$. It implies that $\boldsymbol{n} \in \overline{\Phi_{\boldsymbol{w}}(\psi)}^{\mathbb{N}}$ if and only if $\frac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l} \in \overline{\psi}^{\mathbb{N}}$. Since $\frac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l} \in \overline{\psi}^{\mathbb{N}}$ if and only if $\boldsymbol{n} \in b^l \times \overline{\psi}^{\mathbb{N}} + \overline{\boldsymbol{w}}^{\mathbb{N}}$, by transitivity of equivalence it implies that $\boldsymbol{n} \in \overline{\Phi_{\boldsymbol{w}}(\psi)}^{\mathbb{N}}$ if and only if $\boldsymbol{n} \in b^l \times \overline{\psi}^{\mathbb{N}} + \overline{\boldsymbol{w}}^{\mathbb{N}}$.

It remains to prove by induction on ψ that $(\Phi_{\boldsymbol{w}}(\psi))(\boldsymbol{n})$ if and only if $\phi\left(\frac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l}\right)$.

The induction cases are trivial, the base cases are now proven:

- Let us assume that ψ is $x_i + c \doteq x_j$. Then:

$$\begin{aligned}(\Phi_{\boldsymbol{w}}(\psi))(\boldsymbol{n}) &\iff n_i + \left(b^l \times c - w_i + w_j\right) \doteq n_j \\ &\iff n_i - w_i + b^l \times c \doteq n_j - w_j \\ &\iff \tfrac{n_i - w_i}{b^l} + c \doteq \tfrac{n_j - w_j}{b^l} \\ &\iff \psi(\tfrac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l}).\end{aligned}$$

- The case $x_i \doteq c$ is similar.

- Let us assume that ψ is $x_i < x_j$. Then:

$$\begin{aligned}(\Phi_{\boldsymbol{w}}(\psi))(\boldsymbol{n}) &\iff n_i + w_j - w_i < n_j \\ &\iff n_i - w_i < n_j - w_j \\ &\iff \tfrac{n_i - w_i}{b^l} < \tfrac{n_j - w_j}{b^l} \\ &\iff \psi(\tfrac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l}).\end{aligned}$$

- Finally if ψ is $x_i \equiv c \mod m$ then:

$$\begin{aligned}(\Phi_{\boldsymbol{w}}(\psi))(\boldsymbol{n}) &\iff n_i \equiv b^l \times c + w_i \mod b^l \times m\\ &\iff n_i - w_i \equiv b^l \times c \mod b^l \times m\\ &\iff \tfrac{n_i - w_i}{b^l} \equiv c \mod m\\ &\iff \psi(\tfrac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l}).\end{aligned}$$

The formula ϕ which defines R is:

$$\bigvee_{\boldsymbol{w}\in\left(A_b^d\right)^l} \left\{\boldsymbol{x} \equiv \boldsymbol{w} \mod b^l \wedge \Phi_{\boldsymbol{w}}(\phi_w)(\boldsymbol{x})\right\}.$$

It is now proven that ϕ defines R. Let $\boldsymbol{n} \in \mathbb{N}^d$ and let us prove that $\boldsymbol{n} \in R$ is equivalent to $\phi(n)$:

$$\begin{aligned}\boldsymbol{n} \in R &\iff \textstyle\bigvee_{\boldsymbol{w}\in\left(A_b^d\right)^l} \{\boldsymbol{n} \equiv \overline{\boldsymbol{w}}^{\mathbb{N}} \mod b^l \wedge \tfrac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l} \in \boldsymbol{w}^{-1}R\}\\ &\iff \textstyle\bigvee_{\boldsymbol{w}\in\left(A_b^d\right)^l} \{\boldsymbol{n} \equiv \overline{\boldsymbol{w}}^{\mathbb{N}} \mod b^l \wedge \ \phi_{\boldsymbol{w}}\left(\tfrac{\boldsymbol{n}-\overline{\boldsymbol{w}}^{\mathbb{N}}}{b^l}\right) \ \}\\ &\iff \textstyle\bigvee_{\boldsymbol{w}\in\left(A_b^d\right)^l} \{\boldsymbol{n} \equiv \overline{\boldsymbol{w}}^{\mathbb{N}} \mod b^l \wedge \ \Phi_{\boldsymbol{w}}(\phi_{\boldsymbol{w}})(\boldsymbol{n}) \ \}\\ &\iff \phi(\boldsymbol{n}).\end{aligned}$$

□

This lemma has a straightforward corollary in term of automata.

Corollary 7.2.8. *Let $\mathcal{A}$ be an automaton and let $l \in \mathbb{N}$. Let S be the set of states accessible in l steps. If $\overline{\mathcal{A}_q}^{\mathbb{N}}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set for all $q \in S$ then R is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.*

Example 7.2.6 is now resumed.

Example 7.2.9. Let $\mathcal{A}$ be the automaton of Figure 7.5. Since the automaton $\mathcal{A}_{q_1} = \mathcal{A}_{\delta(q_0,(0,0))}$ accepts the set defined by the formula $x_0 \equiv x_1 \mod 3 \wedge x_0 < x_1$, the automaton $\mathcal{A}_{q_2} = \mathcal{A}_{\delta(q_0,(1,1))}$ accepts the set defined by the formula $x_0 - 1 \equiv x_1 \mod 3 \wedge \neg(x_1 < x_0)$ and the automaton $\mathcal{A}_{q_f} = \mathcal{A}_{\delta(q_0,(0,1))} = \mathcal{A}_{\delta(q_0,(1,0))}$ accepts the empty set defined by the formula False, then $\mathcal{A}$ accepts

$$\begin{array}{llllll}
\{x_0 \equiv 0 \mod 2 \wedge x_1 \equiv 0 \mod 2 \wedge \text{False} & & & & & \}\vee\\
\{x_0 \equiv 0 \mod 2 \wedge x_1 \equiv 1 \mod 2 \wedge x_0 - 1 \equiv x_1 & \mod 6 \wedge & x_0 < x_1 & & & \}\vee\\
\{x_0 \equiv 1 \mod 2 \wedge x_1 \equiv 1 \mod 2 \wedge \text{False} & & & & & \}\vee\\
\{x_0 \equiv 1 \mod 2 \wedge x_1 \equiv 0 \mod 2 \wedge x_0 - 1 \equiv x_1 & \mod 6 \wedge & \neg(x_1 < x_0) & & & \}.
\end{array}$$

The following proposition is similar to Corollary 7.2.8, but the set S of states accessible in a single step is replaced by the set of cyclic states.

Proposition 7.2.10. Let $\mathcal{A}$ be an automaton such that for each cyclic state q, the set $\overline{\mathcal{A}_q}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable. Then the set $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

Proof. Let $\mathcal{A} = (Q, A, \delta, q_0, F)$ be an automaton with n states. Let us assume that $\overline{\mathcal{A}_q}^{\mathbb{N}}$ is defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula ϕ_q for all cyclic states $q \in Q$.

The proof that $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable is by induction on n. Two cases must be considered. If q_0 is cyclic, then $\overline{\mathcal{A}}^{\mathbb{N}}$ is defined by ϕ_{q_0}. Otherwise, by Lemma 7.2.7, it suffices to prove that for all $\boldsymbol{a} \in A_b^d$, the set $\boldsymbol{a}^{-1}\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

Since $\boldsymbol{a}^{-1}\overline{\mathcal{A}}^{\mathbb{N}} = \overline{\mathcal{A}_{\delta(q_0,\boldsymbol{a})}}^{\mathbb{N}}$, it is enough to prove that $\overline{\mathcal{A}_{\delta(q_0,\boldsymbol{a})}}^{\mathbb{N}}$ is defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula.

Since q_0 is not cyclic, it is not accessible from $\mathcal{A}_{\delta(q_0,\boldsymbol{a})}$. Hence, $\mathcal{A}_{\delta(q_0,\boldsymbol{a})}$ has at most $n-1$ states and the induction hypothesis can be applied.

For each cyclic state q of $\mathcal{A}_{\delta(q_0,\boldsymbol{a})}$, $(\mathcal{A}_{\delta(q_0,\boldsymbol{a})})_q = \mathcal{A}_q$ hence $\overline{(\mathcal{A}_{\delta(q_0,\boldsymbol{a})})_q}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable. By the induction hypothesis, $\mathcal{A}_{\delta(q_0,\boldsymbol{a})}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable. □

This lemma can be used to decide whether an automaton $\mathcal{A}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set. An algorithm to compute the set of cyclic states is now introduced.

***Algorithm 7.2.11** (Tarjan's algorithm, [Tar72])**.** Given a graph with v vertices and e edges, Tarjan's algorithm compute the set of strongly connected components in time $O(v+e)$. A state is cyclic if and only if there exists $\boldsymbol{a} \in A_b^d$ such that q and $\delta(q,\boldsymbol{a})$ belongs to the same strongly connected components. Hence for an automaton $\mathcal{A}$ over the alphabet A_b^d with n states, the set of cyclic states is computable in time $O\left(nb^d\right)$.

Let n be the number of states of $\mathcal{A}$. Let us assume that there is an algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ which decides in time T if an initially-cyclic automaton accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set. Then deciding whether $\mathcal{A}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set can be done in time $O(nT)$, testing whether $\overline{\mathcal{A}_q}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ for all cyclic state q. A more efficient algorithm is given as Algorithm 9.4.6.

It should be noted that if q is cyclic, then $\mathcal{A}_q$ is initially-cyclic, hence $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ can indeed be applied to $\mathcal{A}_q$. Hence, to characterize automata accepting $\Sigma_0[\mathcal{V}_\iota']$-definable set, it remains to characterize the set defined by initially-cyclic automata. A first characterization is given in the following section.

The length of the formula generated by Lemma 7.2.7 is not polynomially bounded. The algorithm $CEF(\mathcal{V}_\iota^{\mathbb{N}})$ uses another construction. In order to give the algorithm $CEF(\mathcal{V}_\iota^{\mathbb{N}})$, the following lemma is first needed.

***Lemma 7.2.12** (ϕ^n)**.** Let $\phi \in \Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, and $n \in \mathbb{N}$. There exists a formula $\phi^n \in \Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ such that $\overline{\phi^n}^{\mathbb{N}} \cap \mathbb{N}^d$ equals $b^n\phi(\boldsymbol{x})$, that is $\{b^n\boldsymbol{x} \mid \phi(\boldsymbol{x})\}$. The formula ϕ^n is computable in time $O(n\log(b)|\phi|)$.

Proof. The proof is a straightforward induction on ϕ when ϕ^n is defined this way:

ϕ	ϕ^n	ϕ	ϕ^n
$\exists^+ x.\psi$	$\exists^+ x.\psi^n$	$\exists^- x.\psi$	$\exists^- x.\psi^n$
$\psi \vee \xi$	$\psi^n \vee \xi^n$	$\neg\psi$	$\neg\psi^n$
$x + c = y$	$x + cb^n = y$	$x = c$	$x = cb^n$
$x < y$	$x < y$	$x = a \mod m$	$x = ab^n \mod mb^n$

□

The algorithm $CEF(\mathcal{V}_\iota^{\mathbb{N}})$, is now given, it uses the algorithm $CEF'(\mathcal{V}_\iota^{\mathbb{N}})$, given as Algorithm 10.4.3. The algorithm $CEF'(\mathcal{V}_\iota^{\mathbb{N}})$ takes as input an initially-cyclic automaton $\mathcal{A}$ which accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set, and returns an $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula which defines $\overline{\mathcal{A}}^{\mathbb{N}}$.

It is then proven that the algorithm $CEF(\mathcal{V}_\iota^{\mathbb{N}})$ returns a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula which defines $\overline{\mathcal{A}}^{\mathbb{N}}$.

***Algorithm 7.2.13** (*CEF*($\mathcal{V}_\iota^{\mathbb{N}}$))**.** Let $\mathcal{A}$ be an automaton over $\mathbb{N}$ which accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set with n states. Let A' be the minimal automaton of $\mathcal{A}$.

The algorithm runs on each cyclic state q of A'. For each q, the algorithm applies the algorithm *CEF'*($\mathcal{V}_\iota^{\mathbb{N}}$) to A'_q to compute a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula $\phi_{1,\mathbb{N}}^{A'_q}$. The algorithm then construct $(\phi_{1,\mathbb{N}}^{A'_q})^n$, using Lemma 7.2.12.

Recall that the notation $\exists^\nu$ is introduced in Definition 7.1.3. Then, let $\chi_{C'}$ be The algorithm set $\phi_{\boldsymbol{x}}$ to:

$$\boldsymbol{x^0} \doteq \boldsymbol{x} \wedge \bigwedge_{j=0}^{n-2} \bigvee_{\boldsymbol{a}\in A_b^d} \boldsymbol{x^{j+1}} + b^j\boldsymbol{a} \doteq \boldsymbol{x^j},$$

$\phi_{\boldsymbol{t}}$ to:

$$\begin{array}{l}\left[t^0_{q_0} \doteq 0\right] \wedge \left\{\bigwedge_{j=0}^{n-1}\bigwedge_{q\neq q'\in Q} t^j_q \not\doteq 0 \vee t^j_{q'} \not\doteq 0\right\}\wedge \\ \left\{\bigwedge_{j=0}^{n-2}\bigvee_{q\in Q}\bigvee_{\boldsymbol{a}\in A_b^d}\left(t^j_q \doteq 0 \wedge \boldsymbol{x^{j+1}} + b^j\boldsymbol{a} \doteq \boldsymbol{x^j}\right)\Longrightarrow t^{j+1}_{\delta(q,\boldsymbol{a})} \doteq 0.\right\},\end{array}$$

and $\phi_{1,\mathbb{N}}^{A'}$ to:

$$\exists^+\left(t^j_q\right)_{j\in[n-1],q\in Q}.\exists^\nu\left(\boldsymbol{x}^j\right)_{j\in[n-1]}.\phi_{\boldsymbol{x}}\wedge\phi_{\boldsymbol{t}}\wedge\phi_Q.$$

The algorithm returns $\phi_{1,\mathbb{N}}^{A'}$.

This algorithm is now proven. Note that the proof of Theorem 7.1.16 uses Proposition 10.4.4, which states that the algorithm *CEF'*($\mathcal{V}_\iota^{\mathbb{N}}$) behaves indeed as described above.

Theorem 7.2.14. *Let $\mathcal{V}_\iota^{\mathbb{N}}$ be a set of $\mathbb{V}_+$. Let $\mathcal{A}$ be an automaton such that for each cyclic state q, $\overline{\mathcal{A}_q}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable. The algorithm* CEF($\mathcal{V}_\iota^{\mathbb{N}}$) *outputs in time:*

$$O\left(n^3 2^d d\log(b)\left(\log(n)+d^2\right)\right),$$

a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula $\phi_{\mathcal{A}}$ of length:

$$O\left(n^3\log(b)\left(\log(n)d^2+2^d\right)\right),$$

which accepts $\overline{\mathcal{A}}^{\mathbb{N}}$.

When b and d are fixed, the length is $O\left(n^3\log(n)\right)$. To prove this algorithm, the following lemma is needed.

Proof. The minimal automaton A' of $\mathcal{A}$ can be computed in time $O\left(nb^d\right)$.

Intuitively, the formula simulates the runs of the automaton A' on the n first letters of the word $\boldsymbol{w} = \underline{\boldsymbol{x}}_{\mathbb{N}}$. The first n states of the simulation are denoted by $q_0,\ldots,q_{n-1}$. Let us prove that the nth state of a run is cyclic. Let us first prove that the ith state is cyclic for some $i < n$. In each complete automaton, at least one state is cyclic. Hence, if the n states belong to the run, one of the q_i is cyclic. Otherwise, a state q_i appears twice in the run, hence is cyclic. By Corollary 9.4.4, since A' is minimal, the set of cyclic states of A' is closed under taking transition, hence q_{n-1} is cyclic.

By Proposition 10.4.4, the algorithm *CEF'*($\mathcal{V}_\iota^{\mathbb{N}}$) returns a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula ϕ_q which defines $\overline{\mathcal{A}_q}^{\mathbb{N}}$

In order to prove that $\phi_{1,\mathbb{N}}^{A'}$ defines $\overline{A'}^{\mathbb{N}}$, that is $\overline{\mathcal{A}}^{\mathbb{N}}$, a word must be said about the formulas $\phi_{\boldsymbol{x}}$, $\phi_{\boldsymbol{t}}$ and $\phi_{1,\mathbb{N}}^{A'}$:

- The formula $\phi_{\boldsymbol{x}}$ asserts that the n d-tuples of variables $\left(\boldsymbol{x^j}\right)_{j\in[n-1]}$ are such that $\boldsymbol{x^j} = b^j\left\lfloor\frac{\boldsymbol{x}}{b^j}\right\rfloor$.
- The formula $\phi_{\boldsymbol{t}}$ asserts that t_q^j holds if and only if the jth state of the run is the state q for each $j \in [n-1]$ and for each state q of A'.
- Finally, the formula ϕ_Q states that A'_q accepts $\left\lfloor\frac{\boldsymbol{x^{n-1}}}{b^{n-1}}\right\rfloor$.

Hence, the conjunction of those three formulas states that $\boldsymbol{x}$ is accepted by A'.

Let us now study the computation time, it gives an upper bound of the length of $\phi_{\mathcal{A}}$.

There are $O(n)$ cyclic states. The Proposition 10.4.4 returns in time:

$$O\Big(n^3 2^d d\log(b)\Big(\log(n)+d^2\Big)\Big),$$

a formula of size

$$O\Big(n\Big(\log(n)d^2+2^d\Big)\Big).$$

Then, the algorithm of Lemma 7.2.12 returns in time $O\Big(n\log(b)n\Big(\log(n)d^2+2^d\Big)\Big) = O\Big(n^3\log(b)\Big(\log(n)d^2+2^d\Big)\Big)$. Finally, the whole algorithm runs in time:

$$O\Big(n^3\log(b)\Big(\log(n)d^2+2^d\Big)\Big).$$

□

7.2.2 Initially-Cyclic Automata

The $\Sigma_0\Big[\mathcal{V}_\iota^{\mathbb{N}}\Big]/\nu$-definable sets which are accepted by an initially-cyclic automaton are logically characterized in this section. As shown in the previous section, in Proposition 7.2.10, the problem considered in this part is solved over the set of all automata as soon as it is solved over the set of initially-cyclic automata.

The main result of this section is that a $\Sigma_0\Big[\mathcal{V}_\iota^{\mathbb{N}}\Big]/\nu$-definable set is accepted by an initially-cyclic automaton if and only if it belongs to the fragment $\Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$ which is introduced in Section 7.2.2.2. Some intermediate fragments $\Sigma_0\Big[\mathcal{V}_\iota^{\mathbb{N}}(e,a,M)\Big]/\nu$ and $\Sigma_0[\mathcal{V}'_\iota]/\nu$ are first introduced in Section 7.2.2.1. These fragments satisfy the following inclusion:

$$\Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu \subseteq \Sigma_0[\mathcal{V}'_\iota]/\nu \subseteq \Sigma_0\Big[\mathcal{V}_\iota^{\mathbb{N}}(e,a,M)\Big]/\nu \subseteq \Sigma_0\Big[\mathcal{V}_\iota^{\mathbb{N}}\Big]/\nu.$$

7.2.2.1 The Fragment $\Sigma_0\Big[\mathcal{V}_\iota^{\mathbb{N}}(e,a,M)\Big]/\nu$

The first fragment of the logic is defined by restricting the vocabulary.

The vocabulary $\mathcal{V}_\iota^{\mathbb{N}}(e,a,M)$ is parametrized by two integers e and a and by a set M of integers. The e parameter restricts the constants used in equality predicate, the a parameter restricts the constants used in addition predicate and the M parameter restricts the modulus used in this vocabulary. Those restrictions are used for inductive proofs.

Definition 7.2.15. For all integers $a \in \mathbb{N}^{>0}$, $e \in \mathbb{N}$, $M \subseteq \mathbb{N}^{>0}$, let $\mathcal{V}_\iota^{\mathbb{N}}(e,a,m)$ denote the subset of $\mathcal{V}_\iota^{\mathbb{N}}$ which contains exactly:

- $\doteq c$ if only if $c \leq e$,
- $\doteq$,
- $<$ if and only if it belongs to $\mathcal{V}_\iota^{\mathbb{N}}$.
- $+c$ if and only if $c \leq a$.
- $\bmod m$ if and only if $m \in M$.

Since each formula uses a finite number of predicates, the following lemma holds:

Lemma 7.2.16. *Let $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, there exists $a \in \mathbb{N}^{>0}$, $e \in \mathbb{N}$, $M \subseteq \mathbb{N}^{>0}$ such that $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}(e,a,M)\right]/\nu$.*

The following lemma explains how taking the quotient of a formula relates to the syntactical fragments of the logic.

Lemma 7.2.17. *Let $a \in \mathbb{N}^{>0}$, let $e \in \mathbb{N}$ and let $m \in \mathbb{N}^{>0}$. Let $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}(e,a,\{m\})\right]/\nu$ and let $\boldsymbol{w} \in \left(A_b^d\right)^*$.*

The formula $\boldsymbol{w}^{-1}\phi$ belongs to

$$\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\left(\left\lfloor\frac{e}{b^{|\boldsymbol{w}|}}\right\rfloor, \left\lfloor\frac{a-1}{b^{|\boldsymbol{w}|}}\right\rfloor + 1, \left\{\frac{m}{\gcd(m, b^{|\boldsymbol{w}|})}\right\}\right)\right]/\nu.$$

Proof. By induction on ϕ, the induction cases are trivial, the base cases are now proven:

- Let us assume that ϕ is $x_i \doteq x_j + c$. By hypothesis $c \leq a$.

  Two cases must be considered: If $\overline{w_i}^{\mathbb{N}} \not\equiv \overline{w_j}^{\mathbb{N}} + c \mod b^n$ then $\boldsymbol{w}^{-1}\phi$ is the formula False, which belongs to all logic considered in this part.

  Otherwise $\overline{w_i}^{\mathbb{N}} \equiv \overline{w_j}^{\mathbb{N}} + c \mod b^n$. Then $\boldsymbol{w}^{-1}\phi$ is the formula $x_i \doteq x_j + \frac{c - \overline{w_i}^{\mathbb{N}} + \overline{w_j}^{\mathbb{N}}}{b^{|\boldsymbol{w}|}}$. It remains to prove that $\frac{c - \overline{w_i}^{\mathbb{N}} + \overline{w_j}^{\mathbb{N}}}{b^{|\boldsymbol{w}|}} \leq \left\lfloor\frac{a-1}{b^{|\boldsymbol{w}|}}\right\rfloor + 1$.

  Since $\overline{w_i}^{\mathbb{N}} \geq 0$ and since $\overline{w_j}^{\mathbb{N}} \leq b^{|\boldsymbol{w}|} - 1$, $c - \overline{w_i}^{\mathbb{N}} + \overline{w_j}^{\mathbb{N}} \leq a + b^{|\boldsymbol{w}|} - 1$, which implies that

  $$\frac{c - \overline{w_i}^{\mathbb{N}} + \overline{w_j}^{\mathbb{N}}}{b^{|\boldsymbol{w}|}} \leq \left\lfloor\frac{a + b^{|\boldsymbol{w}|} - 1}{b^{|\boldsymbol{w}|}}\right\rfloor = \left\lfloor\frac{a-1}{b^{|\boldsymbol{w}|}}\right\rfloor + 1.$$

- The proof is similar for the case $x_i \doteq c$.
- Let us assume that ϕ is $x_i \equiv c \mod m$. Let $g = \gcd(b^n, m)$. Two cases must be considered. If g does not divide $c - \overline{w_i}^{\mathbb{N}}$ then $\boldsymbol{w}^{-1}\phi$ is the formula False.

  Otherwise, let us assume that g divides $c - \overline{w_i}^{\mathbb{N}}$. Let $b' = \frac{b^n}{g}$ and let b'^{-1} be the inverse of b' modulo $\frac{m}{g}$. Then $\boldsymbol{w}^{-1}\phi$ is $x_i \equiv c \times b'^{-1} \bmod \frac{m}{g}$.
- There is nothing to prove for the case $x_i < x_j$.

□

It should be noted that, for $e \geq 0$ and $a \geq 1$, when $|\boldsymbol{w}|$ is great enough then $\left\lfloor\frac{e}{b^{|\boldsymbol{w}|}}\right\rfloor$ is equal to 0 and $\left\lfloor\frac{a-1}{b^{|\boldsymbol{w}|}}\right\rfloor + 1$ is equal to 1. The following definition introduces the function giving the value of $\frac{m}{\gcd(m, b^{|\boldsymbol{w}|})}$ when $|\boldsymbol{w}|$ is great enough.

Definition 7.2.18 ($C_b(m)$, $c_b(m)$)**.** Let $b \in \mathbb{N}^{>0}$ and $m \in \mathbb{N}$. Let $C_b(m)$ be the greatest divider of m which is coprime with b. Let $c_b(m)$ be the least integer such that $m/C_b(m)$ divides $b^{c_b(m)}$.

An example is now given.

Example 7.2.19. Consider $m = 45$ and $b = 6$, then $C_6(45) = 5$ since $6 = 2 \times 3$ and $45 = 3^2 \times 5$. Then $c_b(m) = 2$, since $m/C_b(m) = \frac{45}{5} = 9$ divides $b^{c_b(m)} = 6^2 = 36$ while 9 does not divide 6.

This definition can also be given in term of the prime decomposition of m and b. Let us assume that m and b have q prime numbers in common, $p_0, \ldots, p_{q-1}$, in their prime decomposition. Then $m = c \times \prod_{i=0}^{q-1} p_i^{a_i}$ and $b = c' \times \prod_{i=0}^{a-1} p_i^{a'_i}$ with $a_i, a'_i > 0$, c coprime to c', and the p_i's do not divide c and c'.
Then $C_b(m) = \prod_{i=0}^{q-1} p_0^{a_0} \times \cdots \times p_{j-1}^{a_{j-1}}$ and $c_b(m) = \max\left\{\left\lceil \frac{a_i}{a'_i} \right\rceil \mid i \in [q-1]\right\}$.
In particular, if m is coprime to b then $C_b(m) = m$.

The following corollary states that, for any formula ϕ, when a word $\boldsymbol{w}$ is long enough, $\boldsymbol{w}^{-1}\phi$ belongs to a restricted logic. This logic is introduced in the following definition.

***Definition 7.2.20** ($\mathbb{C}_b$, $\mathcal{V}_\iota'$, $\mathcal{V}_\iota'(m)$)**.** Let $\mathbb{C}_b$ be the set of integers coprime to b.
Let $\mathcal{V}_\iota'$ be the vocabulary $\mathcal{V}_\iota^{\mathbb{N}}(0,1,\mathbb{C}_b)$, it is the intersection of $\{\doteq 0, \doteq, <, +1, \mathrm{mod}\,\mathbb{C}_b\}$ and of $\mathcal{V}_\iota^{\mathbb{N}}$. For $m \in \mathbb{C}_b$, let $\mathcal{V}_\iota'(m)$ be $\mathcal{V}_\iota^{\mathbb{N}}(0,1,\{m\})$, it is the subset of $\mathcal{V}_\iota^{\mathbb{N}}(0,1,\mathbb{C}_b)$ containing only the m modulus.

The above-mentioned corollary is now formally stated.

Corollary 7.2.21. *Let $e, m \in \mathbb{N}$, and $a \in \mathbb{N}^{>0}$, let $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}(e,a,\{m\})\right]$ and let*

$$l_\phi = \max(\log(e+1), \log(a), c_b(m)).$$

Let $\boldsymbol{w} \in \left(A_b^d\right)^*$ of length at least l_ϕ. The formula $\boldsymbol{w}^{-1}\phi$ belongs to $\Sigma_0[\mathcal{V}_\iota']/\nu$.

The proof is a straightforward induction on ϕ. In particular, this corollary implies that a quotient of $\Sigma_0[\mathcal{V}_\iota']/\nu$ belongs to $\Sigma_0[\mathcal{V}_\iota']/\nu$.
An example illustrating the corollary is now given.

Example 7.2.22. Consider the basis $b = 2$ and consider ϕ equal to $x_0 + 2 \doteq x_1 \vee (x_1 \doteq 1 \wedge x_1 \equiv 1 \mod 6)$. Then

$$l_\phi = \max(\log_2(1+1), \log_2(2), c_2(6)) = \max(1,1,1) = 1.$$

The four quotients by a word of length 1 are:

- $(0,0)^{-1}\phi$ equals $x_0 + 1 \doteq x_1 \vee (\mathrm{False} \wedge \mathrm{False})$,
- $(0,1)^{-1}\phi$ equals $\mathrm{False} \vee (x_1 \doteq 0 \wedge x_1 \equiv 0 \mod 3)$,
- $(1,0)^{-1}\phi$ equals $\mathrm{False} \vee (\mathrm{False} \wedge \mathrm{False})$,
- $(1,1)^{-1}\phi$ equals $x_0 + 1 \doteq x_1 \vee (x_1 \doteq 0 \wedge x_1 \equiv 0 \mod 3)$,

and they all belong to $\Sigma_0[\mathcal{V}_\iota']/\nu = \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}(1,0,\mathbb{C}_b)\right]$.

7.2.2.2 The Fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$

The fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$ of $\Sigma_0[\mathcal{V}_\iota']/\nu$ is introduced in this section. This fragment exactly characterizes the subsets of $\mathbb{N}^d$ which are a strict quotient of themselves.

The fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$ is defined as:

$$\bigcup_{\zeta,\beta\subseteq[d-1]|\zeta\cap\beta=\emptyset} \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu,$$

where the fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ is defined in this section, with the two parameters ζ and β restricting the variables that can be used in certain position as argument of the predicates. It is first explained why, to obtain formulas which are strict quotient of themselves, these restrictions are needed.

Let ϕ be a formula, if $x_i + 1 \doteq x_j$ appears in ϕ then x_i is said to be in a predecessor positions and x_j is said to be in a successor position. The sets ζ and β restrict the variables which can be in successor and predecessor position respectively. The following example show why those sets must be restricted.

Example 7.2.23. Let ϕ be the formula $x_0 + 1 \doteq x_1 \vee x_1 + 1 \doteq x_2$. Let us assume that there is a word $\boldsymbol{w}$ such that $\boldsymbol{w}^{-1}\phi = \phi$. Then $\boldsymbol{w}$ is such that $\boldsymbol{w}^{-1}\{x_0 + 1 \doteq x_1\}$ is equal to $x_0 + 1 \doteq x_1$. By Definition 7.2.1, it implies that $(1 - \overline{w_0}^{\mathbb{N}} + \overline{w_1}^{\mathbb{N}})/b^{|\boldsymbol{w}|} = 1$. Hence $-\overline{w_0}^{\mathbb{N}} + \overline{w_1}^{\mathbb{N}} = b^{|\boldsymbol{w}|} - 1$. Since $\overline{w_0}^{\mathbb{N}}$ and since $\overline{w_1}^{\mathbb{N}}$ belong to $[b^{|\boldsymbol{w}|} - 1]$, then $\overline{w_0}^{\mathbb{N}} = 0$ and $\overline{w_1}^{\mathbb{N}} = b^{|\boldsymbol{w}|} - 1$, hence $w_0 \in 0^+$ and $w_1 \in (b-1)^+$.

Similarly $\boldsymbol{w}^{-1}\{x_1 + 1 \doteq x_2\}$ is equal to $x_1 + 1 \doteq x_2$. Hence $w_1 \in 0^+$ and $w_2 \in (b-1)^+$. It implies that $w_1 \in 0^+ \cap (b-1)^+ = \emptyset$, which is a contradiction.

This contradiction is due to the fact that x_1 is both in a successor and in a predecessor position. This is why the set of successor positions and the set of predecessor positions are disjoint in $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$.

For similar reason, the variables which are compared to 0 should not be in predecessor position, hence the set ζ restricts the variables which can be compared to 0.

Furthermore, in the formula $x_0 + 1 \doteq x_1 \wedge x_1 \doteq x_2$, the variable x_2 is also said to be in a successor position, since it is equal to a variable in successor position. Indeed, it is clear that, if $x_0 + 1 \doteq x_1 \vee x_1 + 1 \doteq x_2$ is not a strict quotient of itself, then $x_1 \doteq x_3 \wedge (x_0 + 1 \doteq x_1 \vee x_3 + 1 \doteq x_2)$ is not a strict quotient of itself either. Hence the sets ζ and β restrict the variables which can be used in equality relations.

The following example explains why the order relation are also restricted in the fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$.

Example 7.2.24. Let ϕ be the formula $x_0 + 1 \doteq x_1 \vee x_1 < x_0$. Let us assume that ϕ is a strict quotient of itself. Then there exists $\boldsymbol{w} \in \left(A_b^d\right)^+$ such that $\boldsymbol{w}^{-1}\phi = \phi$, and, as explained in the previous example, $w_0 \in (b-1)^+$ and $w_1 \in 0^+$, hence $\overline{w_0}^{\mathbb{N}} > \overline{w_1}^{\mathbb{N}}$. It implies that $\boldsymbol{w}^{-1}(x_1 < x_0)$ is $\neg(x_0 < x_1)$, hence $\boldsymbol{w}^{-1}\phi \neq \phi$, which is a contradiction.

The definition of $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$ is now given.

Definition 7.2.25 ($\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$, $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$)**.** Let ζ,β be two disjoint subsets of $[d-1]$. Let $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ denote the fragment of $\Sigma_0[\mathcal{V}_\iota'(m)]/\nu$ which contains exactly as atomic predicates:

1. $x_i \doteq 0$ if and only if $i \in \zeta$,
2. $x_i \doteq x_j$ if and only if $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$, and $(i \in \beta) \Longleftrightarrow (j \in \beta)$,
3. $x_i < x_j$ if and only if [either $i \in \beta$, or $j \in \zeta$, or $i, j \notin \zeta \cup \beta$] and $<$ belongs to $\Sigma_0[\mathcal{V}_\iota'(m)]/\nu$,
4. $x_i + 1 \doteq x_j$ if and only if $i \in \beta$, and $j \in \zeta$,

5. $x_i \doteq c \mod m$ for $c \in [m-1]$ if and only if $\bmod m$ belongs to $\Sigma_0[\mathcal{V}_\iota'(m)]/\nu$.

Let $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$ be the union of $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ for $\zeta,\beta \subseteq [d-1]$ disjoint.

In the case where a state is cyclic, that is, when a set is a strict quotient of itself, the values ζ and β can be given. Let us first introduce a notation for the ζ and β used instead of $\cdot,\cdot$.

Definition 7.2.26 ($\zeta_{\boldsymbol{w}}$, $\beta_{\boldsymbol{w}}$)**.** For $\boldsymbol{w} \in \left(A_b^d\right)^+$, let:

$$\zeta_{\boldsymbol{w}} = \{i \in [d-1] \mid w_i \in 0^+\},$$

and

$$\beta_{\boldsymbol{w}} = \{i \in [d-1] \mid w_i \in (b-1)^+\}.$$

For ϕ a formula, when $\boldsymbol{w}$ is long enough, the quotient of ϕ by $\boldsymbol{w}$ belongs to the fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$. The following lemma proves that the set of $\Sigma_0[\mathcal{V}_\iota']/\cdot,\cdot,\nu$-formulas is invariant under the right action $\cdot^{-1}$.

Lemma 7.2.27. *Let $m \in \mathbb{C}_b$. Let $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$, and let $\boldsymbol{w} \in \left(A_b^d\right)^*$ such that $\overline{w_i}^{\mathbb{N}} + 1 \neq \overline{w_j}^{\mathbb{N}}$ for all $i,j \in [d-1]$. Then $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$.*

Proof. Since $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$, by definition of $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$, there exists ζ and β disjoint such that $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$. Let us prove that $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta \cap \zeta_{\boldsymbol{w}}, \beta \cap \beta_{\boldsymbol{w}}, \nu$.

The proof is by induction on ϕ. The induction cases are trivial. The base cases consist in studying the values of $\boldsymbol{w}^{-1}\phi$ when ϕ is atomic:

- Let us assume that ϕ is $x_i \doteq 0$.Two cases must be considered. Either $w_i \in 0^*$ then $\boldsymbol{w}^{-1}\phi$ is $x_i \doteq 0$, hence $i \in \zeta_{\mathcal{A}}$. Or $w_i \notin 0^*$, and then $\boldsymbol{w}^{-1}\phi$ is the formula False.
- Let us assume that ϕ is $x_i \doteq x_j$.Two cases must be considered: either $w_i = w_j$ then $\boldsymbol{w}^{-1}\phi$ is $x_i \doteq x_j$, hence $(i \in \zeta_{\mathcal{A}}) \Longleftrightarrow (j \in \zeta_{\mathcal{A}})$ and $(i \in \beta_{\mathcal{A}}) \Longleftrightarrow (j \in \beta_{\mathcal{A}})$. Or $w_i \neq w_j$ and $\boldsymbol{w}^{-1}\phi$ is the formula False.
- Let us assume that ϕ is $x_i < x_j$. Then $\boldsymbol{w}^{-1}\phi$ is:
  - $\neg\left(x_i > x_j\right)$ if $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$. In this case $w_i \notin (b-1)^*$ and $w_j \notin 0^*$. Since $w_i \notin (b-1)^*$, $i \notin \beta_{\mathcal{A}}$. Since $w_j \notin 0^*$, $j \notin \zeta_{\mathcal{A}}$. Two cases must be considered, depending on whether ($i \in \zeta_{\mathcal{A}}$ or $j \in \beta_{\mathcal{A}}$) or not.
    - If ($i \in \zeta_{\mathcal{A}}$ or $j \in \beta_{\mathcal{A}}$) then $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta_{\mathcal{A}}, \beta_{\mathcal{A}}, \nu$.
    - Otherwise let us assume that $i \notin \zeta_{\mathcal{A}}$ and $j \notin \beta_{\mathcal{A}}$. Since $i \notin \zeta_{\mathcal{A}}$, $i \notin \beta_{\mathcal{A}}$, $j \notin \beta_{\mathcal{A}}$ and $j \notin \zeta_{\mathcal{A}}$, it follows that $i,j \notin \zeta_{\mathcal{A}} \cup \beta_{\mathcal{A}}$, hence $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta_{\mathcal{A}}, \beta_{\mathcal{A}}, \nu$.
  - $x_i < x_j$ if $\overline{w_i}^{\mathbb{N}} \geq \overline{w_j}^{\mathbb{N}}$. Three cases are possible, depending on which set contains i:
    - If $i \in \beta_{\mathcal{A}}$ then $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta_{\mathcal{A}}, \beta_{\mathcal{A}}, \nu$.
    - If $i \in \zeta_{\mathcal{A}}$ then $w_i \in 0^*$, that is $\overline{w_i}^{\mathbb{N}} = 0$. Since $\overline{w_i}^{\mathbb{N}} = 0$ and since $\overline{w_i}^{\mathbb{N}} \geq \overline{w_j}^{\mathbb{N}}$, $\overline{w_j}^{\mathbb{N}} = 0$, that is $w_j \in 0^*$, hence $j \in \zeta_{\mathcal{A}}$. Since $j \in \zeta_{\mathcal{A}}$, $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta_{\mathcal{A}}, \beta_{\mathcal{A}}, \nu$.
    - If $i \notin \zeta_{\mathcal{A}} \cup \beta_{\mathcal{A}}$, the same disjunction must be considered, depending on the set which contains j.
      - If $j \in \beta_{\mathcal{A}}$ or $j \in \zeta_{\mathcal{A}}$ the proof is similar to the case $i \in \zeta_{\mathcal{A}}$ or $i \in \beta_{\mathcal{A}}$.
      - Let us assume that $j \notin \zeta_{\mathcal{A}} \cup \beta_{\mathcal{A}}$. Since $i,j \notin \zeta_{\mathcal{A}} \cup \beta_{\mathcal{A}}$, $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta_{\mathcal{A}}, \beta_{\mathcal{A}}, \nu$.
- Let us assume that ϕ is $x_i + 1 \doteq x_j$.Three cases must be considered:

– Either $w_i \in (b-1)^*$ and $w_j \in 0^*$. In this case $\boldsymbol{w}^{-1}\phi$ is $x_i + 1 \doteq x_j$ and $i \in \beta \cap \beta_{\boldsymbol{w}}$ and $j \in \zeta \cap \zeta_{\boldsymbol{w}}$.
– Or $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$, this contradicts the hypothesis.
– Or $\boldsymbol{w}^{-1}\phi$ is False otherwise.

- Let us assume that ϕ is $x_i \equiv c \mod m$ then $\gcd(m,b) = 1$, hence $\boldsymbol{w}^{-1}\phi$ is $x_i \equiv c - \overline{w_i}^{\mathbb{N}} \times \left(b^{|\boldsymbol{w}|}\right)^{-1} \bmod m$.

□

The above-mentioned lemma is now proven.

Lemma 7.2.28. *Let $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\nu$. There exists $l'_\phi \in \mathbb{N}$, such that for all $\boldsymbol{w} \in \left(A_b^d\right)^+$ of length at least l'_ϕ, $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$.*

Proof. Let l'_ϕ be the number of atomic predicates of the form $x_i + 1 \doteq x_j$ occurring in ϕ, plus one. Let $\boldsymbol{w}$ be a word of length at least l'_ϕ.

It is now proven that there is a prefix $\boldsymbol{v}$ of $\boldsymbol{w}$ such that $\boldsymbol{v}^{-1}\phi$ belongs to $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$. By the previous lemma, it implies that $\boldsymbol{w}^{-1}\phi$ belongs to $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$. Note that $\underline{ww}_{\mathbb{N}i} + 1 \neq \overline{ww}^{\mathbb{N}}{}_j$.

For $i \leq |\boldsymbol{w}|$, let ϕ_i be the left-quotient of ϕ by the prefix of $\boldsymbol{w}$ of length i. It is defined by induction on i by $\phi_0 = \phi$ and $\phi_i = (\boldsymbol{w}[i-1])^{-1}\phi_{i-1}$. The set of atomic predicates of the form $x_i + 1 \doteq x_j$ occurring in ϕ_{i+1} is a subset of the set of the predicates of the form $x_i + 1 \doteq x_j$ occurring in ϕ_i. Hence, by the pigeon hole principle, there exists $s \in [l'_\phi]$ such that ϕ_s and ϕ_{s+1} have the same set of predicates of the form $x_i + 1 \doteq x_j$.

Let $\zeta = \{i \in [d-1] \mid w[s]_i = 0\}$ and let $\beta = \{i \in [d-1] \mid w[s]_i = (b-1)\}$. Let us show that ϕ_{s+1} is a $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-formula.

The proof is by induction on ϕ, the induction cases are trivial. The base cases are now proven.

- Let us assume that ϕ_s is $x_i \doteq 0$. The formula ϕ_{s+1} is $x_i \doteq 0$ if and only if $w[s]_i \doteq 0$, so if and only if $i \in \zeta$. Otherwise ϕ_{s+1} is the formula False.

- Let us assume that ϕ_s is $x_i \doteq x_j$. Then ϕ_{s+1} is $x_i \doteq x_j$ if and only if $w[s]_i \doteq w[s]_j$, which implies that $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$ and $(i \in \beta) \Longleftrightarrow (j \in \beta)$. Otherwise ϕ_{s+1} is the formula False.

- Let us assume that ϕ_s is $x_i < x_j$. Then ϕ_{s+1} is:

  – $x_i < x_j$ if and only if $w[s]_i \geq w[s]_j$, this can happen in three cases:
    * $w[s]_i = (b-1)$, hence $i \in \beta$,
    * $w[s]_j = 0$, hence $j \in \zeta$ or
    * $b - 1 > w[s]_i \geq w[s]_j > 0$, $w[s]_i \neq b-1$, and $w[s]_j \neq 0$, hence $i, j \notin \zeta \cup \beta$.
  – $\neg\left(x_j < x_i\right)$ if and only if $w[s]_i < w[s]_j$, this can happen in three cases:
    * $w[s]_i = 0$ and $w[s]_j \neq 0$, hence $i \in \zeta$,
    * $w[s]_j = b-1$ and $w[s]_j \neq (b-1)$, hence $j \in \beta$ or
    * $0 < w[s]_i < w[s]_j < b-1$, hence $i, j \notin \zeta \cup \beta$.

- Let us assume that ϕ_s is $x_i + 1 \doteq x_j$. Then ϕ_{s+1} is:

  – $x_i + 1 \doteq x_j$ if $w[s]_j = 0$ and $w[s]_j = (b-1)$, which implies that $i \in \beta$ and $j \in \zeta$,

– by definition of s, the other cases can not happen.

□

Combining Corollary 7.2.21 and Lemma 7.2.28 admits the following corollary:

Corollary 7.2.29. *Let $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$. There exists l'_ϕ such that for every $\boldsymbol{w} \in \left(A_b^d\right)^+$, with $|\boldsymbol{w}| \geq l'_\phi$, the formula $\boldsymbol{w}^{-1}\phi$ belongs to $\Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$.*

Definition 7.2.30 (l'_ϕ)**.** For $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, let $l'_\phi \in \mathbb{N}$ denote the least integer such that $\boldsymbol{w}^{-1}\phi \in \Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$ for all $\boldsymbol{w} \in \left(A_b^d\right)^+$ of length at least l'_ϕ.

By Corollary 7.2.29, such an integer exists. Note that $l'_\phi < l'_{\boldsymbol{w}^{-1}\phi}$ for all $\boldsymbol{w} \in \left(A_b^d\right)^+$ and $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$.

The main proposition of this section is now given. The $\Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$-definable fragment characterizes the $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable sets which are strict quotient of themselves.

Proposition 7.2.31. Let $R \subseteq \mathbb{N}^d$ be a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set and let $\boldsymbol{w} \in \left(A_b^d\right)^+$. Those two properties are equivalent:

1. there exists $n \in \mathbb{N}^{>0}$ such that $(\boldsymbol{w}^n)^{-1}R = R$ and
2. the set R is $\Sigma_0[\mathcal{V}'_\iota]/\zeta_{\boldsymbol{w}}, \beta_{\boldsymbol{w}}, \nu$-definable.

In order to prove this proposition, the following lemma is needed.

Lemma 7.2.32. *Let $\boldsymbol{w} \in A_b^d$, and let m be coprime to b. Let $\omega_{b,m}$ be the order of b modulo m. Then $\overline{\boldsymbol{w}^{\omega_{b,m}}}^{\mathbb{N}} \equiv \mathbf{0} \mod m$.*

Proof. It suffices to see that:

$$\overline{\boldsymbol{w}^{\omega_{b,m}}}^{\mathbb{N}} = \sum_{i=0}^{\omega_{b,m}-1} \overline{\boldsymbol{w}}^{\mathbb{N}} b^{|w|i} = \overline{\boldsymbol{w}}^{\mathbb{N}} \frac{b^{\omega_{b,m}} - 1}{b-1} \equiv \overline{\boldsymbol{w}}^{\mathbb{N}} \frac{0}{b-1} = \mathbf{0} \mod m.$$

□

Proof. Let $R \subseteq \mathbb{N}^d$ be a set defined by a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula ϕ. The equivalence is proven by two implications.

$1 \Longrightarrow 2$ Let us assume that $\boldsymbol{w}^{-1}R = R$.

By Corollary 7.2.29 there exists $l'_\phi \in \mathbb{N}$ such that $\left(\boldsymbol{w}^{l'_\phi}\right)^{-1}\phi$ belongs to $\Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$. Note that $\overline{w_i^2}^{\mathbb{N}} + 1 \neq \overline{w_j^2}^{\mathbb{N}}$, for all $i, j \in [d-1]$, hence by Lemma 7.2.27 $\left(\boldsymbol{w}^{l'_\phi+2}\right)^{-1}\phi$ belongs to $\Sigma_0[\mathcal{V}'_\iota]/\zeta_{\boldsymbol{w}}, \beta_{\boldsymbol{w}}, \nu$.

Let us prove that $\left(\boldsymbol{w}^{l'_\phi+2}\right)^{-1}\phi$ defines R. It implies that R is $\Sigma_0[\mathcal{V}'_\iota]/\zeta_{\boldsymbol{w}}, \beta_{\boldsymbol{w}}, \nu$-definable.

By an easy induction on $i \in \mathbb{N}$, the set $\left(\boldsymbol{w}^i\right)^{-1}R$ is equal to R. By Lemma 7.2.4

$$\overline{(\boldsymbol{w}^i)^{-1}\phi}^{\mathbb{N}} = \left(\boldsymbol{w}^i\right)^{-1}\overline{\phi}^{\mathbb{N}} = \left(\boldsymbol{w}^i\right)^{-1}R = R.$$

In particular, $(\boldsymbol{w}^{l'_\phi+2})^{-1}\phi$ defines R.

$2 \Longrightarrow 1$ Let $m \in \mathbb{C}_b$ such that R is $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta_{\boldsymbol{w}}, \beta_{\boldsymbol{w}}, \nu$-definable.

Let us claim that $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi = \phi$ for all $\phi \in \Sigma_0[\mathcal{V}_\iota']/\zeta, \beta, \nu$. Since R is $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta, \beta, \nu$-definable, it implies that R is a strict quotient of itself.

Let us prove that $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi = \phi$. The proof is by induction on ϕ, the induction cases are trivial, the base cases are now proven:

- if ϕ is $x_i = 0$, then $i \in \zeta_{\boldsymbol{w}}$, hence $w_i \in 0^*$, hence $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi = \phi$.
- if ϕ is $x_i = x_j$, then $(i \in \beta_{\boldsymbol{w}}) \Longleftrightarrow (j \in \beta_{\boldsymbol{w}})$, $(i \in \zeta_{\boldsymbol{w}}) \Longleftrightarrow (j \in \zeta_{\boldsymbol{w}})$, hence $w_i = w_j$, hence $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi = \phi$.
- if ϕ is $x_i < x_j$, then either $i \in \beta_{\boldsymbol{w}}$, or $j \in \zeta_{\boldsymbol{w}}$, or $i, j \notin \zeta_{\boldsymbol{w}} \cup \beta_{\boldsymbol{w}}$. In the three cases, $\overline{(\boldsymbol{w}^{\omega_{b,m}})_i}^{\mathbb{N}} \geq \overline{(\boldsymbol{w}^{\omega_{b,m}})_j}^{\mathbb{N}}$, hence $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi = \phi$.
- if ϕ is $x_i + 1 = x_j$, then $i \in \beta_{\boldsymbol{w}}$, $j \in \zeta_{\boldsymbol{w}}$, hence $w_i \in (b-1)^*$, $w_j \in 0^*$, hence $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi = \phi$.
- if ϕ is $x_i = c \mod m$, then $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi$ equals $x_i \equiv b^{\omega_{b,m}} c + \overline{w_i^{\omega_{b,m}}}^{\mathbb{N}} \mod m$. By Lemma 7.2.32, the formula $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi$ is equal to $x_i \equiv b^{\omega_{b,m}} c \mod m$, and since $b^{\omega_{b,m}} \equiv 1 \mod m$, the formula $(\boldsymbol{w}^{\omega_{b,m}})^{-1}\phi$ is equal to $x_i \equiv c \mod m$, that is, to ϕ.

□

7.2.3 Defining the Automaton $\mathcal{A}'_{\phi,\nu}$

In this section, for $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, the problem of creating an automaton $\mathcal{A}'_{\phi,\nu}$ which accepts $\overline{\phi}^{\mathbb{N}}$ is reduced to a simpler problem.

Definition 7.2.33 ($\mathcal{A}'_{\phi,\nu}$)**.** Let $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\nu$ which does not belong to $\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot, \cdot, \nu$. then $\mathcal{A}'_{\phi,\nu}$ is defined by induction on l_ϕ. For all $\boldsymbol{a} \in A_b^d$, by induction let $\mathcal{A}_{\boldsymbol{a}^{-1}\phi} = \left(Q_{\boldsymbol{a}}, A_b^d, \delta_{\boldsymbol{a}}, q_0, F_{\boldsymbol{a}}\right)$. Then let $\mathcal{A}'_{\phi,\nu}$ be (Q, A, δ, q_0, F), where

- $Q = \{q_0\} \cup \bigcup_{\boldsymbol{a} \in A_b^d} \{(\boldsymbol{a}, q) \mid q \in Q_{\boldsymbol{a}}\}$,
- let F' be $\{q_0\}$ if $\mathbf{0} \in \overline{\phi}^{\mathbb{N}}$, and $\emptyset$ otherwise. Let F be $F' \cup \bigcup_{\boldsymbol{a} \in A_b^d} \{(\boldsymbol{a}, q) \mid q \in F_{\boldsymbol{a}}\}$,
- $\delta(q_0, \boldsymbol{a}) = (\boldsymbol{a}, q_0)$, and $\delta((\boldsymbol{a}, q), \boldsymbol{a}') = (\boldsymbol{a}, \delta_{\boldsymbol{a}}(q, \boldsymbol{a}'))$,

By Corollary 7.2.29, the induction is well-founded. The base case of the induction of Definition 7.2.33 is given in Definition 7.3.39 of the following section.

7.3 Totally Ordered Partitions

In this section, an automaton $\mathcal{A}'_{\phi,\nu}$ which accepts the set defined by $\phi \in \Sigma_0[\mathcal{V}_\iota']/\cdot, \cdot, \nu$ is described. The existence of such an automaton is proven in [BHMV94].

The automaton $\mathcal{A}'_{\phi,\nu}$ is not minimal. Its minimal automaton is described in Chapter 8, using notions introduced in this section.

Let ζ, β two disjoint subsets of $[d-1]$ be fixed in this section, they are parameters as introduced in Section 7.2. The construction of the automaton $\mathcal{A}'_{\phi,\nu}$ depends on the values of ζ and of β. To be more precise, from now on, this automaton is denoted by $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$.

Let $m \in \mathbb{C}_b$ be fixed in this section, it is the only modulus used in the formulas studied in this section. Let $\phi \in \Sigma_0[\mathcal{V}'_\iota(m)]/\cdot,\cdot,\nu$ be fixed in this section. An automaton accepting ϕ is described. It should be noted that there is a finite number of distinct atomic formulas in $\Sigma_0[\mathcal{V}'_\iota(m)]/\zeta,\beta,\nu$. Hence there exists a finite number of $\Sigma_0[\mathcal{V}'_\iota(m)]/\zeta,\beta,\nu$-definable sets.

A mathematical structure, the totally-ordered partitions, representing sets of words is introduced in the first section. The interaction of $\Sigma_0[\mathcal{V}'_\iota(m)]/\zeta,\beta,\nu$-formulas with totally-ordered partitions are explained in Section 7.3.1. The relation between logical formulas and totally-ordered partitions is given in Section 7.3.2. The description of $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ in term of totally-ordered partitions is given in section Section 7.3.3.

7.3.1 Totally Ordered Partitions

In this section, the monoid $\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}$ is introduced, it is the set of *totally ordered* $\nu,\mathcal{V}'_\iota(m)$*-partitions over* $[d-1]$, abbreviated as $(\nu,\mathcal{V}'_\iota)^m$*-tops*.

Intuitively, a $(\nu,\mathcal{V}'_\iota)^m$-top represents a subset of $\left(A_b^d\right)^*$ defined by some set of constraints. Those constraints are of the form $w_i \in 0^*$, $w_i \in (b-1)^*$, $w_i = w_j$, $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$, $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$, $\overline{w_i}^{\mathbb{N}} \equiv c \mod m$ and $|\boldsymbol{w}| \equiv c \mod \omega_{b,m}$ where $\omega_{b,m}$ is the order of b modulo m.

It is called a *totally ordered* partition because, for each $i,j \in [d-1]$ such that $(i \in \nu) \Longleftrightarrow (j \in \nu)$, one of the three following constraints belong to the $(\nu,\mathcal{V}'_\iota)^m$-top: $x_i < x_j$, $x_i = x_j$ or $x_i > x_j$. Furthermore, the set of constraints should be consistent. For example, the constraints $x_i + 1 = x_j$ and $x_i > x_j$ can not both belong to the same $(\nu,\mathcal{V}'_\iota)^m$-top. Hence, $\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}$, the set of $(\nu,\mathcal{V}'_\iota)^m$-tops, partition the set of A_b^d-words.

In this section, a monoid structure is given on $(\nu,\mathcal{V}'_\iota)^m$-tops, and it is explained how they can be used to compute left-quotients of formulas, and furthermore how they can be used as argument of $\Sigma_0[\mathcal{V}'_\iota(m)]/\cdot,\cdot,\nu$-formulas with d free variables.

7.3.1.1 Definition

Before formally defining the set of $(\nu,\mathcal{V}'_\iota)^m$-tops, some notations are introduced in this section.

To avoid any ambiguity, new notations are introduced to formalize constraints.

- The symbol $\mathbb{E}$ stands for equality constraint.
- The symbol $\mathbb{S}$ stands for the "successor" constraint.
- The symbol $\mathbb{P}$ stands for the "predecessor" constraint.
- The symbol $\mathbb{L}$ stands for the "less than" constraint.
- The symbol $\mathbb{G}$ stands for the "greater than" constraint.
- The symbol $\mathbb{O}$ stands for the constraint "belonging to 0^*".
- Finally, the symbol $\mathbb{B}$ stands for the constraint "belonging to $(b-1)^*$".

It must be noted that if the symbol $<$ does not belong to the vocabulary $\mathcal{V}'_\iota(m)$, then the "$\mathbb{L}$" part of the $(\nu,\mathcal{V}'_\iota)^m$-top should be ignored. Hence the next definition gives the sets of useful symbols of constraint.

***Definition 7.3.1** ($I^1_{\mathcal{V}'_\iota}$, $I^2_{\mathcal{V}'_\iota}$)**.** Let $I^1_{\mathcal{V}'_\iota} = \{\mathbb{O},\mathbb{B}\}$. The set $I^2_{\mathcal{V}'_\iota}$ contains exactly:

- $\mathbb{E}$, $\mathbb{S}$, $\mathbb{P}$ and
- $\mathbb{L}$ and $\mathbb{G}$ if $<$ belongs to $\mathcal{V}_\iota'$.

The functions which associate to an A_b^d-word w the constraints satisfied by w are now introduced.

***Definition 7.3.2** ($\text{TOP}^m_{\nu,\mathcal{V}_\iota'}$)**.** Let $\boldsymbol{w} \in \left(A_b^d\right)^*$.

- Let $\text{LENGTH}_{m,b}[\boldsymbol{w}] \in [\omega_{b,m} - 1]$ be the length of $\boldsymbol{w}$ modulo $\omega_{b,m}$. Recall that $\omega_{b,m}$ is the order of b modulo m.
- Let $\text{MODULO}_m[\boldsymbol{w}] \in [m-1]^d$ be the d-tuple such that its ith component is $\overline{w_i}^{\mathbb{N}}$ modulo m.
- Let $\text{POSITION}_{\mathcal{V}_\iota'(m)}[\boldsymbol{w}] \in \left(\mathbb{P}(I^1_{\mathcal{V}_\iota'})\right)^d$ be the d-tuple of subsets of $I^1_{\mathcal{V}_\iota'}$ such that its ith component contains exactly:
  - $\mathbb{O}$ if and only if $w_i \in 0^*$.
  - $\mathbb{B}$ if and only if $w_i \in (b-1)^*$.
- Let $\text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[\boldsymbol{w}] \in \mathbb{P}(I^2_{\mathcal{V}_\iota'})^{d\times d}$ be the $d \times d$-matrix of subsets of $I^2_{\mathcal{V}_\iota'}$ such that its (i,j)th element is the empty set if $i \in \nu \Longleftrightarrow j \notin \nu$, otherwise it contains exactly:
  - $\mathbb{E}$ if and only if $w_i = w_j$.
  - $\mathbb{S}$ if and only if $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$.
  - $\mathbb{P}$ if and only if $\overline{w_i}^{\mathbb{N}} - 1 = \overline{w_j}^{\mathbb{N}}$.
  - $\mathbb{L}$ if and only if $<$ belongs to $\mathcal{V}_\iota'$ and $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$.
  - $\mathbb{G}$ if and only if $<$ belongs to $\mathcal{V}_\iota'$ and $\overline{w_i}^{\mathbb{N}} > \overline{w_j}^{\mathbb{N}}$.

Now, let:

$$\text{TOP}_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \left(\text{POSITION}_{\mathcal{V}_\iota'(m)}[\boldsymbol{w}], \text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[\boldsymbol{w}]\right).$$

Similarly, let:

$$\text{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \left(\text{LENGTH}_{m,b}[\boldsymbol{w}], \text{MODULO}_m[\boldsymbol{w}], \text{TOP}_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})\right).$$

The value of $\text{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ (respectively, $\text{TOP}_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$) is called the $(\nu,\mathcal{V}_\iota')^m$-top (respectively $(\nu,\mathcal{V}_\iota')$-top) of $\boldsymbol{w}$.

For T being $\text{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ or $\text{TOP}_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$, the same notations $\text{MODULO}_m[T]$, $\text{LENGTH}_{m,b}[T]$, $\text{POSITION}_{\mathcal{V}_\iota'(m)}[T]$ and $\text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[T]$ are used to designate the parts of T.

$(\nu,\mathcal{V}_\iota')$-top and $(\nu,\mathcal{V}_\iota')^m$-top are tuple belonging to the set introduced in the following definition:

***Definition 7.3.3** ($\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$)**.** Let:

$$\mathbb{PAIR}_{\nu,\mathcal{V}_\iota'} = \mathbb{P}(I^1_{\mathcal{V}_\iota'})^d \times \mathbb{P}(I^2_{\mathcal{V}_\iota'})^{d\times d}.$$

For $m \in \mathbb{C}_b$ let

$$\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'} = [\omega_{b,m} - 1] \times [m-1]^d \times \mathbb{PAIR}_{\nu,\mathcal{V}_\iota'}.$$

A name is now given to the images of $\text{TOP}_{\nu,\mathcal{V}_\iota'}$ and of $\text{TOP}^m_{\nu,\mathcal{V}_\iota'}$.

***Definition 7.3.4** ($\mathbb{TOP}_{\nu,\mathcal{V}_\iota'}$, $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$)**.** Let $\mathbb{TOP}_{\nu,\mathcal{V}_\iota'}$ be

$$\left\{\text{TOP}_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \mid \boldsymbol{w} \in \left(A_b^d\right)^*\right\}.$$

Similarly, let $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ be

$$\left\{\text{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \mid \boldsymbol{w} \in \left(A_b^d\right)^*\right\}.$$

The inverse function of $\text{TOP}^m_{\nu,\mathcal{V}_\iota'}$ must also be considered.

Notation 7.3.5 ($\underline{T}_{\mathcal{V}_\iota'(m)}$)**.** For $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ and $m \in \mathbb{C}_b$, let $\underline{T}_{\mathcal{V}_\iota'(m)}$ be $\left\{\boldsymbol{w} \in \left(A_b^d\right)^* \mid \text{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T\right\}$.

The set of $(\nu,\mathcal{V}_\iota')^m$-tops, $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$, is a strict subset of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, it is precisely characterized in Section 7.3.1.2.

The different cases of Definition 7.3.2 are straightforward. For example, $\mathbb{E}$ belongs to the set $\text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[\boldsymbol{w}](i,j)$ if the two words w_i and w_j are equals.

An example of image of $\text{TOP}^m_{\nu,\mathcal{V}_\iota'}$ is now given.

Example 7.3.6. Consider the dimension d be 7. Let ν be $\{0,1,2,3\}$. Consider the base b be 4. Let the modulus be $m = 5$. Then the order of b modulo m is $\omega_{b,m} = 2$. Let $\boldsymbol{w} = (0,1,2,3,0,0,3)$, then $\boldsymbol{w}$ satisfies the constraints shown in Table 7.3. The (i,j)th-element of $\text{RELATION}_{\nu,\mathcal{V}_1'(m)}[\boldsymbol{w}]$ is represented in the ith column and the jth row.

$$\left(\begin{array}{ccc|cccccccc}
 & 0 & \mathbb{O} & \mathbb{E} & \mathbb{S},\mathbb{L} & \mathbb{L} & \mathbb{L} & & & \\
 & 1 & & \mathbb{P},\mathbb{G} & \mathbb{E} & \mathbb{S},\mathbb{L} & \mathbb{L} & & & \\
 & 2 & & \mathbb{G} & \mathbb{P},\mathbb{G} & \mathbb{E} & \mathbb{S},\mathbb{L} & & & \\
1, & 3, & \mathbb{B}, & \mathbb{G} & \mathbb{G} & \mathbb{P},\mathbb{G} & \mathbb{E} & & & \\
 & 0 & \mathbb{O} & & & & & \mathbb{E} & \mathbb{E} & \mathbb{L} \\
 & 0 & \mathbb{O} & & & & & \mathbb{E} & \mathbb{E} & \mathbb{L} \\
 & 3 & \mathbb{B} & & & & & \mathbb{G} & \mathbb{G} & \mathbb{E}
\end{array}\right)$$

Table 7.3: T_0

Table 7.4: T_0 of Example 7.3.6

As indicated in Table 7.3, $|\boldsymbol{w}| \equiv 1 \mod 2$, $\overline{w_6}^{\mathbb{N}} \equiv 2 \mod 3$, and $w_6 \in (b-1)^*$, hence the set $\text{POSITION}_{\mathcal{V}_1'(m)}[\boldsymbol{w}](6)$ is $\{\mathbb{B}\}$, which explain the 6th line of the first two vectors. And $\overline{w_1}^{\mathbb{N}} + 1 = \overline{w_2}^{\mathbb{N}}$, which explains that the $(1,2)$th cell is "$\mathbb{S},\mathbb{L}$".

For the sake of readability, many notations concerning $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ are now introduced. Let $i,j \in [d-1]$.

- For $\triangle \in \{\mathbb{E},\mathbb{L},\mathbb{G},\mathbb{S},\mathbb{P}\}$, let $i \triangle_T j$ denote that $\triangle \in \text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[T](i,j)$.
- Let $\mathbb{O}_T$ be the set of $i \in [d-1]$ such that $\text{POSITION}_{\mathcal{V}_\iota'(m)}[T](i)$ contains $\mathbb{O}$.
- Let $\mathbb{B}_T$ be the set of $i \in [d-1]$ such that $\text{POSITION}_{\mathcal{V}_\iota'(m)}[T](i)$ contains $\mathbb{B}$.
- Let $\overline{\mathbb{O}}\,\overline{\mathbb{B}}_T$ be $[d-1] \setminus (\mathbb{O}_T \cup \mathbb{B}_T)$.

Intuitively, in the two following notations, $\bar{\cdot}$ represents the complement of a relation.

- Let $i \; \overline{\mathbb{L}} \; \overline{\mathbb{E}} \; \overline{\mathbb{G}}_T \; j$ denote that neither $i \; \mathbb{L}_T \; j$, nor $i \; \mathbb{E}_T \; j$, nor $i \; \mathbb{G}_T \; j$.
- Let $\mathbb{E} \wr \mathbb{S}_T$ denote the equivalence relation over $[d-1]$ generated by the pairs (i, j) such that $i \; \mathbb{E}_T \; j$ and $i \; \mathbb{S}_T \; j$.

Intuitively, the symbol $\wr$ means that the closure of the union is taken. Appending two symbols without $\wr$ means that the intersection of the relations is considered.

- Let $i \; \mathbb{L} \wr \mathbb{E} \wr \mathbb{S}_T \; j$ denote that $i \; \mathbb{L}_T \; j$ or $i \; \mathbb{E} \wr \mathbb{S}_T \; j$, it corresponds intuitively to the "less than or equal" relation.
- Let $i \; \mathbb{L} \overline{\mathbb{S}}_T \; j$ denote that $i \; \mathbb{L}_T \; j$ holds and not $i \; \mathbb{S}_T \; j$. The notation of $i \; \mathbb{G} \overline{\mathbb{P}}_T \; J$ is defined similarly.
- For I an $\mathbb{E} \wr \mathbb{S}_T$-classes and $j \in [d-1]$, let $I \; \mathbb{L} \wr \mathbb{E} \wr \mathbb{S}_T \; j$ (respectively $I \; \mathbb{L} \overline{\mathbb{S}}_T \; j$) denote that for all $i \in I$, $i \; \mathbb{L} \wr \mathbb{E} \wr \mathbb{S}_T \; j$ (respectively $i \; \mathbb{L} \overline{\mathbb{S}}_T \; j$). For J an $\mathbb{E} \wr \mathbb{S}_T$-classes, $I \; \mathbb{L} \wr \mathbb{E} \wr \mathbb{S}_T \; J$ and $I \; \mathbb{L} \overline{\mathbb{S}}_T \; j$ are defined similarly. Note that $I \; \mathbb{L}_T \; j$ and $I \; \mathbb{L}_T \; J$ are not defined.
- An $\mathbb{E}_T$-class (respectively $\mathbb{E} \wr \mathbb{S}_T$-class) E which contains $i \in E$ such that $i \in \mathbb{O}_T$, is said to be a $\mathbb{E}_T^{\mathbb{O}}$-class (respectively, $\mathbb{E} \wr \mathbb{S}_T^{\mathbb{O}}$-class). There are zero, one or two $\mathbb{O}_T$-classes (respectively $\mathbb{E} \wr \mathbb{S}_T^{\mathbb{O}}$-classes), at most one included in ν and one in disjoint from ν.
- The definition of the $\mathbb{E}_T^{\mathbb{B}}$-classes and $\mathbb{E} \wr \mathbb{S}_T^{\mathbb{B}}$-classes are similar.
- An $\mathbb{E}_T$-class (respectively, $\mathbb{E} \wr \mathbb{S}_T$-class) E is said to be an $\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}$-class (respectively, $\mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}$-class) if it is neither a $\mathbb{E}_T^{\mathbb{O}}$-class nor a $\mathbb{E}_T^{\mathbb{B}}$-class (respectively, neither a $\mathbb{E} \wr \mathbb{S}_T^{\mathbb{O}}$-class nor a $\mathbb{E} \wr \mathbb{S}_T^{\mathbb{B}}$-class).
- If C is an $\mathbb{E} \wr \mathbb{S}_T$-class, let $C_0, \ldots, C_{l-1}$ be the decomposition of C in equivalence classes in increasing order. The class C is said to be of length l.
- Let $|\mathbb{E}_T|$, (respectively $\left|\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}\right|$, respectively $\left|\mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}\right|$) be the number of $\mathbb{E}_T$-classes (respectively of $\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}$-classes, respectively of $\mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}$-classes).
- Let $\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(0), \ldots, \mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(\left|\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}\right| - 1)$ (respectively, $\mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(0), \ldots, \mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(\left|\mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}\right| - 1)$) be a sequence of those sets $\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}$ (respectively, $\mathbb{E} \wr \mathbb{S}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}$) in a non-$\mathbb{L}_T$-decreasing order.

Note that the sequences such as $\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(0), \ldots, \mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(\left|\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}\right| - 1)$ are ambiguously defined, as there may exists many sequence which satisfies the hypothesis. Unless otherwise stated, an arbitrary sequence $\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(0), \ldots, \mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}(\left|\mathbb{E}_T^{\overline{\mathbb{O}} \; \overline{\mathbb{B}}}\right| - 1)$ as in the definition is fixed.

It is possible that $i \in \mathbb{O}_T$ and $i \in \mathbb{B}_T$ simultaneously hold, since the empty word satisfies those two constraints.

7.3.1.2 Image of $\textsc{top}^m_{\nu, \mathcal{V}_\iota'}$

Some element of $\mathbb{QUAD}^m_{\nu, \mathcal{V}_\iota'}$ are not in the image of $\textsc{top}^m_{\nu, \mathcal{V}_\iota'}$. As in the following example.

Example 7.3.7. The element of $\mathbb{QUAD}^m_{\nu, \mathcal{V}_\iota'}$ represented in 1 is not in the image of $\textsc{top}^m_{\nu, \mathcal{V}_\iota'}$, since it is impossible that $\overline{w_0}^{\mathbb{N}} + 1 = \overline{w_0}^{\mathbb{N}}$.

$$\left(0,\boxed{0},\boxed{[}\right],\boxed{\mathbb{S}}\right)$$

Table 7.5: T_1

The image of $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$ is now studied. Let $w \in \left(A^d_b\right)^*$ and let $T = \textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w})$. A list of 21 axioms which characterizes the $(\nu,\mathcal{V}'_\iota)^m$-tops are now given. After each axiom, it is proven that T satisfies this axiom. Then, Lemma 7.3.10 prove that an element of $\mathbb{QUAD}^m_{\nu,\mathcal{V}'_\iota}$ which satisfies those axioms belongs to $\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}$.

In the rest of this section, let $i,j,k \in [d-1]$ be three integers such that either i, j and k all belongs to ν, or i, j and k all belongs to $[d-1] \setminus \nu$.

Axiom 1 ($\mathbb{E}$ equivalence)**.** *The relation $\mathbb{E}$ is an equivalence relation. Namely:*

- $i\ \mathbb{E}_T\ i$,
- *if* $i\ \mathbb{E}_T\ j$ *then* $j\ \mathbb{E}_T\ i$, *and*
- *if* $i\ \mathbb{E}_T\ j$ *and* $j\ \mathbb{E}_T\ k$ *then* $i\ \mathbb{E}_T\ k$.

Proof. If the vocabulary contains the equality, then a position is equal to itself. Otherwise there is no constraint about $\textsc{relation}_{\nu,\mathcal{V}'_\iota(m)}[T](i,i)$.

And the equality is an equivalence relation.

□

Axiom 2 ($i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$)**.** *$i\ \mathbb{S}_T\ j$ is equivalent to $j\ \mathbb{P}_T\ i$. If ($i\ \mathbb{S}_T\ j$ and $i\ \mathbb{S}_T\ k$), or if ($i\ \mathbb{P}_T\ j$ and $i\ \mathbb{P}_T\ k$), then $j\ \mathbb{E}_T\ k$.*

Proof. The first part holds because $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$ if and only if $\overline{w_j}^{\mathbb{N}} - 1 = \overline{w_i}^{\mathbb{N}}$. The second part is similar to the equality axiom. If two positions are successors of the same position, or if they both are predecessor of the same position, then they are equal.

□

Axiom 3 ($i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$)**.** *If $i\ \mathbb{E}_T\ j$ then ($i\ \mathbb{S}_T\ k$ implies $j\ \mathbb{S}_T\ k$) and ($i\ \mathbb{P}_T\ k$ implies $j\ \mathbb{P}_T\ k$).*

Proof. Clearly, if $\overline{w_i}^{\mathbb{N}} = \overline{w_j}^{\mathbb{N}}$ and $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_k}^{\mathbb{N}}$ then $\overline{w_j}^{\mathbb{N}} + 1 = \overline{w_k}^{\mathbb{N}}$.

□

Axiom 4 ($\mathbb{S}$ and $\mathbb{E}$ incompatible)**.** *If $i\ \mathbb{E}_T\ j$ then $i\ \mathbb{S}_T\ j$ does not hold.*

Proof. Clearly, if $\overline{w_i}^{\mathbb{N}} = \overline{w_j}^{\mathbb{N}}$ then $\overline{w_i}^{\mathbb{N}} + 1 \neq \overline{w_j}^{\mathbb{N}}$.

□

Axiom 5 ($\mathbb{S}$ not cyclic)**.** *There are no sequence $i_0,\ldots,i_{l-1}$, such that for all $j \in [l-2]$, $i_j\ \mathbb{S}_T\ i_{j+1}$ and $i_{l-1}\ \mathbb{S}_T\ i$.*

Proof. Indeed, there are no l integers $n_0,\ldots,n_{l-1}$ such that for all $j \in [l-2]$, $n_j + 1 = n_{i+1}$ and $n_{l-1} + 1 = n_0$.

□

Axiom 6 (POSITION$_{\mathcal{V}_\iota'(m)}$ and $\mathbb{E}$ compatible)**.** *If $(i, j \in \mathbb{O}_T$ or $i, j \in \mathbb{B}_T)$ then $i\ \mathbb{E}_T\ j$.*

Proof. Let us assume that $i \in \mathbb{B}_T$ and $j \in \mathbb{B}_T$. Since $i \in \mathbb{B}_T$, $w_i \in (b-1)^*$, since $i \in \mathbb{B}_T$, $w_j \in (b-1)^*$. Since w_i and w_j have the same length, then $w_i = w_j$. Hence $i\ \mathbb{E}_T\ j$.

The case $i \in \mathbb{O}_T$ is similar. □

Axiom 7 (POSITION$_{\mathcal{V}_\iota'(m)}$ and $\mathbb{S}$ compatible)**.** *If $i\ \mathbb{S}_T\ j$ then $j \notin \mathbb{O}_T$ and $i \notin \mathbb{B}_T$.*

Proof. If $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$ then $\overline{w_j}^{\mathbb{N}} > 0$ and $w_i < w_j \leq b^{|\boldsymbol{w}|} - 1$.

□

Axiom 8 ($\mathbb{L}$ asymmetric)**.** *The relation $\mathbb{L}_T$ is asymmetric. Namely, if $i\ \mathbb{L}_T\ j$ holds then $j\ \mathbb{L}_T\ i$ does not hold. Furthermore $i\ \mathbb{L}_T\ j$ is equivalent to $j\ \mathbb{G}_T\ i$.*

Proof. Clearly, $\overline{w_i}^{\mathbb{N}}$ is less than $\overline{w_j}^{\mathbb{N}}$ if and only if $\overline{w_j}^{\mathbb{N}}$ is greater than $\overline{w_i}^{\mathbb{N}}$. Furthermore, it implies that w_j is not less than w_i.

□

Axiom 9 ($\mathbb{L}$ transitive)**.** *The relation $\mathbb{L}_T$ is transitive. Namely, if $i\ \mathbb{L}_T\ j$ and $j\ \mathbb{L}_T\ k$ hold, then $i\ \mathbb{L}_T\ k$ holds.*

Proof. Clearly, $w_i < w_j < w_k$ implies $w_i < w_k$.

□

Axiom 10 ($i\ \mathbb{E}_T\ j$,$i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$)**.** *Let us assume that $i\ \mathbb{E}_T\ j$, then ($j\ \mathbb{L}_T\ k$ implies $i\ \mathbb{L}_T\ k$) and ($k\ \mathbb{L}_T\ i$, then $k\ \mathbb{L}_T\ j$).*

Proof. Clearly, $w_j = w_i < w_k$ implies $w_j < w_k$.

□

Axiom 11 ($\mathbb{L}$ and $\mathbb{E}$ incompatible)**.** *If $i\ \mathbb{E}_T\ j$ then $i\ \mathbb{L}_T\ j$ does not hold.*

Proof. Clearly, if $\overline{w_i}^{\mathbb{N}} = \overline{w_j}^{\mathbb{N}}$ then $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$ does not hold.

□

Axiom 12 (POSITION$_{\mathcal{V}_\iota'(m)}$ and $\mathbb{L}$ compatible)**.** *If [($i \in \mathbb{O}_T$ and $j \notin \mathbb{O}_T$) or ($i \notin \mathbb{B}_T$ and $j \in \mathbb{B}_T$)], and if $\mathbb{L}$ belongs to $I^2_{\mathcal{V}_\iota'}$ then $i\ \mathbb{L}_T\ j$.*

Proof. If $i \in \mathbb{O}_T$ and $j \notin \mathbb{O}_T$, then $\overline{w_i}^{\mathbb{N}} = 0$ and $\overline{w_j}^{\mathbb{N}} \neq 0$, then $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$. The other case is similar.

□

Axiom 13 ($\mathbb{S}$ implies $\mathbb{L}$)**.** *If $\mathbb{L}$ belongs to $I^2_{\mathcal{V}_\iota'}$, then $i\ \mathbb{S}_T\ j$ implies that $i\ \mathbb{L}_T\ j$.*

Proof. If $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$ then $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$.

□

Axiom 14 ($(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$)**.** *If $i\ \mathbb{S}_T\ j$ and $i\ \mathbb{L}_T\ k$ then either $i\ \mathbb{E}_T\ k$ or $i\ \mathbb{L}_T\ k$.*

Proof. Let us assume that $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$ and $\overline{w_i}^{\mathbb{N}} < \overline{w_k}^{\mathbb{N}}$. Since both number are integers, $\overline{w_i}^{\mathbb{N}} + 1 \leq \overline{w_k}^{\mathbb{N}}$ hence $\overline{w_j}^{\mathbb{N}} \leq \overline{w_k}^{\mathbb{N}}$, that is $w_j = w_k$ or $w_j < w_k$.

□

Axiom 15 ($\mathbb{O}$ and mod)**.** *If $i \in \mathbb{O}_T$ then $\textsc{modulo}_m[T]_i = 0$.*

Proof. If $i \in \mathbb{O}_T$, then $\overline{w_i}^{\mathbb{N}} = 0$, hence $\overline{w_i}^{\mathbb{N}} \equiv 0 \mod m$.

□

Axiom 16 ($\mathbb{E}$ and mod)**.** *If $i\ \mathbb{E}_T\ j$ then $\textsc{modulo}_m[T]_i = \textsc{modulo}_m[T]_j$.*

Proof. If $\overline{w_i}^{\mathbb{N}} = \overline{w_j}^{\mathbb{N}}$ then clearly, $\overline{w_i}^{\mathbb{N}} \equiv \overline{w_j}^{\mathbb{N}} \mod m$.

□

Axiom 17 ($\mathbb{S}$ and mod)**.** *If $i\ \mathbb{S}_T\ j$ then $\textsc{modulo}_m[T]_i + 1 = \textsc{modulo}_m[T]_j$.*

Proof. If $\overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}$ then clearly, $\overline{w_i}^{\mathbb{N}} + 1 \equiv \overline{w_j}^{\mathbb{N}} \mod m$.

□

Axiom 18 ($\mathbb{B}$ and mod)**.** *If $i \in \mathbb{B}_T$ then $\textsc{modulo}_m[T]_i = b^{\textsc{length}_{m,b}[T]} - 1 \mod m$.*

Proof. If $w_i \in (b-1)^*$ and $|w_i| \equiv \textsc{length}_{m,b}[T] \mod \omega_{b,m}$, then $\overline{w_i}^{\mathbb{N}} = b^{|\boldsymbol{w}|} - 1 \equiv b^{|\boldsymbol{w} \mod \omega_{b,m}|} - 1 \mod m$.

□

The following axiom considers the case where an element of $\mathbb{O}_T$ and one of $\mathbb{B}_T$ are $\mathbb{E}\mathbb{S}_T$-equivalent. A name is now given to this case.

Definition 7.3.8 (Rigid)**.** Let $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}'_\iota}$ and $l \in \mathbb{N}$. The $(\nu,\mathcal{V}'_\iota)^m$-top T is said to be rigid, if there exists a sequence $s_0, \ldots, s_{l-1}$ such that $s_0 \in \mathbb{O}_T$, $s_k\ \mathbb{S}_T\ s_{k+1}$ for all $k \in [l-2]$ and $s_{l-1} \in \mathbb{B}_T$. The width of T is said to be l.

Example 7.3.9. The $(\nu,\mathcal{V}'_\iota)^m$-top T_0 of Example 7.3.6 is rigid.

Axiom 19 (Rigid case)**.** *If T is rigid of width l for some $l \in \mathbb{N}$ then l is of the form b^c with $c \equiv \textsc{length}_{m,b}[T] \mod \omega_{b,m}$. There exists $\boldsymbol{n} \in [l-1]^d$ such that $T = \textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\underline{\boldsymbol{n}}_{\mathbb{N}})$.*

Proof. If there is a sequence $s_0, \ldots, s_{l-1} \in [d-1]$ which satisfies the definition 7.3.8, then by induction on $j \in [l-1]$, one has $\overline{w_{s_j}}^{\mathbb{N}} = j$, hence $\overline{w_{i_{l-1}}}^{\mathbb{N}} = l-1$, and since $w_{s_{l-1}} \in (b-1)^*$ and $|\boldsymbol{w}| = \textsc{length}_{m,b}[T]$, then l is of the form $b^{c\omega_{b,m}+\textsc{length}_{m,b}[T]}$.

Then, for all $j \in [d-1]$, $\overline{w_j}^{\mathbb{N}} < l$, hence any antecedent of T by $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$ belongs to $[l-1]^d$.

□

This axiom justify the name rigid, indeed, it is the only case where the width of the word in the preimage of T by $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$ is fixed.

Axiom 20 (ν)**.** *Let $l \in [d-1]$ such that $i \in \nu \Longleftrightarrow l \notin \nu$, then $i\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_T\ l$.*

Proof. It means that there is no constraints for variables with different polarities. It holds by definition of $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$.

□

Axiom 21 ($\mathbb{L}$ total order)**.** *If $\mathbb{L}$ belongs to $I^2_{\mathcal{V}'_\iota}$, then exactly one of those three properties holds: $i\ \mathbb{L}_T\ j$, $i\ \mathbb{E}_T\ j$ or $i\ \mathbb{G}_T\ j$.*

Proof. One of those three properties hold: $\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$, $\overline{w_i}^{\mathbb{N}} = \overline{w_j}^{\mathbb{N}}$ or $\overline{w_i}^{\mathbb{N}} > \overline{w_j}^{\mathbb{N}}$.

□

The previous axiom justifies the word «totally» in «totally ordered partition». The set of «partially ordered partitions» is introduced in Chapter 8. It is the subset of $\mathbb{QUAD}^m_{\nu,\mathcal{V}'_\iota}$ which satisfies every axioms but Axiom (21 - $\mathbb{L}$ total order).

The following lemma shows that an element of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_t'}$ which satisfies those 21 axioms belongs to $\mathbb{TOP}^m_{\nu,\mathcal{V}_t'}$.

***Lemma 7.3.10** (From $(\zeta,\beta,\nu,\mathcal{V}_t')^m$-top to words)**.** Let $\mathbb{QUAD}^m_{\nu,\mathcal{V}_t'}$ as in Definition 7.3.3. For each $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_t'}$ which satisfies all of those 21 axioms, there exists $\boldsymbol{w} \in \underline{T}_{\mathcal{V}_t'(m)}$ of length at most $\lceil \log_b(d(m+1)) \rceil + \omega_{b,m}$. This word is computable in time $O\left(d^2 + \omega_{b,m}\right)$.

In particular, this lemma implies that $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_t'}$. Intuitively, the algorithm given in the proof computes the minimal word $\boldsymbol{w}$ such that $\textsc{top}^m_{\nu,\mathcal{V}_t'}(\boldsymbol{w}) = T$.

Proof. Let $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_t'}$ which satisfies all of those 21 axioms. Let us prove that there exists a word $\boldsymbol{w} \in \left(A_b^d\right)^*$ of length at most $\lceil \log_b(dm+1) \rceil + \omega_{b,m} - 1$ such that $\textsc{top}^m_{\nu,\mathcal{V}_t'}(\boldsymbol{w}) = T$. For this, Algorithm 2 computes $\boldsymbol{n} \in \mathbb{N}^d$.

First, properties about the subsets of $[d-1]$ are now given, using the 21 axioms. Those properties are used by the Algorithm 2 for its computation.

By Axioms (1 - $\mathbb{E}$ equivalence), $\mathbb{E}_T$ is an equivalence relation over $[d-1]$. An equivalence class for $\mathbb{E}_T$ is called an $\mathbb{E}_T$-class.

Axioms (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$), (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible) and (5 - $\mathbb{S}$ not cyclic), proves that the successors and predecessors relations behave indeed as a successor relation and are consistent with the equivalence relation. Hence the $\mathbb{E}\wr\mathbb{S}$-relation and the notion of decomposition of $\mathbb{E}\wr\mathbb{S}$-classes introduced in Section 7.3.1.1 can be used.

Axiom (6 - $\textsc{position}_{\mathcal{V}_t'(m)}$ and $\mathbb{E}$ compatible) asserts that the notions of minimality and maximality are consistent with the equality, that is, there exists at most one $\mathbb{E}^{\mathbb{O}}_T$-class included in ν and at most one disjoint from ν, and similarly for the $\mathbb{E}^{\mathbb{B}}_T$-classes. Axiom (7 - $\textsc{position}_{\mathcal{V}_t'(m)}$ and $\mathbb{S}$ compatible) asserts that those notions are consistent with the successor relations. Hence the notion of $\mathbb{E}^{\mathbb{O}}_T$-, $\mathbb{E}\wr\mathbb{S}^{\mathbb{O}}_T$-, $\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_T$-, $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_T$-, $\mathbb{E}^{\mathbb{B}}_T$- and $\mathbb{E}\wr\mathbb{S}^{\mathbb{B}}_T$-classes, introduced in Section 7.3.1.1 after Example 7.3.6, can be used.

By Axioms (8 - $\mathbb{L}$ asymmetric) and (9 - $\mathbb{L}$ transitive) the relation $\mathbb{L}_T$ is a strict partial order. By Axioms (10 - $i\ \mathbb{E}_T\ j, i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$) and (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible), this order is compatible with the equivalence relation $\mathbb{E}_T$. By Axiom (12 - $\textsc{position}_{\mathcal{V}_t'(m)}$ and $\mathbb{L}$ compatible) it is consistent with minimal and maximal values, and by Axioms (13 - $\mathbb{S}$ implies $\mathbb{L}$) and (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$) it is consistent with the successor relation.

Finally, Axioms (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod) and (17 - $\mathbb{S}$ and mod) assert that the modular restrictions are consistent with the $\mathbb{O}_T$ restriction, the $\mathbb{E}_T$ restriction and the $\mathbb{S}_T$ restriction respectively. Axiom (18 - $\mathbb{B}$ and mod) asserts that if $w_i \in (b-1)^*$ and $|w_i| \equiv c \mod \omega_{b,m}$, then $\overline{w_i}^{\mathbb{N}} \equiv b^c - 1 \mod m$.

The algorithm which computes $\boldsymbol{n}$ is now described. When the algorithm starts, $\boldsymbol{n}$ is an array of d symbols $\perp$'s. The values of n_i are computed iteratively for i in an $\mathbb{L}$-non-decreasing order. The values for the $\mathbb{E}\wr\mathbb{S}^{\mathbb{O}}_T$-classes are assigned first, at it is known that their least values is 0. Then the values for the $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_T$-classes are chosen, ensuring:

- that the modular constraints are satisfied,
- that the values assigned to n_1 are positive,
- that their values are not successor of any already assigned value with the same polarity.

Two cases must be considered, depending on whether there is $\mathbb{E}\mathbb{S}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}$-class or not. If there are no $\mathbb{E}\mathbb{S}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}$-class then $\boldsymbol{w}$ is obtained by appending some $\mathbf{0}$ to $\boldsymbol{w}' = \underline{\boldsymbol{n}}_{\mathbb{N}}$, to ensure that for all i, $w_i \notin (b-1)^*$ and that $|\boldsymbol{w}| \equiv \textsc{length}_{m,b}[T] \mod \omega_{b,m}$. Otherwise, if there is one or two $\mathbb{E}\mathbb{S}_T^{\mathbb{B}}$-classes, they are assigned such that their maximal values are the same, their base-b expansion belongs to $(b-1)^*$ and their modular value is the one constrained by T.

Then $\boldsymbol{w}$ can be computed from $\boldsymbol{n}$, adding at most $\omega_{b,m}$ letters to $\underline{\boldsymbol{n}}_{\mathbb{N}}$.

Concerning the length of the word, an induction over the number of assigned positions proves that the ith assigned position in a non $\mathbb{E}\mathbb{S}_T^{\mathbb{B}}$-class is assigned to at most $i(m+1)$. Then, the maximal value for the $\mathbb{B}'$-classes is at most $b^{\omega_{b,m}} d(m+1)$. Then the word $\boldsymbol{w}$ is of length at most $\lceil \log_b(b^{\omega_{b,m}} d(m+1)) \rceil = \omega_{b,m} + \lceil \log_b(d(m+1)) \rceil$.

Finally, for each i, j such that $i \in \nu \Longleftrightarrow j \notin \nu$, $i\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{\boldsymbol{w}}\ j$, and by Axiom (20 - ν), $i\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_T\ j$, hence $\textsc{relation}_{\nu,\mathcal{V}_\iota'(m)}[T](i,j) = \textsc{relation}_{\nu,\mathcal{V}_\iota'(m)}[\boldsymbol{w}](i,j)$. And for each i, j such that $(i \in \nu) \Longleftrightarrow (j \in \nu)$, either $i\ \mathbb{L}_T\ j$, $i\ \mathbb{E}_T\ j$ or $i\ \mathbb{G}_T\ j$, which is asserted by Axiom (21 - $\mathbb{L}$ total order). Which ends the proof that $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T$.

Concerning the computation time, it is first proven that $\boldsymbol{n}$ is computed in time $O\left(d^2\right)$. It is enough to see that d numbers are assigned, and each assignation can be done in time $O(d)$. Then the word $\boldsymbol{w}$ can be computed, adding at most $\omega_{b,m}$ letters. Hence the total computation time is $O\left(d^2 + \omega_{b,m}\right)$.

□

7.3.1.3 $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$'s Product

As stated in the introduction of Section 7.3.1, since the $(\nu,\mathcal{V}_\iota')^m$-tops are abstraction for words, it should be associated to a product operation such that $(\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}, \cdot)$ is a monoid and $(\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}, \cdot)$ a submonoid of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$.

A binary operation over $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, such that $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}$ is a morphism of monoid, is introduced in the following definition. Then $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$, the image of $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}$, is isomorphic to the quotient monoid $\left(A_b^d\right)^* / \textsc{top}^m_{\nu,\mathcal{V}_\iota'}$. Quotient monoids are defined in Section 2.3.1.

***Definition 7.3.11** ($\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$'s product)**.** Let T, U belonging to $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ or to $\mathbb{PAIR}_{\nu,\mathcal{V}_\iota'}$. Let $T \cdot U$ be the binary operation defined for $i, j \in [d-1]$ by:

1. $i \in \mathbb{O}_{T\cdot U}$ if and only if $i \in \mathbb{O}_T$ and $i \in \mathbb{O}_U$.
2. $i \in \mathbb{B}_{T\cdot U}$ if and only if $i \in \mathbb{B}_T$ and $i \in \mathbb{B}_U$.
3. $i\ \mathbb{E}_{T\cdot U}\ j$ if and only if $i\ \mathbb{E}_T\ j$ and $i\ \mathbb{E}_U\ j$.
4. $i\ \mathbb{L}_{T\cdot U}\ j$ if and only if $i\ \mathbb{L}_U\ j$ or ($i\ \mathbb{L}_T\ j$ and $i\ \mathbb{E}_U\ j$).
5. $i\ \mathbb{S}_{T\cdot U}\ j$ if and only if ($i\ \mathbb{S}_U\ j$, $i \in \mathbb{B}_T$ and $j \in \mathbb{O}_T$) or ($i\ \mathbb{S}_T\ j$ and $i\ \mathbb{E}_U\ j$).
6. if $T, U \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, then $\textsc{modulo}_m[T \cdot U]_i = \textsc{modulo}_m[T]_i + b^{\textsc{length}_{m,b}[T]} \textsc{modulo}_m[U]_i$.
7. $\textsc{length}_{m,b}[T \cdot U] = \textsc{length}_{m,b}[T] + \textsc{length}_{m,b}[U]$.

Lemma 7.3.12. *The binary operation $\cdot$ is a semi-group operation over $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ and over $\mathbb{PAIR}_{\nu,\mathcal{V}_\iota'}$.*

The proof is a straightforward case study of each part of the definition.

Example 7.3.6 is now resumed in order to give an example of monoid operation.

Algorithm 2: Computing $\boldsymbol{w}$

Input: $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}'_\iota}$

Let $M_+ := 0$, $M_- := 0$;
Let n be an array of length d initialized to $\perp$;
Function `assign(`n, i`)`
  foreach j *such that* $i\ \mathbb{E}_T\ j$ **do**
    let $n_j := n$;
  end
  let $M_{\nu(i)} := n$; `/* ` $\nu(i)$ `is - if` $i \in \nu$ `and + otherwise */`
  if *there exists* j *such that* $i\ \mathbb{S}_T\ j$ **then**
    `assign(`$n+1$, j`);`
  end
end
foreach $i \in \mathbb{O}_T$ *unassigned* **do**
  `assign(0,`i`);`
end
Let $M_+ := \max(M_+, 1)$ and $M_- := \max(M_-, 1)$;
foreach $i \in \overline{\mathbb{O}}\,\overline{\mathbb{B}}_T$ *unassigned,* $\mathbb{L}$*-minimal* **do**
  let x be the least integer greater than $M_{\nu(i)} + 1$ equivalent to $\textsc{modulo}_m[T]_i$ mod m;
  `assign(`x,i`);`
end
if *for all* $p \in [d-1]$ *such that* $n_p \neq \perp$ **then**
  let $\boldsymbol{w'} := \underline{\boldsymbol{n}}_{\mathbb{N}}$;
  let l be the minimal positive integer equivalent to $\textsc{length}_{m,b}[T] - |w'|$;
  let $\boldsymbol{w} := \boldsymbol{w'0}^l$;
else
  Let l be the maximum length of the $\mathbb{E}\mathbb{S}^{\mathbb{B}}_T$-classes;
  Let x be the least integer of the form $b^{c\omega_{b,m}+\textsc{length}_{m,b}[T]} - 1$ greater than $\max(M_+, M_-) + l + 1$ for some $c \in \mathbb{N}$;
  foreach $\mathbb{E}\mathbb{S}^{\mathbb{B}}_T$*-classes* C *of length* l', $i \in C$, $\mathbb{L}_T$*-minimal* **do**
    `assign(`$x - l'$, i`);`
  end
  Let $\boldsymbol{w} := \underline{\boldsymbol{n}}_{\mathbb{N}}$;
end
return $\boldsymbol{w}$

Example 7.3.13. Consider the dimension d be 7, ν be $\{0,1,2,3\}$, and the base b be 4. Let the modulus be $m = 5$. Then the order of b modulo m be $\omega_{b,m} = 2$.

As in Example 7.3.6, let $\boldsymbol{w} = (0,1,2,3,0,0,3)$ and let $T_0 = \textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w})$ be the $(\nu,\mathcal{V}'_\iota)^m$-top represented in Tables 7.3. Let $\boldsymbol{w'} = (11,33,00,33,00,11,00)$, then $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w'}) = T_2$ represented in Table 7.6. Then

$$\boldsymbol{w'} \cdot \boldsymbol{w} = (110,331,002,333,000,110,003)$$

and $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w'} \cdot \boldsymbol{w}) = T_2 \cdot T_0$, denoted by T_3, is represented in Table 7.7.

The following lemma states that $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$ is a morphism. It implies that $\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}$ is a monoid.

0,	0		$\mathbb{E}$	$\mathbb{L}$	$\mathbb{G}$	$\mathbb{L}$			
	0	$\mathbb{B}$	$\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$	$\mathbb{E}$			
	0	$\mathbb{O}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{E}$	$\mathbb{L}$			
	0	$\mathbb{B}$,	$\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$	$\mathbb{E}$			
	0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{E}$
	0						$\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$
	0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{E}$

Table 7.6: T_2

1,	0		$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{L}$			
	1		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{S},\mathbb{L}$	$\mathbb{L}$			
	2		$\mathbb{G}$	$\mathbb{P},\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$			
	3	$\mathbb{B}$,	$\mathbb{G}$	$\mathbb{G}$	$\mathbb{G}$	$\mathbb{E}$			
	0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$
	0						$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$
	3						$\mathbb{G}$	$\mathbb{G}$	$\mathbb{E}$

Table 7.7: T_3

Lemma 7.3.14. *Let $\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}$ be the set of $(\nu,\mathcal{V}'_\iota)^m$-tops, as introduced in Definition 7.3.2, with the binary operation $\cdot$ introduced in Definition 7.3.11. The function $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$ is a morphism from the monoid $\left(\left(A^d_b\right)^*,\cdot\right)$ to $\left(\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota},\cdot\right)$.*

Proof. The proof is a long but straightforward application of each of the axioms of Definition 7.3.2 and 7.3.11 over two $\left(A^d_b\right)^*$-words.

For all $i,j \in [d-1]$:

- The equivalence of the $\mathbb{O}$-class is straightforward from the definition:

$$\begin{aligned} i \in \mathbb{O}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{v}\boldsymbol{w})} &\iff v_i w_i \in 0^* \\ &\iff v_i \in 0^* \wedge w_i \in 0^* \\ &\iff i \in \mathbb{O}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{v})} \wedge i \in \mathbb{O}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w})} \\ &\iff i \in \mathbb{O}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{v})\cdot\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w})}. \end{aligned}$$

- The $\mathbb{B}$ case is similar.

- The proof of $\mathbb{E}$ is straightforward from the definition:

$$\begin{aligned} i \,\mathbb{E}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{v}\boldsymbol{w})}\, j &\iff v_i w_i = v_j w_j \\ &\iff v_i = v_j \wedge w_i = w_j \\ &\iff i \,\mathbb{E}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{v})}\, j \wedge i \,\mathbb{E}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w})}\, j \\ &\iff i \,\mathbb{E}_{\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{v})\cdot\textsc{top}^m_{\nu,\mathcal{V}'_\iota}(\boldsymbol{w})}\, j \end{aligned}$$

- The proof of $\mathbb{S}$ is similar but uses two cases:

$$\begin{aligned}
i\ \mathbb{S}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{vw})}\ j &\Longleftrightarrow \overline{v_i w_i}^{\mathbb{N}} + 1 = \overline{v_j w_j}^{\mathbb{N}} \\
&\Longleftrightarrow (\overline{v_i}^{\mathbb{N}} + 1 = \overline{v_j}^{\mathbb{N}} \wedge w_i = w_j \qquad)\vee \\
&\quad\ (v_i \in (b-1)^* \ \wedge v_j \in 0^* \qquad \wedge \overline{w_i}^{\mathbb{N}} + 1 = \overline{w_j}^{\mathbb{N}}) \\
&\Longleftrightarrow (i\ \mathbb{S}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v})}\ j \ \wedge i\ \mathbb{E}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}\ j \qquad)\vee \\
&\quad\ (i \in \mathbb{B}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v})} \wedge j \in \mathbb{O}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v})} \wedge i\ \mathbb{S}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}\ j \ \ ) \\
&\Longleftrightarrow i\ \mathbb{S}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v})\cdot\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}\ j.
\end{aligned}$$

- The proof for $\mathbb{L}$ is similar. If $\mathbb{L}$ belongs to $I^2_{\mathcal{V}_\iota'}$:

$$\begin{aligned}
i\ \mathbb{L}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{vw})}\ j &\Longleftrightarrow \overline{v_i w_i}^{\mathbb{N}} < \overline{v_j w_j}^{\mathbb{N}} \\
&\Longleftrightarrow [\overline{v_i}^{\mathbb{N}} < \overline{v_j}^{\mathbb{N}} \quad \wedge w_i = w_j \qquad] \vee \overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}} \\
&\Longleftrightarrow [i\ \mathbb{L}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v})}\ j \wedge i\ \mathbb{E}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}\ j\,] \vee i\ \mathbb{L}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}\ j \\
&\Longleftrightarrow i\ \mathbb{L}_{\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v})\cdot\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}\ j.
\end{aligned}$$

Since $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}$ is a surjective morphism, its image is also a monoid. Its neutral element, denoted by $1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$, is $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\epsilon)$. Then $1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$ is such that for all $i,j \in [d-1]$, $\mathrm{POSITION}_{\mathcal{V}_\iota'(m)}\left[1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}\right](i) = I^1_{\mathcal{V}_\iota'}$ where $I^1_{\mathcal{V}_\iota'}$ is the set of unary relations, introduced in Definition 7.3.1, and $\mathrm{RELATION}_{\nu,\mathcal{V}_\iota'(m)}\left[1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}\right](i,j)$ is $\{\mathbb{E}\}$ if $(i \in \nu) \Longleftrightarrow (j \in \nu)$ and $\emptyset$ otherwise. □

The previous lemma implies the following corollary.

Corollary 7.3.15. *The pair* $(\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}, \cdot)$ *is a monoid.*

Proof. The image of a monoid by a morphism is a monoid. □

Using this morphism and the product operation, a right action $\cdot$ of $\left(A^d_b\right)^*$ over $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ is now introduced.

Definition 7.3.16. For $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ and $\boldsymbol{w} \in \left(A^d_b\right)^*$, let $T \cdot \boldsymbol{w}$ denote $T \cdot \mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$.

7.3.1.4 Adding ζ and β

This section deals with the relation between $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\zeta,\beta,\nu$-formulas introduced in Section 7.2.2.2 and $(\nu,\mathcal{V}_\iota')^m$-tops.

The set $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, which is now defined, is a subset of $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$. Its elements are called the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top.

Definition 7.3.17 (ζ,β-totally ordered partition)**.** Let ζ,β be some disjoint subsets of $[d-1]$. Let $\mathbb{PAIR}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ denote the subsets of $\mathbb{PAIR}_{\nu,\mathcal{V}_\iota'}$ and of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ respectively which contains exactly the elements T such that, for all $i,j \in [d-1]$:

a. if $i \in \mathbb{O}_T$ then $i \in \zeta$,

b. if $i \in \mathbb{B}_T$ then $i \in \beta$,

c. if $i\ \mathbb{S}_T\ j$ then $i \in \beta$, $j \in \zeta$,

d. if $i \quad \mathbb{E}_T \quad j$ then $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$, and $(i \in \beta) \Longleftrightarrow (j \in \beta)$,

Let $\mathbb{TOP}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} = \mathbb{TOP}_{\nu,\mathcal{V}_\iota'} \cap \mathbb{PAIR}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'} = \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'} \cap \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. The elements of $\mathbb{TOP}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ are called the $(\zeta,\beta,\nu,\mathcal{V}_\iota'(m))$-totally ordered partitions, abbreviated as "$(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops".

The definition of $\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is similar to the fragment $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ introduced in Definition 7.2.25. The only difference between the definitions of $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ and of $\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is that there is no restriction on the order which can appear in $\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

Note that, for $T \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $U \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, the product satisfy the following properties.

- $i\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{T\cdot U}\ j$ holds if and only if $i\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_U\ j$ or ($i\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_T\ j$ and $i\ \mathbb{E}_T\ j$).
- $i\ \mathbb{L}\overline{\mathbb{S}}_{T\cdot U}\ j$ holds if and only if:
  - $i\ \mathbb{L}\overline{\mathbb{S}}_T\ j$ and $i\ \mathbb{E}_U\ j$, or
  - (either $j \notin \mathbb{B}_T$ or $i \notin \mathbb{O}_T$) and $i\ \mathbb{S}_U\ j$, or
  - $i\ \mathbb{L}\overline{\mathbb{S}}_U\ j$.
- $i\ \mathbb{E}\wr\mathbb{S}_{T\cdot U}\ j$ is equivalent to:
  - ($i\ \mathbb{E}\wr\mathbb{S}_T\ j$ and $i\ \mathbb{E}_U\ j$), or
  - ($j \in \mathbb{O}_T$ and $i \in \mathbb{B}_T$ and $i\ \mathbb{S}_U\ j$) or
  - ($i \in \mathbb{O}_T$ and $j \in \mathbb{B}_T$ and $j\ \mathbb{S}_U\ i$).

Furthermore, if $T,U \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $i\ \mathbb{E}\wr\mathbb{S}_T\ j$ then ($i\ \mathbb{E}_U\ j$ implies $i\ \mathbb{E}_T\ j$) and ($i\ \mathbb{S}_U\ j$ implies $i\ \mathbb{S}_T\ j$).

For T a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top, $\mathbb{O}_T$ and $\mathbb{B}_T$ are subsets of ζ and of β respectively. Example 7.3.13 is now resumed.

Example 7.3.18. Consider $\zeta = \{2,4,6\}$ and $\beta = \{1,3\}$. Let T_2 and T_3 be the $(\nu,\mathcal{V}_\iota')^m$-top as in Example 7.3.6 and 7.3.13. They belong to $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. On the other hand, T_0 of example 7.3.6 does not belong to $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ as $5 \in \mathbb{O}_{T_0}$ and $5 \notin \zeta$.

On the one hand the set $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is not a submonoid of $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$, indeed $1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}} \notin \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. For the sake of contradiction, let us assume that $1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}} \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, since $0 \in \mathbb{O}_{1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}}$, $0 \in \zeta$, hence $0 \notin \beta$, and finally $0 \in \mathbb{B}_{1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}}$ does not hold, which is a contradiction.

On the other hand, the following lemma states that $\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is invariant under the right action $\cdot$ of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$:

Lemma 7.3.19. *The set $\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is invariant for the right action $\cdot$ of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ on $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$.*

Proof. Let $T \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $U \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$.

a.. If $i \in \mathbb{O}_{T\cdot U}$ then $i \in \mathbb{O}_T$, hence $i \in \zeta$.

b.. If $i \in \mathbb{B}_{T\cdot U}$ then $i \in \mathbb{B}_T$, hence $i \in \beta$.

c.. If $i\ \mathbb{S}_{T\cdot U}\ j$ then

- either $i\ \mathbb{S}_T\ j$ and $i\ \mathbb{E}_U\ j$, hence $i \in \beta, j \in \zeta$, or
- $i\ \mathbb{S}_U\ j$, $i \in \mathbb{B}_T$ hence $i \in \beta$, and $j \in \mathbb{O}_T$ hence $j \in \zeta$.

d.. If $i \mathbb{E}_{T\cdot U} j$ then $i \mathbb{E}_T j$, hence $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$, and $(i \in \beta) \Longleftrightarrow (j \in \beta)$.

□

The previous lemma has the following corollary:

Corollary 7.3.20. *The set $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is invariant for the right action $\cdot$ of $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ on $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$.*

Proof. Let $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $U \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$. By Lemmas 7.3.15, $T\cdot U \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ and by Lemma 7.3.19, $T \cdot U \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, hence $T \cdot U \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. □

Note that, even if it can easily be shown that the pair $\left(\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}, \cdot\right)$ is a semigroup, this is never used in this part. Indeed, the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top represents the state of the automaton while the $(\nu,\mathcal{V}_\iota')^m$-top represents the word, and there is no reason to consider product of states.

A function $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is now introduced, which associates to each word $\boldsymbol{w}$ the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top the most similar to $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$. For this, we first define the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top which is the initial state of the automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$. It is the element of $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ which is the most similar to $1_{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$.

Definition 7.3.21. Let $\nu \subseteq [d-1]$. Let $\zeta, \beta \subseteq [d-1]$ be two disjoint subsets, then $T_{\zeta,\beta,\nu}$ is the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top such that for all $i,j \in [d-1]$, if $i \in \nu \Longleftrightarrow j \notin \nu$ then $i \overline{\mathbb{L}}\,\overline{\mathbb{E}}\,\overline{\mathbb{G}}_{T_{\zeta,\beta,\nu}} j$, otherwise:

- $i \mathbb{E}_{T_{\zeta,\beta,\nu}} j$ if and only if $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$ and $(i \in \beta) \Longleftrightarrow (j \in \beta)$.
- $i \mathbb{L}_{T_{\zeta,\beta,\nu}} j$ if and only if $(i \in \zeta$ and $j \notin \zeta)$ or $(i \notin \beta$ and $j \in \beta)$.
- $i \in \mathbb{O}_{T_{\zeta,\beta,\nu}}$ if and only if $i \in \zeta$.
- $i \in \mathbb{B}_{T_{\zeta,\beta,\nu}}$ if and only if $i \in \beta$.
- $i \mathbb{S}_{T_{\zeta,\beta,\nu}} j$ does not hold.

An example of a particular value of $T_{\zeta,\beta,\nu}$ is now given.

Example 7.3.22. Consider $\zeta = \{1,3,5\}$, $\beta = \{4,6\}$ and $\nu = \{0,4,5,6\}$. Then $T_{\zeta,\beta,\nu}$ is equal to the $(\nu,\mathcal{V}_\iota')^m$-top T_1 of example 7.3.6.

The function $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ can now be defined.

Definition 7.3.23 ($\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$)**.** For $\boldsymbol{w} \in \left(A_b^d\right)^*$, let $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ denote $T_{\zeta,\beta,\nu} \cdot \boldsymbol{w}$.

The function $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ can be equivalently defined as follow:

Lemma 7.3.24. *Let $\boldsymbol{w} \in \left(A_b^d\right)^*$.*

- *$i \in \mathbb{O}_{\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}$ holds if and only if $i \in \zeta$ and $w_i \in 0^*$,*
- *$i \in \mathbb{B}_{\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}$ holds if and only if $i \in \beta$ and $w_i \in (b-1)^*$,*
- *$i \mathbb{E}_{\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})} j$ holds if and only if $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$ and $(i \in \beta) \Longleftrightarrow (j \in \beta)$ and $w_i = w_j$,*
- *$i \mathbb{S}_{\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})} j$ holds if and only if $j \in \zeta$ and $i \in \beta$ and $w_i + 1 = w_j$,*

- *i $\mathbb{L}_{\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})}$ j holds if and only if $<$ belongs to $\mathcal{V}_\iota'$ and $\{\overline{w_i}^{\mathbb{N}} < \overline{w_j}^{\mathbb{N}}$ or $[w_i = w_j$ and $<(i \in \zeta, j \notin \zeta)$ or $(i \notin \beta$ and $j \in \beta)>]\}$,*

The proof is straightforward from the definition. Note that:

$$\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \left(\mathrm{LENGTH}_{m,b}[\boldsymbol{w}], \mathrm{MODULO}_m[\boldsymbol{w}], \mathrm{POSITION}_{\zeta,\beta,\mathcal{V}_\iota'(m)}[\boldsymbol{w}], \mathrm{RELATION}_{\zeta,\beta,\nu,\mathcal{V}_\iota'(m)}[\boldsymbol{w}]\right),$$

and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is equal to $\left\{\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \mid \boldsymbol{w} \in \left(A_b^d\right)^*\right\}$.

The function $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is not a morphism, indeed $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \neq \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \cdot \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\varepsilon)$ for some words $\boldsymbol{w}$. On the other hand, the following lemma holds.

Lemma 7.3.25. *Let $\boldsymbol{w} \in \left(A_b^d\right)^*$. The $(\nu,\mathcal{V}_\iota')^m$-top $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ belongs to $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.*

Proof. Since $T_{\zeta,\beta,\nu}$ belongs to $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and by Lemma 7.3.19, $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is invariant under the right action $\cdot$ of $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ over $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, then $T_{\zeta,\beta,\nu} \cdot \boldsymbol{w} \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. Hence $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ belongs to $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ for all $\boldsymbol{w} \in \left(A_b^d\right)^*$. □

Example 7.3.13 is now resumed.

Example 7.3.26. Let $\boldsymbol{w} = (000, 200, 010, 110, 000, 000, 222)$, then $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ is equal to T_3 of Table 7.7.

Finally, the functions $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}$ admit the following result:

Lemma 7.3.27. *Let $\boldsymbol{w} \in \left(A_b^d\right)^*$, $\boldsymbol{v} \in \left(A_b^d\right)^*$. Then $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \cdot \mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v}) = \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}\boldsymbol{v})$.*

Proof. Let $\boldsymbol{w} \in \left(A_b^d\right)^*$, $\boldsymbol{v} \in \left(A_b^d\right)^*$. Then:

$$\begin{aligned}
\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \cdot \mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v}) &= T_{\zeta,\beta,\nu} \cdot \mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \cdot \mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{v}) \\
&= T_{\zeta,\beta,\nu} \cdot \mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w} \cdot \boldsymbol{v}) \\
&= \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}\boldsymbol{v}).
\end{aligned}$$

□

Finally, it is proven that an antecedent by $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is computable in time $O\left(d^2 + \omega_{b,m}\right)$.

Lemma 7.3.28. *Let $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. There exists a word $\boldsymbol{w} \in \left(A_b^d\right)^*$ of length at most $\lceil \log(d(m+1)) \rceil + \omega_{b,m} - 1$, computable in time $O\left(d^2 + \omega_{b,m}\right)$ such that $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T$.*

Proof. Let $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. Let $\boldsymbol{w}$ be the word obtained by the Algorithm 2 of Lemma 7.3.10. The word $\boldsymbol{w}$ is such that $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}\boldsymbol{w} = T$ and its length is at most $\lceil \log(d(m+1)) \rceil + \omega_{b,m} - 1$. □

As for $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}$, the inverse of the function $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is now introduced.

Notation 7.3.29 ($\underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta}$, $\overline{T}^{\mathbb{Z}}$)**.** For $T \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, let $\underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta}$ denote

$$\left\{\boldsymbol{w} \in \left(A_b^d\right)^* \mid \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T\right\},$$

and let $\overline{T}^{\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}}$ denote

$$\overline{\left(\underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta}\right)}^{\mathbb{N}}.$$

By Lemma 7.3.28, for $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, the set $\underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta}$ is not empty.

A $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-formula which defines $\overline{T}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$ is now introduced.

Notation 7.3.30 ($\phi_T(\boldsymbol{x})$)**.** Let $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, let $\phi_T(\boldsymbol{x})$ be the conjunction of

- $x_i \doteq 0$ if $i \in \mathbb{O}_T$,
- $x_i \neq 0$ if $i \in \zeta$, and $i \notin \mathbb{O}_T$,
- $x_i \doteq x_j$ if $i \mathbb{E}_T j$,
- $x_i \neq x_j$ if $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$, $(i \in \beta) \Longleftrightarrow (j \in \beta)$ and $i \mathbb{E}_T j$ does not hold,
- $x_i + 1 \doteq x_j$ if $i \mathbb{S}_T j$,
- $x_i + 1 \neq x_j$ if $i \in \beta$, $j \in \zeta$ and $i \mathbb{S}_T j$ does not hold,
- $x_i < x_j$ if $i \mathbb{L}_T j$ and
- $x_i \equiv c \mod m$ if $\text{MODULO}_m[T]_i = c$.

It should be noted that there are no restriction of the form $w_i \in (b-1)^*$ or $|\boldsymbol{w}| = c \mod \omega_{b,m}$. The following lemma is straightforward from the definition.

Lemma 7.3.31. *The formula $\phi_T(\boldsymbol{x})$ defines the set of $\boldsymbol{x} \in \mathbb{N}^d$ which admits an expansion $\boldsymbol{w}$ such that $\text{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T$.*

7.3.2 $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$

The relation between the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops and an automaton accepting a $\Sigma_0[\mathcal{V}_\iota'(m)]$-definable set are introduced in this section.

7.3.2.1 Interpretation

It is now proven that, for any $\boldsymbol{w} \in \left(A_b^d\right)^*$, the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top $\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ contains enough information to determine whether $\boldsymbol{w}$ is accepted by the automaton $\mathcal{A}'_{\phi,\nu}$. More precisely, the exact information needed is the one contained in a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top T, with the exception of $\text{LENGTH}_{m,b}[T]$. Indeed, the length of a word does not change the tuple of integer it represents. Adding leading $\mathbf{0}$'s to an A_b^d-word changes the length but not the integer value. Hence the next definition is now introduced.

Lemma 7.3.32. *Let $R \subseteq \mathbb{N}^d$, let ζ and β be two disjoint subsets of $[d-1]$, let $m \in \mathbb{C}_b$, an integer coprime to b. The following assertions are equivalent:*

1. *The set R is $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-definable.*
2. *For all $\boldsymbol{w},\boldsymbol{w'} \in \left(A_b^d\right)^*$, if $\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})$ then $\left(\overline{\boldsymbol{w}}^{\mathbb{N}} \in R\right) \Longleftrightarrow \left(\overline{\boldsymbol{w'}}^{\mathbb{N}} \in R\right)$.*
3. *For all $\boldsymbol{w},\boldsymbol{w'} \in \left(A_b^d\right)^+$ ending by $\mathbf{0}$, if $\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})$ then $\left(\overline{\boldsymbol{w}}^{\mathbb{N}} \in R\right) \Longleftrightarrow \left(\overline{\boldsymbol{w'}}^{\mathbb{N}} \in R\right)$.*

Proof. The proof is done by three implications. The implication $2 \Longrightarrow 3$ is trivial, let us prove the other implications.

$1 \Longrightarrow 2$ Let $\boldsymbol{w}, \boldsymbol{w'} \in \left(A_b^d\right)^*$ such that $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})$. The proof is by induction on the $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-formula ϕ which defines R. The induction cases are trivial, one base case is proven, the other cases are similar. Let us assume that ϕ is the formula $x_i \doteq x_j$. Since $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$ and since $x_i \doteq x_j$, $(i \in \zeta) \Longleftrightarrow (j \in \zeta)$, $(i \in \beta) \Longleftrightarrow (j \in \beta)$, and $(i \in \nu) \Longleftrightarrow (j \in \nu)$. Hence

$$\begin{array}{lll}
\phi(\boldsymbol{w}) & \Longleftrightarrow & w_i = w_j \\
& \Longleftrightarrow & i \ \mathbb{E}_{\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})} \ j \qquad \left(\text{using the definition of } \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}\right) \\
& \Longleftrightarrow & i \ \mathbb{E}_{\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})} \ j \qquad \left(\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})\right) \\
& \Longleftrightarrow & w_i' = w_j' \qquad \left(\text{using the definition of } \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}\right) \\
& \Longleftrightarrow & \phi(\boldsymbol{w'}).
\end{array}$$

$3 \Longrightarrow 1$ Let $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ without $\mathbb{B}$-classes, let $N_T = \left\{\overline{\boldsymbol{w}}^{\mathbb{N}} \mid \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T\right\}$ be the set of d-tuple of numbers which have a representation whose $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top is T. Then N_T is $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-definable by the formula $\phi_T(\boldsymbol{x})$ introduced in Notation 7.3.30.

Let S be the set of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops T with $\mathbb{B}_T = \emptyset$ such that there exists $\boldsymbol{w} \in \left(A_b^d\right)^+$ whose last letter is $\mathbf{0}$, such that $\overline{\boldsymbol{w}}^{\mathbb{N}} \in R$ and $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \in T$. Then $\overline{w}^{\mathbb{N}} \in R$ is equivalent to $\boldsymbol{w} \in T \in S$. Then, $R = \bigcup_{T \in S} N_T$, hence R is defined by the finite disjunction of the formulas $\phi_T(\boldsymbol{x})$ for $T \in S$. □

This lemma admits this straightforward corollary.

Corollary 7.3.33. *A set $R \subseteq \mathbb{N}^d$ is $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-definable if and only if if it an union of sets $\overline{T}^{\mathbb{Z}}$.*

Given a word $\boldsymbol{w} \in \left(A_b^d\right)^*$, the image of $\boldsymbol{w}$ by $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ contains enough information to decide whether $\overline{\boldsymbol{w}}^{\mathbb{N}}$ belongs to a set defined by a formula. It leads to the following definition.

Definition 7.3.34 (Interpretation)**.** Let $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\nu$. Let $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$. Let $\phi(T)$ denote that $\phi(\overline{\boldsymbol{w}}^{\mathbb{N}})$ holds for some $\boldsymbol{w} \in \left(A_b^d\right)^*$ such that $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T$.

The truth value of $\phi(T)$ is defined by induction on ϕ. The induction cases are standard.

- If ϕ is $x_i \equiv c \mod m$ then $\phi(T)$ holds if and only if $\textsc{modulo}_m[T]_i = c$.
- If ϕ is $x_i \doteq 0$, then $\phi(T)$ holds if and only if $i \in \mathbb{O}_T$.
- If ϕ is $x_i \doteq x_j$, then $\phi(T)$ holds if and only if $i \ \mathbb{E}_T \ j$.
- If ϕ is $x_i + 1 \doteq x_j$, then $\phi(T)$ holds if and only if $i \ \mathbb{S}_T \ j$.
- Finally if ϕ is $x_i < x_j$, then $\phi(T)$ holds if and only if $i \ \mathbb{L}_T \ j$.

The notation for the set of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops satisfying a formula is now introduced.

Notation 7.3.35. Let $\overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$ (respectively, $\overline{\phi}^{\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}}$) denote the set of $(\nu,\mathcal{V}_\iota')^m$-tops (respectively $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops) T such that $\phi(T)$. Formally:

$$\begin{array}{lll}
\overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}} = & \left\{T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'} \mid \phi(T)\right\} \\
\overline{\phi}^{\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}} = & \left\{T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \mid \phi(T)\right\}.
\end{array}$$

7.3.2.2 Quotients and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$

Acceptation or rejection of words where considered in Section 7.3.2.1. Quotients by a word and $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops are considered in this section.

The following lemma states that $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ contains exactly the information needed to study $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-definable sets.

Lemma 7.3.36. *Let $R \subseteq \mathbb{N}^d$, let ζ and β be two disjoint subsets of $[d-1]$, the two assertions are equivalent:*

1. *The set R is $\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$-definable.*
2. *Let $\boldsymbol{w},\boldsymbol{w'} \in \left(A_b^d\right)^*$ such that $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})$ then $\boldsymbol{w}^{-1}R = \boldsymbol{w'}^{-1}R$.*

Proof. Both side of the implications are based on the lemma 7.3.32.

$1\Longrightarrow 2$ Let us assume that Property 1 holds. It is the same than Property 1 of Lemma 7.3.32. Hence, Property 2 of Lemma 7.3.32 holds.

Let $\boldsymbol{w},\boldsymbol{w'} \in \left(A_b^d\right)^*$ with $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})$, let us prove that $\boldsymbol{w}^{-1}R = \boldsymbol{w'}^{-1}R$, that is, for all $\boldsymbol{v} \in \left(A_b^d\right)^*$, $\boldsymbol{v} \in \boldsymbol{w}^{-1}R$ if and only if $\boldsymbol{v} \in \boldsymbol{w'}^{-1}R$. It is proved by the following equivalences:

$$\begin{aligned}
\overline{\boldsymbol{v}}^{\mathbb{N}} \in \boldsymbol{w}^{-1}R &\Longleftrightarrow \overline{\boldsymbol{w}\boldsymbol{v}}^{\mathbb{N}} \in R && \left(\text{using the definition of } {}^{-1}\right)\\
&\Longleftrightarrow \overline{\boldsymbol{w}\boldsymbol{v}\boldsymbol{0}}^{\mathbb{N}} \in R && \left(\text{Since } \overline{\boldsymbol{w}\boldsymbol{v}}^{\mathbb{N}} = \overline{\boldsymbol{w}\boldsymbol{v}\boldsymbol{0}}^{\mathbb{N}}\right)\\
&\Longleftrightarrow \overline{\boldsymbol{w'}\boldsymbol{v}\boldsymbol{0}}^{\mathbb{N}} \in R && \text{(using Lemma 7.3.32, Property 2)}\\
&\Longleftrightarrow \overline{\boldsymbol{w'}\boldsymbol{v}}^{\mathbb{N}} \in R && \left(\text{Since } \overline{\boldsymbol{w'}\boldsymbol{v}}^{\mathbb{N}} = \overline{\boldsymbol{w'}\boldsymbol{v}\boldsymbol{0}}^{\mathbb{N}}\right)\\
&\Longleftrightarrow \overline{\boldsymbol{v}}^{\mathbb{N}} \in \boldsymbol{w'}^{-1}R && \left(\text{using the definition of } {}^{-1}\right).
\end{aligned}$$

$2\Longrightarrow 1$ Let us assume that Property 2 holds. By Lemma 7.3.32, it suffices to prove that the equality $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w'})$ implies $\overline{\boldsymbol{w}}^{\mathbb{N}} \in R \Longleftrightarrow \overline{\boldsymbol{w'}}^{\mathbb{N}} \in R$ for all $\boldsymbol{w},\boldsymbol{w'} \in \left(A_b^d\right)^*$. This is a straightforward corollary of Property 2. □

Thanks to the preceding lemma, the notion of *left-quotient by a $(\nu,\mathcal{V}_\iota')^m$-top* is introduced.

Definition 7.3.37 (Left quotient)**.** Let $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$, and $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$. Let $T^{-1}\phi$ be a $\Sigma_0[\mathcal{V}_\iota'(m)]/\mathbb{O}_T,\mathbb{B}_T,\nu$-formula defined by induction on ϕ as follows:

ϕ	if	then $T^{-1}\phi$ is	otherwise $T^{-1}\phi$ is
$x_i \doteq 0$	$i \in \mathbb{O}_T$	$x_i \doteq 0$	false
$x_i \doteq x_j$	$i\ \mathbb{E}_T\ j$	$x_i \doteq x_j$	false
$x_i + 1 \doteq x_j$	$i\ \mathbb{S}_T\ j$	$x_i \doteq x_j$	if $i \in \mathbb{B}_T, j \in \mathbb{O}_T$ then $x_i + 1 \doteq x_j$ otherwise false
$x_i > x_j$	$i\ \mathbb{G}_T\ j$	$x_i \geq x_j$	$x_i > x_j$
$x_i \equiv c \mod m$		$x_i \equiv (c - \textsc{modulo}_m[T]_i)\left(\left(b^{\textsc{length}_{m,b}[T]}\right)^{-1}\right) \bmod m$	

The following lemma implies that this definition behaves as expected.

Lemma 7.3.38. *Let $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and let $U \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$. Then $T^{-1}\phi(U)$ if and only if $\phi(T \cdot U)$.*

The lemma implies in particular that $(\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})^{-1}\phi)(\boldsymbol{v})$ if and only if $\phi(\overline{\boldsymbol{w}\boldsymbol{v}}^{\mathbb{N}})$.

Proof. The proof is by induction on ϕ. The induction cases are trivial, and the base cases are a straightforward study of the rules of the $(\nu,\mathcal{V}_\iota')^m$-tops' product. □

7.3.3 Automata

In this section, an automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$, which accepts the formula $\phi \in \Sigma_0[\mathcal{V}'_\iota(m)]/\zeta,\beta,\nu$, is defined using the notions introduced in the previous section. This automaton is not a part of the proof, it is used to give examples and show how $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-top are used.

Definition 7.3.39 ($\mathcal{A}'_{\phi,\zeta,\beta,\nu}$)**.** Let the automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ be

$$\left(\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}, A_b^d, \cdot, T_{\zeta,\beta,\nu}, \overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}}\right).$$

- Here $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ is the set of $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-tops as in Definition 7.3.17,
- the transition function $\cdot$ is the right action introduced in Definition 7.3.16,
- the initial state $T_{\zeta,\beta,\nu}$ is the $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-top as in Definition 7.3.21 and
- the set of accepting states $\overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}}$ is the subset of $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ introduced in Notation 7.3.35.

The set of states and the transition function of this automaton depend of the vocabulary $\mathcal{V}'_\iota(m)$, the sets ζ, β and ν, but not of the formula ϕ itself. The only part of the quintuple which depends of ϕ is the set of accepting states. When the dimension $d = 1$, this automaton is called $\mathcal{B}^M_{m,1}$ in [MS13]. We now prove that $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ accepts $\overline{\phi}^{\mathbb{N}}$.

Lemma 7.3.40. *Let $\phi \in \Sigma_0[\mathcal{V}'_\iota(m)]/\zeta,\beta,\nu$. The automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ accepts $\overline{\phi}^{\mathbb{N}}$.*

Proof. Let $\boldsymbol{n} \in \mathbb{N}^d$.

$$\begin{aligned}
\boldsymbol{n} \in \overline{\mathcal{A}'_{\phi,\zeta,\beta,\nu}}^{\mathbb{N}} &\iff T_{\zeta,\beta,\nu} \cdot \underline{\boldsymbol{n}}_{\mathbb{N}} \in \overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}} \\
&\iff \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}\left(\underline{\boldsymbol{n}}_{\mathbb{N}}\right) \in \overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}'_\iota}} \qquad \text{(using Lemma 7.3.27)} \\
&\iff \boldsymbol{n} \in \overline{\phi}^{\mathbb{N}} \qquad \text{(using Lemma 7.3.32).}
\end{aligned}$$

□

7.3.3.1 Examples

Some examples of automata $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ are given in this section. Consider the basis $b = 2$. Consider the dimension d equal to the number of variables of the formula. Consider $m = 1$, apart in the last example where $m = 3$. It is assumed in the examples that $\nu = \emptyset$.

When the dimension $d = 2$, there are six distinct parameters which characterize a $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-top. For the sake of readability, the labels of the states only contains the parameters that differ between the different $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-top.

The caption below each automaton contains the following information:

- the formula ϕ defining the set accepted by the automaton,
- the vocabulary $\mathcal{V}$,
- the values of ζ and β and
- *Label* = (What is written in the circle of the state in the figure.).

The case of dimension $d = 1$. The automaton of Figure 7.6a is completely explained, the other automata used in the examples of this part are similar. The Figure 7.6a represents the automata $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ for the formula ϕ equal to True, when $\zeta = \{0\}$, $\beta = \emptyset$. Furthermore, $m = 1$ and then $\omega_{b,m} = 1$. The vocabulary contains the equality to 0, equality between variables and the successor relation. Hence $I^1_{\mathcal{V}'_\iota} = \{\mathbb{O}, \mathbb{B}\}$. Then, there are two $(\zeta, \beta, \nu, \mathcal{V}'_\iota)^m$-tops, which are represented in Table 7.8. The four values correspond

$\left(0, \boxed{0}, \boxed{\mathbb{O}}, \boxed{\mathbb{E}}\right)$	$\left(0, \boxed{0}, \boxed{\ }, \boxed{\mathbb{E}}\right)$
(a) T_4	(b) T_5

Table 7.8: The two $(\zeta, \beta, \nu, \mathcal{V}'_\iota)^m$-top for $d = m = 1$ and $b = 2$.

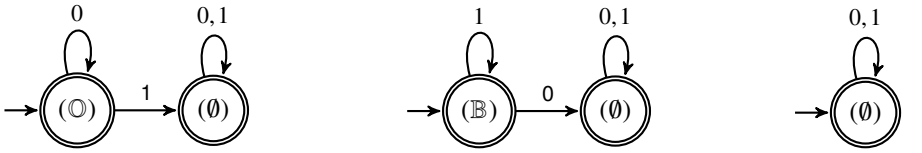
to:

- the value MODULO_m of the word modulo $m = 1$, that is, 0,
- the value $\text{LENGTH}_{m,b}$ of the length of the word modulo $\omega_{b,m} = 1$, that is 0,
- the relation $\text{POSITION}_{\mathcal{V}'_\iota(m)}$ stating that the word "belongs to 0^*" or "belongs to $(b-1)^*$",
- and finally the relation $\text{RELATION}_{\nu,\mathcal{V}'_\iota(m)}$ which compares the first component of the word with itself, that is the equality.

Clearly, since $d = 1$ and $m = 1$, the only important value of such a $(\zeta, \beta, \nu, \mathcal{V}'_\iota)^m$-top T is $\text{POSITION}_{\mathcal{V}'_\iota(m)}[T](0)$, hence, the label of the states of the automaton is

$$\left(\text{POSITION}_{\mathcal{V}'_\iota(m)}[T](0)\right).$$

The Figure 7.6b and 7.6c represent $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ for the other possible values for ζ and β. Note that the automaton of Figure 7.6a is not minimal, as the states contains an information about whether the read number is 0 or is positive.



(a) $\zeta = \{0\}$, $\beta = \emptyset$. (b) $\zeta = \emptyset$, $\beta = \{0\}$. (c) $\zeta = \emptyset$, $\beta = \emptyset$.

Figure 7.6: Let ϕ be *true*, $\mathcal{V} = \{\doteq 0, \doteq, +1, \text{mod}\,\mathbb{C}_b\}$, $Label = \left(\text{POSITION}_{\mathcal{V}'_\iota(m)}[T](0)\right)$.

It should be noted that the statement "$w \in 1^*$" is different from the statement "$\overline{w}^{\mathbb{N}}$ is of the form $2^c - 1$ for some c". Indeed, in the automaton of Figure 7.6a, one has $\delta(q_0, 1) \neq \delta(q_0, 10)$ but $\overline{10}^{\mathbb{N}} = 1 = 2^1 - 1$. Finally, for $\zeta = \emptyset$ and $\beta = \emptyset$, the automaton of Figure 7.6c is minimal.

Let ϕ be the formula $x_0 \doteq 0$, let $\zeta = \{0\}$ and $\beta = \emptyset$, then $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ is the automaton of Figure 7.7. It should be noted that its set of states is the same as in Figure 7.6a. Indeed, the base b, the dimension d, ζ, β and the modulus m are the same.

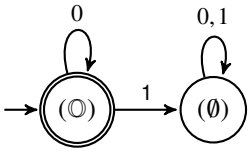


Figure 7.7: Let ϕ be $x_0 \doteq 0$, $\mathcal{V} = \{\doteq 0, \doteq, +1, \mathrm{mod}\,\mathbb{C}_b\}$, $\zeta = \{0\}$, $\beta = \emptyset$, $Label = \Big(\textsc{position}_{\mathcal{V}'_\iota(m)}[T](0)\Big)$.

Equality and Order. Let ϕ be the formula $x_0 \doteq x_1$ and $\zeta = \beta = \emptyset$, then the automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ is given in Figure 7.8. This automaton is not minimal, because, intuitively, the two states $(\mathbb{L})$ and $(\mathbb{G})$ contain some information about which of the two words is the greatest. But this information is not relevant in this context. It is explained when and how to ignore this order relation in the following chapter.

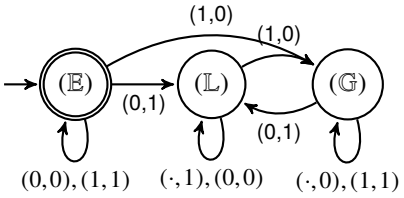
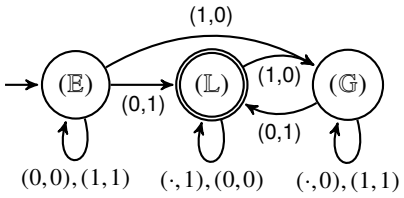
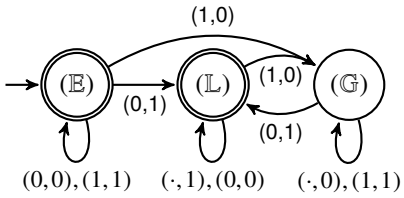


Figure 7.8: Let ϕ be $x_0 \doteq x_1$, $\mathcal{V} = \{\doteq 0, \doteq, <, +1, \mathrm{mod}\,\mathbb{C}_b\}$, $\zeta = \beta = \emptyset$, $Label = \textsc{relation}_{\nu,\mathcal{V}'_\iota(m)}[T](0,1)$.

Let ϕ be the formula $x_0 < x_1$ (respectively, $x_0 \leq x_1$), and $\zeta = \beta = \emptyset$. Then the automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ is given in Figure 7.9a (respectively, Figure 7.9b). Again, the set of states and the transition function of those three automata are the same.



(a) Let ϕ be $x_0 < x_1$.



(b) Let ϕ be $x_0 \leq x_1$.

Figure 7.9: $\mathcal{V} = \{\doteq 0, \doteq, +1, <, \mathrm{mod}\,\mathbb{C}_b\}$, $\zeta = \beta = \emptyset$, $Label = \Big(\textsc{relation}_{\nu,\mathcal{V}'_\iota(m)}[T](0,1)\Big)$.

The case +1. Let ϕ be the formula $x_0 + 1 \doteq x_1$, $\zeta = \{1\}$ and $\beta = \{0\}$, then the automaton $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ is given in Figure 7.10.

As in the automaton of Figure 7.8, the states $(\emptyset, \emptyset, \mathbb{L})$ and $(\emptyset, \emptyset, \mathbb{G})$ contain information about the order of values of the words. And as in the automaton of Figure 7.6a, the state $(\emptyset, \mathbb{O}, \mathbb{G})$ contains information about whether the second word belongs to 0^* or not. And the state $(\mathbb{B}, \emptyset, \mathbb{G})$ is similar for the first word being 1^*.

The modular case Let the modulus be $m = 3$, for a vocabulary with only the mod 3 predicate. Consider the basis b be 5. Then the order of 2 modulo m is $\omega_{b,m} = 2$. Let ϕ be the formula $x_0 \equiv 0 \mod 3$, let $\zeta = \beta = \emptyset$, and let the vocabulary be $\mathcal{V} = \{\mathrm{mod}\}$, then $\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ is the automaton of Figure 7.11. For the sake of the readability, the transitions by the letter 2 are omitted.

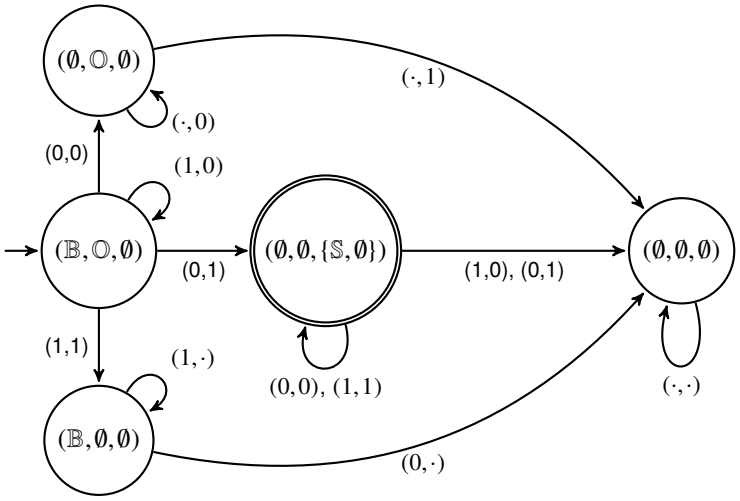


Figure 7.10: Let ϕ be $x_0 + 1 \doteq x_1$, $\mathcal{V} = \{\doteq 0, \doteq, +1, \mathrm{mod}\,\mathbb{C}_b\}$, $\zeta = \{1\}$, $\beta = \{0\}$, $Label = \left(\textsc{position}_{\mathcal{V}_\iota'(m)}[T](0), \textsc{position}_{\mathcal{V}_\iota'(m)}[T](1), \textsc{relation}_{\nu,\mathcal{V}_\iota'(m)}[T](0,1)\right)$.

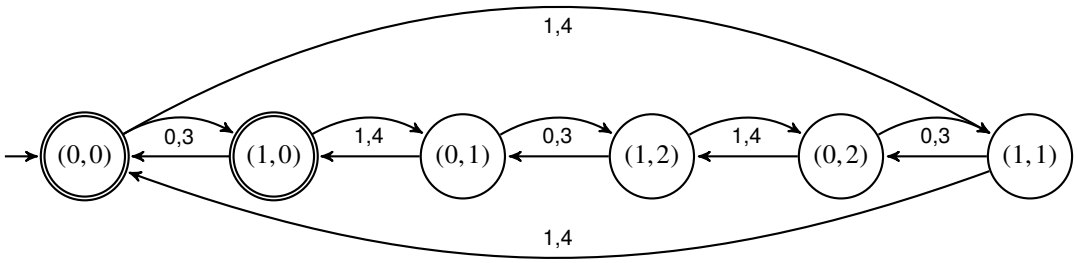


Figure 7.11: $x_0 \equiv 0 \mod 3$, $\mathcal{V} = \{\doteq 0, \doteq, +1, \mathrm{mod}\,\mathbb{C}_b\}$, $\zeta = \emptyset$, $\beta = \emptyset$, $Label = \left(\textsc{length}_{m,b}[T], \mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(0)\right)$.

Its states represent $\left(\textsc{length}_{m,b}[T], \mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(0)\right)$. Then for all $w \in \left(A_b^d\right)^*$, $\delta((0,0),w) = (t',t)$ if and only if $|w| \equiv t' \mod 2$ and $\overline{w}^{\mathbb{N}} \equiv t \mod 3$. It is what [MS13] calls the Pascal automaton $\mathcal{P}_3^0$.

The automata $\mathcal{A}'_{\phi,\nu}$ for ϕ being $x_0 \equiv 0 \mod 2$ for $b = 2$, or for ϕ being $x_0 \doteq 1$ or $x_0 + 2 \doteq x_1$ can not be represented using the characterization of this section, as those predicates do not belongs to $\mathcal{V}_\iota'(m)$. Those cases are treated in Section 7.2.

Chapter 8

The Minimal Automaton $\mathcal{A}_{\phi,\mathbb{N}}$

In this chapter, as in Section 7.3, let $\zeta, \beta \subseteq [d-1]$ such that $\zeta \cap \beta = \emptyset$ be fixed, let $m \geq 1$ such that m is coprime to b be fixed and let $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta, \beta, \nu$ be fixed.

The minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$ accepting $\overline{\phi}^{\mathbb{N}}$ is constructed in this section.

The definitions used in this section are introduced in Section 8.1. The syntactical equivalence is studied in Section 8.2. Finally, the minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$, which accepts $\overline{\phi}^{\mathbb{N}}$, is given is section 8.3.

8.1 Definitions

The definitions used in this section to construct the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ are introduced in this section.

8.1.1 Partially-Ordered Partition

The notion of $(\nu, \mathcal{V}_\iota')^m$-top was introduced in Section 7.3.1. In this section, this notion is extended to the notion of partially ordered $(\nu, \mathcal{V}_\iota'(m))$-partition over $[d-1]$. The set $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ of partially ordered $(\nu, \mathcal{V}_\iota'(m))$-partition over $[d-1]$ is now introduced.

Definition 8.1.1 ($\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$, $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$)**.** Let $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ be the set of $P \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ which satisfies the 20 first axioms of Section 7.3.1.2. Let $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'} = \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'} \cap \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

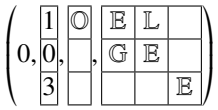
An element of $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ is called a *partially ordered* $(\nu, \mathcal{V}_\iota'(m))$*-partition over* $[d-1]$, abbreviated as $(\nu, \mathcal{V}_\iota')^m$*-pop*. Similarly, an element of $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is called a $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$*-pop*.

Note that $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'} \subseteq \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ and that, for each $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, P satisfies the properties of Definition 7.3.17.

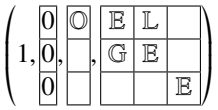
Intuitively, the main difference between a $(\nu, \mathcal{V}_\iota')^m$-top T and a $(\nu, \mathcal{V}_\iota')^m$-pop P is that, for all $i, j \in [d-1]$ with $(i \in \nu) \Longleftrightarrow (j \in \nu)$, by Axiom (21 - $\mathbb{L}$ total order), either $i\ \mathbb{E}_T\ j$, or $i\ \mathbb{L}_T\ j$, or $i\ \mathbb{G}_T\ j$, while it is not required that $i\ \mathbb{E}_P\ j$, or $i\ \mathbb{L}_P\ j$, or $i\ \mathbb{G}_P\ j$ hold. Equivalently, $i\ \overline{\mathbb{L}}\,\overline{\mathbb{E}}\,\overline{\mathbb{G}}_T\ j$ implies that $i \in \nu \Longleftrightarrow j \notin \nu$ while $i\ \overline{\mathbb{L}}\,\overline{\mathbb{E}}\,\overline{\mathbb{G}}_T\ j$ does not imply it.

If $\mathbb{L}$ does not belong to $I^2_{\mathcal{V}_\iota'}$, that is, if $<$ does not belong to the vocabulary $\mathcal{V}_\iota'$, then the set of $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-tops is equal to the set of $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-pops. Some examples of $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-pops are now given.

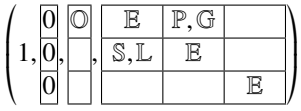
Example 8.1.2. Consider ν be $\emptyset$, the base $b = 4$, the modulus $m = 5$ and the vocabulary $\mathcal{V}_1' = \{\doteq 0, \doteq, <, +1, \mathrm{mod}\}$. Tables 8.1a, 8.1b, 8.1c, and 8.1d represent some $(\nu, \mathcal{V}_\iota')^m$-pop P_0, P_1, P_2 and P_3. They are not $(\nu, \mathcal{V}_\iota')^m$-tops since $1\ \overline{\mathbb{L}}\,\overline{\mathbb{E}}\,\overline{\mathbb{G}}_{P_i}\ 2$ and $(1 \in \nu) \Longleftrightarrow (2 \in \nu)$, for $1 \leq i \leq 3$.



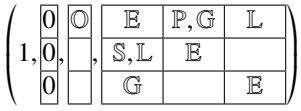
(a) P_0



(b) P_1



(c) P_2



(d) P_3

Table 8.1: Illustration of Example 8.1.2

Note that the product $\cdot$ is defined on $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, hence it is defined on $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$. It leads to the following lemmas whose proof is straightforward from the definition:

Lemma 8.1.3. *The pairs* $(\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'},\cdot)$ *and* $(\mathbb{POP}_{\nu,\mathcal{V}_\iota'},\cdot)$ *are semigroups.*

Lemma 8.1.4. *The set* $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ *is invariant under the right action* $\cdot$ *of* $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$. *Similarly, the set* $\mathbb{POP}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ *is invariant under the right action* $\cdot$ *of* $\mathbb{POP}_{\nu,\mathcal{V}_\iota'}$.

8.1.2 Relations over $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$

In this section, some relations over $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ are introduced. More precisely, some equivalence relations, some preorder relations and some order relations are introduced.

Let us first introduce a notation which associates to an element of $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ its modular part. Intuitively, $\mathbb{M}_\beta(P)$ represents the $(d+1)$-tuple

$$(\textsc{length}_{m,b}[P], \textsc{modulo}_m P).$$

Note that the length of P is considered to belong to the modular part. Intuitively, it is because the length is also defined modulo some integer.

The proofs of the part are easier if $i\ \mathbb{S}_P\ j$ implies $\mathbb{M}_\beta(P,i) = \mathbb{M}_\beta(P,i)$, which leads to the following definition.

***Definition 8.1.5** ($\mathbb{M}_\beta(P)$)**.** Let $P \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$. $(\textsc{modulo}_m P, \textsc{length}_{m,b}[P]) \in \mathbb{N}^{d+1}$ is defined as follows:

- For $i \in [d-1]$, $\mathbb{M}_\beta(P,i)$ equals:
  - $\textsc{modulo}_m[P]_i + 1$ if $i \in \beta$ and
  - $\textsc{modulo}_m[P]_i$ otherwise,
- and $\mathbb{M}_\beta(P,d) = \textsc{length}_{m,b}[P]$,

Let $\mathbb{M}_\beta(P,i)$ denote the $(i+1)$-th element of P. Since, for all $i,j \in [d-1]$, $i\ \mathbb{E}\mathbb{S}_P\ j$ implies $\mathbb{M}_\beta(P,i)$

When $m = 1$, the statement "$i\ \mathbb{S}_P\ j$ implies $\mathbb{M}_\beta(P,i) = \mathbb{M}_\beta(P,i)$" does not hold. Note that if a set R is $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$-definable, it is also $\phi \in \Sigma_0[\mathcal{V}_\iota'(m(b+1))]/\cdot,\cdot,\nu$-definable, and $m(b+1)$ is also coprime to b. It can then be assumed without loss of generality that $m > 1$. The only exception to this rule is Section 8.3.1, where $m = 1$ simplifies the examples.

The equivalence and preorder relations are now introduced for $x \in \left(I^1_{\mathcal{V}_t'} \cup I^2_{\mathcal{V}_t'} \cup \{\mathbb{M}\}\right)$. Intuitively $P \overset{x}{\cong} Q$ states that P and Q admits the same relation x, and $P \overset{x}{\preccurlyeq} Q$ states that if P admits the relations x then Q admits a greater relation. The exact meaning of "greater" depends of x.

***Definition 8.1.6** ($P \overset{x}{\cong} Q$, $P \overset{x}{\preccurlyeq} Q$, $P \overset{x}{\prec} Q$)**.** Let $x \in \left(I^1_{\mathcal{V}_t'} \cup I^2_{\mathcal{V}_t'} \cup \{\mathbb{M}\}\right)$ and $P, Q \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_t'}$. The definitions of $P \overset{x}{\cong} Q$ and of $P \overset{x}{\preccurlyeq} Q$ are given in Table 8.2.

x	$P \overset{x}{\cong} Q$	$P \overset{x}{\preccurlyeq} Q$
$\mathbb{M}$	$\text{MODULO}_m[P] = \text{MODULO}_m[Q]$ and $\text{LENGTH}_{m,b}[P] = \text{LENGTH}_{m,b}[Q]$	$\mathbb{M}_\beta(P) \leq \mathbb{M}_\beta(Q)$ lexicographically
$\mathbb{O}$	$\mathbb{O}_P = \mathbb{O}_Q$	$\mathbb{O}_P \subseteq \mathbb{O}_Q$
$\mathbb{B}$	$\mathbb{B}_P = \mathbb{B}_Q$	$\mathbb{B}_P \subseteq \mathbb{B}_Q$
$\mathbb{E}$	$\mathbb{E}_P = \mathbb{E}_Q$	$\mathbb{E}_P \subseteq \mathbb{E}_Q$
$\mathbb{S}$	$\mathbb{S}_P = \mathbb{S}_Q$	$\mathbb{S}_P \subseteq \mathbb{S}_Q$
$\mathbb{L}$	$\mathbb{L}_P = \mathbb{L}_Q$	for all $i, j \in [d-1]$, $i\ \mathbb{L}\overline{\mathbb{S}}_P\ j$ implies $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_Q\ j$

Table 8.2: Relations over $\mathbb{POP}^m_{\nu,\mathcal{V}_t'}$.

Note that the case $x = \mathbb{L}$, is different from the other cases in the sens that it is considered that $\mathbb{E}\wr\mathbb{S}$ is greater than $\mathbb{L}$. The relations $\mathbb{P}$ and $\mathbb{G}$ are not considered, because, by Axioms (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$) and (8 - $\mathbb{L}$ asymmetric), those relations are the symmetric of the relation $\mathbb{S}$ and $\mathbb{L}$ respectively.

The relations $P \overset{x}{\cong} Q$ and $P \overset{x}{\preccurlyeq} Q$ are now extended to $P \overset{X}{\cong} Q$ and $P \overset{X}{\preccurlyeq} Q$ for X a set of symbols.

***Definition 8.1.7** ($P \overset{X}{\cong} Q$, $P \overset{X}{\preccurlyeq} Q$, $P \overset{X}{\prec} Q$)**.** For a set $X \subseteq \left(I^1_{\mathcal{V}_t'} \cup I^2_{\mathcal{V}_t'} \cup \{\mathbb{M}\}\right)$ and for $P, Q \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_t'}$, the relation $P \overset{X}{\cong} Q$ holds if and only if, for all $x \in X$, $P \overset{x}{\cong} Q$ holds. Similarly, the relation $P \overset{X}{\preccurlyeq} Q$ holds if and only if for all $x \in X$, $P \overset{x}{\preccurlyeq} Q$ holds. Let $P \overset{X}{\prec} Q$ denote that $P \overset{X}{\preccurlyeq} Q$ holds and that $Q \overset{X}{\preccurlyeq} P$ does not hold.

The order relations are now introduced.

Definition 8.1.8 ($P \overset{X}{\sqsubseteq} Q$, $P \overset{X}{\sqsubset} Q$)**.** Let X be a subset of $\left(I^1_{\mathcal{V}_t'} \cup I^2_{\mathcal{V}_t'} \cup \{\mathbb{M}\}\right)$ and $\overline{X}$ be $\left(I^1_{\mathcal{V}_t'} \cup I^2_{\mathcal{V}_t'} \cup \{\mathbb{M}\}\right) \setminus X$. It is said that $P \overset{X}{\sqsubseteq} Q$ holds if and only if $P \overset{X}{\preccurlyeq} Q$ holds and $P \overset{\overline{X}}{\cong} Q$. Let $P \overset{X}{\sqsubset} Q$ denote that $P \overset{X}{\sqsubseteq} Q$ and that $Q \overset{X}{\sqsubseteq} P$ does not hold.

Equivalently, $P \overset{X}{\sqsubset} Q$ holds if and only if $P \overset{X}{\sqsubseteq} Q$ and $P \neq Q$.

Note that, when the value of X is fixed, the congruence $\overset{X}{\cong}$ is noted without the curly brackets and without commas. For example, when $X = \{\mathbb{O}, \mathbb{E}, \mathbb{S}, \mathbb{B}, \mathbb{L}\}$ then $\overset{\mathbb{OESBL}}{\cong}$ is used instead of $\overset{\{\mathbb{O},\mathbb{E},\mathbb{S},\mathbb{B},\mathbb{L}\}}{\cong}$, and similarly for $\overset{\mathbb{OESBL}}{\preccurlyeq}$ and $\overset{\mathbb{OESBL}}{\sqsubseteq}$.

The notation $\sqsubseteq$ is now introduced, which denotes the intersection off all other order relations considered in this section.

***Definition 8.1.9** ($\sqsubseteq$, $\sqsubset$)**.** Let $P, Q \in \mathbb{POP}^m_{\nu,\mathcal{V}_t'}$. The relation $P \sqsubseteq Q$ holds if and only if $P \overset{X}{\preccurlyeq} Q$ for $X = \{\mathbb{M}, \mathbb{O}, \mathbb{E}, \mathbb{S}, \mathbb{B}, \mathbb{L}\}$. Let $P \sqsubset Q$ denote that $P \sqsubseteq Q$ and $P \neq Q$.

Some examples are now given.

Example 8.1.10. Let P_0, P_1, P_2 and P_3 be the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop of Example 8.1.2. Then $P_2 \overset{\mathbb{L}}{\sqsubset} P_3$, $P_1 \overset{\mathbb{OESBL}}{\sqsubset} P_3$, $P_0 \sqsubset P_1$ and $P_0 \overset{\mathbb{M}}{\prec} P_3$ hold. For $1 \leq i < j \leq 3$, $P_i \sqsubset P_j$.

The relations $\overset{X}{\sqsubseteq}$, $\overset{X}{\preccurlyeq}$ and $\overset{X}{\cong}$ used later in this part, for $X \subseteq \left(I^1_{\mathcal{V}_\iota'} \cup I^2_{\mathcal{V}_\iota'} \cup \{\mathbb{M}\}\right)$, satisfy some properties given in the following lemmas. All proofs are straightforward from the definitions.

Lemma 8.1.11. *Let $X \subseteq Y \subseteq \left(I^1_{\mathcal{V}_\iota'} \cup I^2_{\mathcal{V}_\iota'} \cup \{\mathbb{M}\}\right)$, let $P,Q \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$, then:*

- *$P \overset{Y}{\cong} Q$ implies $P \overset{X}{\cong} Q$,*
- *$P \overset{Y}{\preccurlyeq} Q$ implies $P \overset{X}{\preccurlyeq} Q$,*
- *if $\mathbb{M}$ does not belong to Y or if $\mathbb{S}$ belongs to Y then $P \overset{Y}{\cong} Q$ implies $P \overset{Y}{\preccurlyeq} Q$,*
- *$P \overset{X}{\sqsubseteq} Q$ implies $P \overset{Y}{\sqsubseteq} Q$,*
- *in particular $P \overset{X}{\sqsubseteq} Q$ implies $P \sqsubseteq Q$ and*
- *$P \sqsubseteq Q$ implies $P \overset{X}{\preccurlyeq} Q$.*

Lemma 8.1.12. *For X being $\{\mathbb{M}\}$, $\{\mathbb{O}\}$, $\{\mathbb{B}\}$, $\{\mathbb{O},\mathbb{E},\mathbb{S},\mathbb{B}\}$, $\{\mathbb{O},\mathbb{E},\mathbb{S},\mathbb{B},\mathbb{L}\}$ or the union of some of them, the relation $P \overset{X}{\cong} Q$ is a congruence on the semigroup $(\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'},\cdot)$.*

Lemma 8.1.13. *For X being $\{\mathbb{M}\}$, $\{\mathbb{O}\}$, $\{\mathbb{B}\}$, $\{\mathbb{O},\mathbb{E},\mathbb{S},\mathbb{B}\}$, $\{\mathbb{E},\mathbb{S},\mathbb{L}\}$ or the union of some of them, then the relation $P \overset{X}{\cong} Q$ holds if and only if $P \overset{X}{\preccurlyeq} Q$ and $Q \overset{X}{\preccurlyeq} P$.*

In the case $X = \{\mathbb{M},\mathbb{O},\mathbb{E},\mathbb{S},\mathbb{B},\mathbb{L}\}$, $P \overset{X}{\cong} Q$ is equivalent to $P = Q$.

Lemma 8.1.14. *For X being $\{\mathbb{E}\}$, $\{\mathbb{O}\}$, $\{\mathbb{B}\}$, $\{\mathbb{O},\mathbb{S},\mathbb{B}\}$ or the union of some of them, the triple $\left(\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'},\cdot,\overset{X}{\preccurlyeq}\right)$ is an ordered semi-group. The triple $\left(\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'},\cdot,\overset{\mathbb{L}}{\sqsubseteq}\right)$ is an ordered semi-groups.*

8.1.3 Axiom and orders

In this part, some elements $P \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ are explicitly constructed. In order to prove that an element $P \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ indeed belongs to $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ (or to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$) it is required to prove that P satisfies the axioms of Section 7.3.1.2.

The element P is often defined such that $P \overset{X}{\preccurlyeq} Q$ or $P \overset{X}{\cong} Q$ holds for some Q which is already known to belong to $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ or to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. In this section, it is shown that, for some X, if Q satisfies some axiom, then this axiom is also satisfied by P.

Lemma 8.1.15. *Let $P \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ and $Q \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$.*

- *If $P \overset{\mathbb{E}}{\cong} Q$ then P satisfies Axiom (1 - $\mathbb{E}$ equivalence).*
- *If $P \overset{\mathbb{S}}{\preccurlyeq} Q$ and $P \overset{\mathbb{E}}{\succcurlyeq} Q$ then P satisfies Axiom (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$).*
- *If $P \overset{\mathbb{E}}{\preccurlyeq} Q$ and $P \overset{\mathbb{S}}{\cong} Q$ then P satisfies Axiom (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$).*

- *If* $P \overset{\mathbb{ES}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (4 -* $\mathbb{S}$ *and* $\mathbb{E}$ *incompatible).*
- *If* $P \overset{\mathbb{S}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (5 -* $\mathbb{S}$ *not cyclic).*
- *If* $P \overset{\mathbb{OEB}}{\cong} Q$ *then* P *satisfies Axiom (6 -* $\textsc{position}_{\mathcal{V}_\iota'(m)}$ *and* $\mathbb{E}$ *compatible).*
- *If* $P \overset{\mathbb{OSB}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (7 -* $\textsc{position}_{\mathcal{V}_\iota'(m)}$ *and* $\mathbb{S}$ *compatible).*
- *If* $\mathbb{L}_P \subseteq \mathbb{L}_Q$ *then* P *satisfies Axiom (8 -* $\mathbb{L}$ *asymmetric).*
- *If* $P \overset{\mathbb{L}}{\cong} Q$ *then* P *satisfies Axiom (9 -* $\mathbb{L}$ *transitive).*
- *If* $P \overset{\mathbb{L}}{\cong} Q$ *and* $P \overset{\mathbb{E}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (10 -* $i \mathbb{E}_T\ j, i \mathbb{L}_T\ k \Longrightarrow j \mathbb{L}_T\ k$*).*
- *If* $P \overset{\mathbb{EL}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (11 -* $\mathbb{L}$ *and* $\mathbb{E}$ *incompatible).*
- *If* $\mathbb{L}_P \supseteq \mathbb{L}_Q$ *and* $P \overset{\mathbb{OB}}{\cong} Q$ *then* P *satisfies Axiom (12 -* $\textsc{position}_{\mathcal{V}_\iota'(m)}$ *and* $\mathbb{L}$ *compatible).*
- *If* $\mathbb{L}_P \supseteq \mathbb{L}_Q$ *and* $P \overset{\mathbb{S}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (13 -* $\mathbb{S}$ *implies* $\mathbb{L}$*).*
- *If* $P \overset{\mathbb{L}}{\cong} Q$ *and* $P \overset{\mathbb{S}}{\preccurlyeq} Q$ *and* $P \overset{\mathbb{E}}{\succcurlyeq} Q$ *then* P *satisfies Axiom (14 -* $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$*).*
- *If* $P \overset{\mathbb{O}}{\preccurlyeq} Q$ *and* $P \overset{\mathbb{M}}{\cong} Q$ *then* P *satisfies Axiom (15 -* $\mathbb{O}$ *and* mod*).*
- *If* $P \overset{\mathbb{E}}{\preccurlyeq} Q$ *and* $P \overset{\mathbb{M}}{\cong} Q$ *then* P *satisfies Axiom (16 -* $\mathbb{E}$ *and* mod*).*
- *If* $P \overset{\mathbb{S}}{\preccurlyeq} Q$ *and* $P \overset{\mathbb{M}}{\cong} Q$ *then* P *satisfies Axiom (17 -* $\mathbb{S}$ *and* mod*).*
- *If* $P \overset{\mathbb{B}}{\preccurlyeq} Q$ *and* $P \overset{\mathbb{M}}{\cong} Q$ *then* P *satisfies Axiom (18 -* $\mathbb{B}$ *and* mod*).*
- *If* $P \overset{\mathbb{S}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (19 - Rigid case).*
- *If* $P \overset{\mathbb{LES}}{\preccurlyeq} Q$ *then* P *satisfies Axiom (20 -* ν*).*

If $Q \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ *and* $P \overset{\mathbb{OESB}}{\preccurlyeq} Q$ *then* $P \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

The proof of each statement easily follows from the definitions and from the axioms.

8.1.4 Relation between $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$

In this section, some properties of the subset $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ of $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ are considered. The following lemma characterizes the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops which belongs to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, its proof is straightforward from the definitions.

Lemma 8.1.16. *A* $(\nu,\mathcal{V}_\iota')^m$*-pop* $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ *belongs to* $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ *if and only if* P *is* $\overset{\mathbb{L}}{\sqsubseteq}$*-maximal.*

For $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$, the notation $\underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta}$ introduced in Notation 7.3.5, associates to T the set of $\left(A_b^d\right)^*$-words $\boldsymbol{w}$ such that $\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) = T$. This notation is now extended to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

Notation 8.1.17 ($\underline{P}_{\mathcal{V}_\iota'(m)}$)**.** Let $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, let $\underline{P}_{\mathcal{V}_\iota'(m),\zeta,\beta}$ be the set of words whose $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top is $\overset{\mathbb{L}}{\sqsubseteq}$-greater than P. Formally:

$$\underline{P}_{\mathcal{V}_\iota'(m)} = \bigcup_{T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'} | P \overset{\mathbb{L}}{\sqsubseteq} T} \underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta},$$

that is, $\left\{ \boldsymbol{w} \in \left(A_b^d\right)^* \mid P \overset{\mathbb{L}}{\sqsubseteq} \text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w}) \right\}$.

The following lemma states that there always exists a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top which is $\overset{\mathbb{L}}{\sqsubseteq}$-greater than a given $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. It implies that $\underline{P}_{\mathcal{V}_\iota'(m)}$ is a non empty set as stated in Corollary 8.1.19.

Lemma 8.1.18. *Let $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, there exists $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P \overset{\mathbb{L}}{\sqsubseteq} T$.*

Proof. If $\mathbb{L}$ does not belongs to $I^2_{\mathcal{V}_\iota'}$ then $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'} = \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, hence $P \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

Otherwise, if $\mathbb{L}$ belongs to $I^2_{\mathcal{V}_\iota'}$, let T be such that:

- $T \overset{\text{MOESB}}{\cong} P$ and
- $\mathbb{L}_T$ is a linear extension of $\mathbb{L}_P$ on ν and on $[d-1] \setminus \nu$.

□

Lemmas 7.3.10 and 8.1.18 imply the following corollary.

Corollary 8.1.19. *Let $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, the set $\underline{P}_{\mathcal{V}_\iota'(m)}$ is non empty.*

8.1.5 Syntactically Equivalent States.

The relation of syntactically equivalent states is first defined on $\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and then extended on a subset of $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. This notion is then used to define the minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$.

Notation 8.1.20 ($\sim_\phi$)**.** For $T_0, T_1 \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, let $T_0 \sim_\phi T_1$ denote that $\overline{T_0^{-1}\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}} = \overline{T_1^{-1}\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$.

As explained in Notation 8.1.17, a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop is intuitively a representation of the set of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops which are $\overset{\mathbb{L}}{\sqsubseteq}$-greater than it. Hence, the set of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops P such that all $\overset{\mathbb{L}}{\sqsubseteq}$-greater $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops are syntactically equivalent is now introduced. Those are the only $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops considered in this part.

Definition 8.1.21 ($\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$)**.** Let $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \subseteq \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be the set of $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $T_1 \sim_\phi T_2$ holds for all $T_1, T_2 \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ with $P \overset{\mathbb{L}}{\sqsubseteq} T_1$ and $P \overset{\mathbb{L}}{\sqsubseteq} T_2$.

Let $P_0, P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, let $T_0, T_1 \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P_0 \overset{\mathbb{L}}{\sqsubseteq} T_0$ and $P_1 \overset{\mathbb{L}}{\sqsubseteq} T_1$, then let $P_0 \sim_\phi P_1$ denote that $T_0 \sim_\phi T_1$.

Note that $P_0 \sim_\phi P_1$ is independent of the choice of T_0 and of T_1.

The binary relation $\sim_\phi$ is clearly symmetric and transitive on $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. The notion of left-quotient by a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top is now extended to left-quotient by an element of $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

Notation 8.1.22 ($P^{-1}\phi$)**.** Let $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. Let $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ be the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top such that $P \overset{\mathbb{L}}{\sqsubseteq} T$ and such that $\mathbb{L}_T$ is lexicographically minimal. Let $P^{-1}\phi$ denote $T^{-1}\phi$ and let $\phi(P)$ denote $\phi(T)$.

Note that, for $T, T' \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ such that $P \overset{\mathbb{L}}{\sqsubseteq} T$ and $P \overset{\mathbb{L}}{\sqsubseteq} T'$, it is possible that $T^{-1}\phi \neq T'^{-1}\phi$. This is why we have fixed an arbitrary $(\nu,\mathcal{V}_\iota')^m$-top. Nonetheless, by definition of $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $\overline{T^{-1}\phi}^{\mathbb{N}} = \overline{T'^{-1}\phi}^{\mathbb{N}}$ and furthermore $\phi(T)$ is equivalent to $\phi(T')$.

The following lemma is similar to Lemma 7.3.38 and implies that the preceding definition behaves as expected.

Lemma 8.1.23. *Let $P \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $O \in \mathbb{POP}^{m,P^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. Then $(P^{-1}\phi)(O)$ holds if and only if $\phi(P\cdot O)$ holds.*

Proof. Let T as in Notation 8.1.22 and $U \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $O \overset{\mathbb{L}}{\sqsubseteq} U$. By definition of T, $P^{-1}\phi = T^{-1}\phi$. Since $O \overset{\mathbb{L}}{\sqsubseteq} U$ and $O \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, by definition of $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $(P^{-1}\phi)(O)$ is equivalent to $(P^{-1}\phi)(U)$, hence to $(T^{-1}\phi)(U)$. By Lemma 7.3.38, $(T^{-1}\phi)(U)$ is equivalent to $\phi(T\cdot U)$. By Lemma 8.1.14, $P\cdot O \overset{\mathbb{L}}{\sqsubseteq} T\cdot U$, hence $\phi(T\cdot U)$ is equivalent to $\phi(P\cdot O)$.

By transitivity of equivalences $(P^{-1}\phi)(O)$ holds if and only if $\phi(P\cdot O)$ holds. □

The preceding lemma admits the following corollaries.

Corollary 8.1.24. *Let $O \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $P \in \mathbb{POP}^{m,O^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $Q \in \mathbb{POP}^{m,P^{-1}(O^{-1}\phi)}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, then $(P^{-1}(O^{-1}\phi))(Q)$ if and only if $O^{-1}\phi(P\cdot Q)$.*

Corollary 8.1.25. *Let $O, P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $Q \in \mathbb{POP}^{m,O^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $R \in \mathbb{POP}^{m,P^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $O\cdot Q = P\cdot R$, then $O^{-1}\phi(Q)$ if and only if $P^{-1}\phi(R)$.*

Proof.

$$\begin{array}{rcll} O^{-1}\phi(Q) & \iff & \phi(O\cdot Q) & \text{(using Lemma 8.1.23)} \\ & \iff & \phi(P\cdot R) & (O\cdot Q = P\cdot R) \\ & \iff & (P^{-1}\phi)(R) & \text{(using Lemma 8.1.23).} \end{array}$$

□

The following two lemmas state that the right-action $\cdot$ of $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ on $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is compatible with $\sim_\phi$.

Lemma 8.1.26. *Let $P_0, P_1 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P_0 \sim_\phi P_1$, let $O \in \mathbb{POP}^{m,P_0^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, then $O \in \mathbb{POP}^{m,P_1^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.*

Proof. Let $U_0, U_1 \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ such that $O \overset{\mathbb{L}}{\sqsubseteq} U_0$ and $O \overset{\mathbb{L}}{\sqsubseteq} U_1$, hence $U_0 \sim_{P_0^{-1}\phi} U_1$. In order to prove that $O \in \mathbb{POP}^{m,P_1^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it suffices to prove that $U_0^{-1}(P_1^{-1}\phi) \sim_\phi U_1^{-1}(P_1^{-1}\phi)$, that is, that for all $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$,

$(U_0^{-1}(P_1^{-1}\phi))(T)$ is equivalent to $(U_1^{-1}(P_1^{-1}\phi))(T)$.

$$\begin{array}{rll}
(U_0^{-1}(P_1^{-1}\phi))(T) \iff & (P_1^{-1}\phi)(U_0 \cdot T) & \text{(using Corollary 8.1.24)} \\
\iff & (P_0^{-1}\phi)(U_0 \cdot T) & \left(P_1 \sim_\phi P_0\right) \\
\iff & (U_0^{-1}(P_0^{-1}\phi))(T) & \text{(using Corollary 8.1.24)} \\
\iff & (U_1^{-1}(P_0^{-1}\phi))(T) & \left(U_1 \sim_{P_0^{-1}\phi} U_0\right) \\
\iff & (P_0^{-1}\phi)(U_1 \cdot T) & \text{(using Corollary 8.1.24)} \\
\iff & (P_1^{-1}\phi)(U_1 \cdot T) & \left(P_1 \sim_\phi P_0\right) \\
\iff & (U_1^{-1}(P_1^{-1}\phi))(T) & \text{(using Corollary 8.1.24).}
\end{array}$$

□

Lemma 8.1.27. *Let $P_0, P_1 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P_0 \sim_\phi P_1$, let $O \in \mathbb{POP}^{m,P_0^{-1}\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, then $\overline{(P_0O)^{-1}\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}} = \overline{(P_1O)^{-1}\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$.*

Note that Lemma 8.1.26 implies that $(P_1O)^{-1}\phi$ is defined.

Proof. The lemma follows from this sequence of equivalences:

$$\begin{array}{rll}
(P_0 \cdot O)^{-1}\phi(U) \iff & P_0^{-1}\phi(O \cdot U) & \text{(using Corollary 8.1.24)} \\
\iff & P_1^{-1}\phi(O \cdot U) & \left(\text{using the definition of } P_0 \sim_\phi P_1\right) \\
\iff & (P_1 \cdot O)^{-1}\phi(\quad U) & \text{(using Corollary 8.1.24).}
\end{array}$$

□

8.2 Minimal element of each syntactical equivalence classes.

The relation between the syntactically equivalent $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops and the order relations are considered in this section. The main result of this section is now given, it states that each $\sim_\phi$-classes admits exactly one $\sqsubseteq$-minimal $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop.

Proposition 8.2.1. For every $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, there exists a unique $\sqsubset$-minimal $O \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $O \sim_\phi P$.

This proposition leads to the introduction of the set $\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ of the $\sqsubseteq$-minimal $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop. It is the set of states of the minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$ which accepts $\overline{\phi}^{\mathbb{N}}$ and which is defined in the Section 8.3.

Proposition 8.2.1 is proven in Section 8.2.3. In order to prove this proposition, some intermediates results must be proven in the following sections.

The order $\overset{\mathbb{OESB}}{\preccurlyeq}$ is considered in Section 8.2.1. More precisely, Lemma 8.2.2 implies that each pair of $\sqsubseteq$-minimal $\sim_\phi$-equivalent elements are $\overset{\mathbb{OESB}}{\cong}$-equivalent. The order $\overset{\mathbb{L}}{\preccurlyeq}$ is considered in Section 8.2.2, and, similarly, Lemma 8.2.3 implies that each pair of $\sqsubseteq$-minimal $\sim_\phi$-equivalent elements are $\overset{\mathbb{OESBL}}{\cong}$-equivalent. Finally the order $\overset{\mathbb{M}}{\preccurlyeq}$ is considered in Section 8.2.3 and Lemma 8.2.6 implies that each pair of $\sqsubseteq$-minimal $\sim_\phi$-equivalent elements are equal.

8.2.1 $\sim_\phi$ and $\overset{\mathbb{OESB}}{\preccurlyeq}$

The following lemma implies that two $\sqsubseteq$-minimal $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops belonging to $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ are $\overset{\mathbb{OESB}}{\cong}$-equivalent.

Lemma 8.2.2. *Let $P_0, P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P_0 \sim_\phi P_1$ and $P_0 \overset{\mathbb{OESB}}{\not\preccurlyeq} P_1$.*

There exists $O \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $O \sim_\phi P_0$, and $O \sqsubset P_0$.

Intuitively, the proof consists in removing from P_0 all $\mathbb{OESB}$-relations which does not appear in P_1, in order to obtain a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop O which is $\sim_\phi$-equivalent to P_0.

Lemma 8.2.2 is now proved.

Proof of Lemma 8.2.2. The proof consists of two parts, constructing O and then proving that it satisfies the conditions of the lemma.

Constructing O. Intuitively, the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop O is similar to P_0. Some relations $\mathbb{O}$, $\mathbb{E}$, $\mathbb{S}$ and $\mathbb{B}$ are removed from P_0 in order to create O. Those four relations in O are the intersections of those relations in P_0 and in P_1. Furthermore, some of the relations $i\ \mathbb{ES}_{P_0}\ j$ which are removed from P_0 are transformed into $i\ \mathbb{L}\overline{\mathbb{S}}_O\ j$ or $i\ \mathbb{GP}_O\ j$ in order to be similar to P_1.

Let $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be defined as follows:

- $\textsc{position}_{\mathcal{V}_\iota'(m)}[O](i) = \textsc{position}_{\mathcal{V}_\iota'(m)}[P_0](i) \cap \textsc{position}_{\mathcal{V}_\iota'(m)}[P_1](i)$,
- $i\ \mathbb{E}_O\ j$ if and only if $i\ \mathbb{E}_{P_0}\ j$ and $i\ \mathbb{E}_{P_1}\ j$,
- $i\ \mathbb{S}_O\ j$ if and only if $i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$,
- $i\ \mathbb{L}_O\ j$ if and only if $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$) or ($i\ \mathbb{ES}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$) and
- $O \overset{\mathbb{M}}{\cong} P_0$.

Note that $i\ \mathbb{L}\overline{\mathbb{S}}_O\ j$ if and only if $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{ES}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$). Let us claim that $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. By construction $O \sqsubseteq P_0$. Since $P_0 \neq P_1$ and since $O \sqsubseteq P_0$, $O \sqsubset P_0$. It remains to prove that $O \sim_\phi P_0$.

Proving $P_0 \sim_\phi O$. Let us prove that $O \sim_\phi P_0$, that is, let $Q_0 \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ and let us prove that, $O^{-1}\phi(Q_0)$ is equivalent to $P_0^{-1}\phi(Q_0)$.

Let us first claim that there exists $Q_1, Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ such that $P_0 \cdot Q_0 = P_0 \cdot Q_1$, $P_1 \cdot Q_1 = P_1 \cdot Q_2$ and $P_0 \cdot Q_2 = O \cdot Q_0$. Then

$$\begin{aligned}
P_0^{-1}\phi(Q_0) &\Longleftrightarrow P_0^{-1}\phi(Q_1) && \text{(using Corollary 8.1.25)}\\
&\Longleftrightarrow P_1^{-1}\phi(Q_1) && \big(P_0 \sim_\phi P_1\big)\\
&\Longleftrightarrow P_1^{-1}\phi(Q_2) && \text{(using Corollary 8.1.25)}\\
&\Longleftrightarrow P_0^{-1}\phi(Q_2) && \big(P_0 \sim_\phi P_1\big)\\
&\Longleftrightarrow O^{-1}\phi(Q_0) && \text{(using Corollary 8.1.25)}.
\end{aligned}$$

Constructing Q_1 and Q_2 Two $(\nu, \mathcal{V}_\iota')^m$-pops $Q_1, Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ are now defined, it is then proved that $P_0 \cdot Q_0 = P_0 \cdot Q_1$, $P_1 \cdot Q_1 = P_1 \cdot Q_2$ and $P_0 \cdot Q_2 = O \cdot Q_0$.

Intuitively, for c being 0 or 1, the $(\nu, \mathcal{V}_\iota')^m$-pop Q_{c+1} is similar to Q_c. The relation $\mathbb{O}$ and $\mathbb{B}$ in Q_{c+1} are the intersections of those relations in P_c and in Q_c. More generally, each relation $\mathbb{O}, \mathbb{E}, \mathbb{S}, \mathbb{B}$ occur in Q_{c+1} only if they occur in Q_c and they are mandatory to obtain the equality $P_c \cdot Q_{c+1} = P_c \cdot Q_c$.

Let us now define Q_{c+1}. For all $i, j \in [d-1]$:

- $\textsc{position}_{\mathcal{V}_\iota'(m)}[Q_{c+1}](i) = \textsc{position}_{\mathcal{V}_\iota'(m)}[Q_c](i) \cap \textsc{position}_{\mathcal{V}_\iota'(m)}[P_c](i)$,
- $i \mathbb{E}_{Q_{c+1}} j$ if and only if $i \mathbb{E}_{Q_c} j$ and $i \mathbb{E}\mathbb{S}_{P_c} j$,
- $i \mathbb{S}_{Q_{c+1}} j$ if and only if $i \mathbb{S}_{Q_c} j$ and $i \in \mathbb{B}_{P_c}$ and $j \in \mathbb{O}_{P_c}$,
- $i \mathbb{L}_{Q_{c+1}} j$ if and only if $i \mathbb{L}_{Q_c} j$ or ($i \mathbb{E}_{Q_c} j$ and $i \mathbb{L}\overline{\mathbb{S}}_{P_c} j$) and
- $Q_{c+1} \overset{\mathbb{M}}{\cong} Q_c$,

Let us claim that $Q_0, Q_1 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ and let us prove that Q_1 and Q_2 satisfy the claims.

Proving that $P_c \cdot Q_c = P_c \cdot Q_{c+1}$ The remaining of the proof consists in proving the above-mentioned equalities by a case by case study, and proving that the elements O, Q_1 and Q_2 are indeed $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-pop and $(\nu, \mathcal{V}_\iota')^m$-pop.

Let $c \in \{0,1\}$ and let us prove that $P_c \cdot Q_c = P_c \cdot Q_{c+1}$. For all $i, j \in [d-1]$:

- Let us consider $\textsc{length}_{m,b}$ and $\textsc{modulo}_m$. Since $Q_c \overset{\mathbb{M}}{\cong} Q_{c+1}$ and since $\overset{\mathbb{M}}{\cong}$ is a congruence relation, $P_c \cdot Q_c \overset{\mathbb{M}}{\cong} P_c \cdot Q_{c+1}$.
- Let us consider $\mathbb{O}$, the case $\mathbb{B}$ is similar:

$$\begin{aligned}
i \in \mathbb{O}_{P_c \cdot Q_c} &\iff i \in \mathbb{O}_{P_c} \wedge i \in \mathbb{O}_{Q_c} && \text{(using the definition of } P_c \cdot Q_c\text{)}\\
&\iff i \in \mathbb{O}_{P_c} \wedge i \in \mathbb{O}_{Q_{c+1}} && \text{(using the definition of } Q_{c+1}\text{)}\\
&\iff i \in \mathbb{O}_{P_c \cdot Q_{c+1}}. && \text{(using the definition of } P_c \cdot Q_{c+1}\text{)}
\end{aligned}$$

- Let us consider $\mathbb{E}$.

$$\begin{aligned}
i \mathbb{E}_{P_c \cdot Q_c} j &\iff i \mathbb{E}_{P_c} j \wedge i \mathbb{E}_{Q_c} j && \text{(using the definition of } P_c \cdot Q_c\text{)}\\
&\iff ((i \in \zeta) \iff (j \in \zeta)) \wedge ((i \in \beta) \iff (j \in \beta))\\
&\quad \wedge i \mathbb{E}\mathbb{S}_{P_c} j \wedge i \mathbb{E}_{Q_c} j && \text{(using Definition 7.3.17)}\\
&\iff ((i \in \zeta) \iff (j \in \zeta)) \wedge ((i \in \beta) \iff (j \in \beta))\\
&\quad \wedge i \mathbb{E}\mathbb{S}_{P_c} j \wedge i \mathbb{E}_{Q_{c+1}} j && \text{(using the definition of } Q_{c+1}\text{)}\\
&\iff i \mathbb{E}_{P_c} j \wedge i \mathbb{E}_{Q_{c+1}} j && \text{(using Definition 7.3.17)}\\
&\iff i \mathbb{E}_{P_c \cdot Q_{c+1}} j. && \text{(using the definition of } P_c \cdot Q_{c+1}\text{)}
\end{aligned}$$

- Let us consider $\mathbb{S}$:

$$\begin{aligned}
i \mathbb{S}_{P_c \cdot Q_c} j &\iff (i \mathbb{S}_{P_c} j \wedge i \mathbb{E}_{Q_c} j) \vee\\
&\qquad (j \in \mathbb{O}_{P_c} \wedge i \in \mathbb{B}_{P_c} \wedge i \mathbb{S}_{Q_c} j) && \text{(using the definition of } P_c \cdot Q_c\text{)}\\
&\iff (i \mathbb{S}_{P_c} j \wedge i \mathbb{E}_{Q_{c+1}} j) \vee\\
&\qquad (j \in \mathbb{O}_{P_c} \wedge i \in \mathbb{B}_{P_c} \wedge i \mathbb{S}_{Q_{c+1}} j) && \text{(using the definition of } Q_{c+1}\text{)}\\
&\iff i \mathbb{S}_{P_c \cdot Q_{c+1}} j. && \text{(using the definition of } P_c \cdot Q_{c+1}\text{)}
\end{aligned}$$

- Finally, let us consider $\mathbb{L}$.

  Let us first suppose that $i\ \mathbb{L}_{P_c \cdot Q_c}\ j$ and let us prove that $i\ \mathbb{L}_{P_c \cdot Q_{c+1}}\ j$. Since $i\ \mathbb{L}_{P_c \cdot Q_c}\ j$, either ($i\ \mathbb{L}_{P_c}\ j$ and $i\ \mathbb{E}_{Q_c}\ j$) or $i\ \mathbb{L}_{Q_c}\ j$. The two cases are considered separately.

  - Let us assume that $i\ \mathbb{L}_{P_c}\ j$ and $i\ \mathbb{E}_{Q_c}\ j$ hold. Since $i\ \mathbb{L}_{P_c}\ j$ and $i\ \mathbb{E}_{Q_c}\ j$ by definition of Q_{c+1}, ($i\ \mathbb{L}_{Q_{c+1}}\ j$ or $i\ \mathbb{E}_{Q_{c+1}}\ j$), hence $i\ \mathbb{L}_{P_c \cdot Q_{c+1}}\ j$ holds.
  - Finally, let us assume that $i\ \mathbb{L}_{Q_c}\ j$ holds. By definition of Q_{c+1}, $i\ \mathbb{L}_{Q_{c+1}}\ j$ holds. Since $i\ \mathbb{L}_{Q_{c+1}}\ j$ holds, $i\ \mathbb{L}_{P_c \cdot Q_{c+1}}\ j$ holds.

  Let us now suppose that $i\ \mathbb{L}_{P_c \cdot Q_{c+1}}\ j$ and let us prove that $i\ \mathbb{L}_{P_c \cdot Q_c}\ j$. Since $i\ \mathbb{L}_{P_c \cdot Q_{c+1}}\ j$, either ($i\ \mathbb{L}_{P_c}\ j$ and $i\ \mathbb{E}_{Q_{c+1}}\ j$) or $i\ \mathbb{L}_{Q_{c+1}}\ j$. The two cases are considered separately.

  - Let us first suppose that $i\ \mathbb{L}_{P_c}\ j$ and $i\ \mathbb{E}_{Q_{c+1}}\ j$. Since $i\ \mathbb{E}_{Q_{c+1}}\ j$, by definition of Q_{c+1}, $i\ \mathbb{E}_{Q_c}\ j$. Since $i\ \mathbb{L}_{P_c}\ j$ and $i\ \mathbb{E}_{Q_c}\ j$, $i\ \mathbb{L}_{P_c \cdot Q_c}\ j$.
  - Finally, let us suppose that $i\ \mathbb{L}_{Q_{c+1}}\ j$. By definition of Q_{c+1}, $i\ \mathbb{L}_{Q_c}\ j$ or ($i\ \mathbb{E}_{Q_c}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ j$). The two cases are considered separately.
    - If $i\ \mathbb{L}_{Q_c}\ j$ then $i\ \mathbb{L}_{P_c \cdot Q_c}\ j$
    - If $i\ \mathbb{E}_{Q_c}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ j$ then $i\ \mathbb{L}_{P_c \cdot Q_c}\ j$.

Proving $P_0 \cdot Q_2 = O \cdot Q_0$ Let us now prove that $P_0 \cdot Q_2$ is equal to $O \cdot Q_0$. To simplify the proof, let us first characterize Q_2 directly in term of P_0, P_1 and Q_0. By replacing Q_1 by its definition in the definition of Q_2, it is seen that, for all $i, j \in [d-1]$:

- $\textsc{position}_{\mathcal{V}'_i(m)}[Q_2](i) = \textsc{position}_{\mathcal{V}'_i(m)}[Q_0](i) \cap \textsc{position}_{\mathcal{V}'_i(m)}[P_0](i) \cap \textsc{position}_{\mathcal{V}'_i(m)}[P_1](i)$,
- $i\ \mathbb{E}_{Q_2}\ j$ if and only if $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_1}\ j$,
- $i\ \mathbb{S}_{Q_2}\ j$ if and only if $i\ \mathbb{S}_{Q_0}\ j$ and $i \in \mathbb{B}_{P_0}$ and $i \in \mathbb{B}_{P_1}$ and $j \in \mathbb{O}_{P_0}$ and $j \in \mathbb{O}_{P_1}$,
- $i\ \mathbb{L}_{Q_2}\ j$ if and only if $i\ \mathbb{L}_{Q_0}\ j$ or $\{i\ \mathbb{E}_{Q_0}\ j$ and $[i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or $(i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j)]\}$ and
- $Q_2 \overset{\mathbb{M}}{\cong} Q_0$.

Let $i, j \in [d-1]$:

- Let us consider $\mathbb{O}$, the case $\mathbb{B}$ is similar:

$$
\begin{array}{lll}
& i \in \mathbb{O}_{O \cdot Q_0} & \\
= & i \in \mathbb{O}_O \quad \wedge i \in \mathbb{O}_{Q_0} & \text{(using the definition of } O \cdot Q_0) \\
= & i \in \mathbb{O}_{P_0} \wedge i \in \mathbb{O}_{P_1} \wedge i \in \mathbb{O}_{Q_0} & \text{(using the definition of } O) \\
= & i \in \mathbb{O}_{P_0} \quad \wedge i \in \mathbb{O}_{Q_2} & \text{(using the definition of } Q_2) \\
= & i \in \mathbb{O}_{P_0 \cdot Q_2}. & \text{(using the definition of } P_0 \cdot Q_2)
\end{array}
$$

- Let us consider $\mathbb{E}$.

$$
\begin{array}{lll}
i\ \mathbb{E}_{O \cdot Q_0}\ j \iff & i\ \mathbb{E}_O\ j \quad \wedge i\ \mathbb{E}_{Q_0}\ j & \text{(using the definition of } O \cdot Q_0) \\
\iff & i\ \mathbb{E}_{P_0}\ j \wedge i\ \mathbb{E}_{P_1}\ j \wedge i\ \mathbb{E}_{Q_0}\ j & \text{(using the definition of } O) \\
\iff & i\ \mathbb{E}_{P_0}\ j \quad \wedge i\ \mathbb{E}_{Q_2}\ j & \text{(using the definition of } Q_2) \\
\iff & i\ \mathbb{E}_{P_0 \cdot Q_2}\ j. & \text{(using the definition of } P_0 \cdot Q_2)
\end{array}
$$

- Let us consider $\mathbb{S}$.

$$
\begin{array}{lll}
& i\ \mathbb{S}_{O\cdot Q_0}\ j & \\
\Longleftrightarrow & (i\ \mathbb{S}_O\ j \ \wedge i\ \mathbb{E}_{Q_0}\ j &) \vee \\
& (i \in \mathbb{B}_O \ \wedge \quad j \in \mathbb{O}_O \ \wedge \quad i\ \mathbb{S}_{Q_0}\ j) & \text{(using the definition of } O \cdot Q_0) \\
\Longleftrightarrow & (i\ \mathbb{S}_{P_0}\ j \ \wedge i\ \mathbb{S}_{P_1}\ j \ \wedge i\ \mathbb{E}_{Q_0}\ j &) \vee \\
& (i \in \mathbb{B}_{P_0} \ \wedge i \in \mathbb{B}_{P_1} \wedge j \in \mathbb{O}_{P_0} \wedge j \in \mathbb{O}_{P_1} \wedge i\ \mathbb{S}_{Q_0}\ j) & \text{(using the definition of } O) \\
\Longleftrightarrow & (i\ \mathbb{S}_{P_0}\ j \ \wedge i\ \mathbb{E}_{Q_2}\ j &) \vee \\
& (i \in \mathbb{B}_{P_0} \ \wedge \quad j \in \mathbb{O}_{P_0} \wedge \quad i\ \mathbb{S}_{Q_2}\ j) & \text{(using the definition of } Q_2) \\
\Longleftrightarrow & i\ \mathbb{S}_{P_0\cdot Q_2}\ j. & \text{(using the definition of } P_0 \cdot Q_2)
\end{array}
$$

- Let us now consider $\mathbb{L}$.

  Let us assume that $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$ and let us prove that $i\ \mathbb{L}_{O\cdot Q_0}\ j$. Since $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$, either ($i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_2}\ j$), or $i\ \mathbb{L}_{Q_2}\ j$. The two cases are considered separately.

  - Let us first suppose that $i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_2}\ j$. Since $i\ \mathbb{E}_{Q_2}\ j$, by definition of Q_2, $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_1}\ j$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$, $i\ \mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{S}_{P_0}\ j$ and $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $i \in \beta$ and $j \in \zeta$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_1}\ j$, $P_1 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $i \in \beta$ and $j \in \zeta$, it follows that $i\ \mathbb{S}_{P_1}\ j$. Since $i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$, by definition of O, $i\ \mathbb{S}_O\ j$. Since $i\ \mathbb{S}_O\ j$ and since $i\ \mathbb{E}_{Q_0}\ j$, it follows that $i\ \mathbb{L}_{O\cdot Q_0}\ j$.
  - Finally, let us suppose that $i\ \mathbb{L}_{Q_2}\ j$. Since $i\ \mathbb{L}_{Q_2}\ j$, by definition of Q_2 either $i\ \mathbb{L}_{Q_0}\ j$ or $\{i\ \mathbb{E}_{Q_0}\ j$ and $[i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{E}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$)]$\}$. The two cases are considered separately.
    - If $i\ \mathbb{L}_{Q_0}\ j$ then $i\ \mathbb{L}_{O\cdot Q_0}\ j$.
    - Let us now suppose that $i\ \mathbb{E}_{Q_0}\ j$ and [$i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$)]. By definition of O, $i\ \mathbb{L}_O\ j$.

  Let us now suppose that $i\ \mathbb{L}_{O\cdot Q_0}\ j$, and let us prove that $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$. Since $i\ \mathbb{L}_{O\cdot Q_0}\ j$, either ($i\ \mathbb{L}_O\ j$ and $i\ \mathbb{E}_{Q_0}\ j$), or $i\ \mathbb{L}_{Q_0}\ j$. The two cases are considered separately.

  - Let us first suppose that $i\ \mathbb{L}_O\ j$ and $i\ \mathbb{E}_{Q_0}\ j$. Since $i\ \mathbb{L}_O\ j$, by definition of O, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$) or ($i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$). The three cases are considered separately.
    - Let us first assume that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$, by definition of Q_2, $i\ \mathbb{L}_{Q_2}\ j$. Hence $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.
    - Let us now suppose that $i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$ by definition of Q_2, then $i\ \mathbb{E}_{Q_2}\ j$. Since $i\ \mathbb{S}_{P_0}\ j$ and since $i\ \mathbb{E}_{Q_2}\ j$, $i\ \mathbb{S}_{P_0\cdot Q_2}\ j$ hence $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.
    - Let us finally assume that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$ and $i\ \mathbb{E}_{Q_0}\ j$, by Definition of Q_2, $i\ \mathbb{L}_{Q_2}\ j$. Since $i\ \mathbb{L}_{Q_2}\ j$, $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.
  - If $i\ \mathbb{L}_{Q_0}\ j$, by definition of Q_2, $i\ \mathbb{L}_{Q_2}\ j$, and then $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.

- Let us finally consider $\textsc{length}_{m,b}$ and $\textsc{modulo}_m$. Since $P_0 \overset{\mathbb{M}}{\cong} O$ and $Q_0 \overset{\mathbb{M}}{\cong} Q_2$ and $\overset{\mathbb{M}}{\cong}$ is a congruence relation, then $O \cdot Q_0 \overset{\mathbb{M}}{\cong} P_0 \cdot Q_2$.

Proving $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$ The remaining of the proof consists in a Axiom by Axiom study to show that O belongs to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$ and Q_1 and Q_2 belong to $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota}$. Let us first prove that $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$. This proof, and all following proofs that an element O of $\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota}$ belong to $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota}$ or to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$, is a long but straightforward case study, using the definition of O.

Let $i, j, k \in [d-1]$ such that $i \in \nu \Longleftrightarrow j \in \nu \Longleftrightarrow k \in \nu$.

- Let us consider Axioms (1 - $\mathbb{E}$ equivalence). Since $\mathbb{E}_O$ is the intersection of two equivalence relations, it is an equivalence relation.

- Axioms (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$), (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$) and (6 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{E}$ compatible) hold for O since they hold for P_0 and for P_1, and that the symbols $\mathbb{E}$, $\mathbb{S}$, $\mathbb{O}$ and $\mathbb{B}$ on O are defined as the intersections of the same symbols on P_0 and on P_1.

- Since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$, $O \overset{\mathbb{OESBL}}{\preccurlyeq} P_0$, $O \overset{\mathbb{M}}{\cong} P_0$ and $\mathbb{L}_O \supseteq \mathbb{L}_{P_0}$, by Lemma 8.1.15, O satisfies Axioms (4 - $\mathbb{S}$ and $\overline{\mathbb{E}}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (7 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{S}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod), (19 - Rigid case) and (20 - ν) and $O \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$.

- Let us consider Axiom (8 - $\mathbb{L}$ asymmetric). Let us assume that $i\ \mathbb{L}_O\ j$ and let us prove that $j\ \mathbb{L}_O\ i$ does not hold. Since $i\ \mathbb{L}_O\ j$, by definition of O, either $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$) or ($i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$) hold. The three cases are considered separately.

  - Let us suppose that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ i$ does not hold. Hence by definition of O, $j\ \mathbb{L}_O\ i$ does not hold.
  - Let us assume that $i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$. Since $i\ \mathbb{S}_{P_0}\ j$, $j\ \mathbb{L}_{P_0}\ i$ does not hold. Since $i\ \mathbb{S}_{P_1}\ j$, $j\ \mathbb{L}_{P_1}\ i$ does not hold. Since neither $j\ \mathbb{L}_{P_0}\ i$ nor $j\ \mathbb{L}_{P_1}\ i$ hold, by definition of O, $j\ \mathbb{L}_O\ i$ does not hold.
  - Let us assume that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$ hold. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ holds, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$ does not hold. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$, $j\ \mathbb{L}_{P_1}\ i$ does not hold. Since neither $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$ nor $j\ \mathbb{L}_{P_1}\ i$ hold, by definition of O, $j\ \mathbb{L}_O\ i$ does not hold.

- Let us consider Axiom (9 - $\mathbb{L}$ transitive). Let us assume that $i\ \mathbb{L}_O\ j$ and $j\ \mathbb{L}_O\ k$ and let us prove that $i\ \mathbb{L}_O\ k$.

  Since $i\ \mathbb{L}_O\ j$ by definition of O, either $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or ($i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$) or ($i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$) hold. The three cases are considered separately.

  - Let us suppose that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. It is claimed that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, by definition of O, it implies $i\ \mathbb{L}\overline{\mathbb{S}}_O\ k$. Let us prove that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.

    Since $j\ \mathbb{L}_O\ k$, either $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ or ($j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$) or ($j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$). The three cases are considered separately.

    * Let us suppose that $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.
    * Let us suppose that $j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$. Since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and since $j\ \mathbb{S}_{P_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.
    * Let us suppose that $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and since $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.

  - Let us now suppose that $i\ \mathbb{S}_{P_0}\ j$ and $i\ \mathbb{S}_{P_1}\ j$. Since $i\ \mathbb{S}_{P_0}\ j$ and since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$, $j \in \zeta$.

    Since $j\ \mathbb{L}_O\ k$, either $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ or ($j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$) or ($j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$). The three cases are considered separately.

* Let us suppose that $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. This case is the symmetric of the case where $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$. Indeed, it suffices to remark that (i,j) and (j,k) are switched. This remark holds for all other proofs concerning the Axiom (9 - $\mathbb{L}$ transitive).
Since $i\ \mathbb{S}_{P_0}\ j$ and since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, by definition of O, it implies $i\ \mathbb{L}\overline{\mathbb{S}}_{O}\ k$.
* Let us suppose that $j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$. Since $j\ \mathbb{S}_{P_0}\ k$ and since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $j \in \beta$. Since $j \in \zeta$ and $j \in \beta$ and $\zeta \cap \beta = \emptyset$, it is a contradiction.
* Let us suppose that $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$, $j \in \zeta$ and $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it follows that $j\ \mathbb{P}_{P_0}\ k$ or $j\ \mathbb{E}_{P_0}\ k$, which imply $i\ \mathbb{E}_{P_0}\ k$ and $i\ \mathbb{S}_{P_0}\ k$ respectively. In both cases, $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $i\ \mathbb{L}_{P_1}\ j$ and since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$, by definition of O, $i\ \mathbb{L}\overline{\mathbb{S}}_{O}\ k$.

– Let us assume that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$ hold.

Since $j\ \mathbb{L}_O\ k$, either $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ or ($j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$) or ($j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$). The three cases are considered separately.

* Let us suppose that $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, by definition of O, it implies $i\ \mathbb{L}\overline{\mathbb{S}}_{O}\ k$.
* Let us suppose that $j\ \mathbb{S}_{P_0}\ k$ and $j\ \mathbb{S}_{P_1}\ k$. Since $j\ \mathbb{S}_{P_0}\ k$ and since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $j \in \beta$. Since $j \in \beta$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it follows that $i\ \mathbb{P}_{P_0}\ j$ or $i\ \mathbb{E}_{P_0}\ j$, which imply $i\ \mathbb{E}_{P_0}\ k$ and $i\ \mathbb{S}_{P_0}\ k$ respectively. In both cases $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $j\ \mathbb{S}_{P_0}\ k$ and $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it follows that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$ and since $j\ \mathbb{S}_{P_1}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$, by definition of O, $i\ \mathbb{L}\overline{\mathbb{S}}_{O}\ k$.
* Let us suppose that $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and since $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$, $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ j$ and since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$, by definition of O, $i\ \mathbb{L}\overline{\mathbb{S}}_{O}\ k$.

- Let us consider Axiom (10 - $i\ \mathbb{E}_T\ j, i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$). Let us suppose that $i\ \mathbb{E}_O\ j$ and $i\ \mathbb{L}_O\ k$ hold and let us prove that $j\ \mathbb{L}_O\ k$ or $j\ \mathbb{E}_O\ k$ hold. Since $i\ \mathbb{E}_O\ j$, $i\ \mathbb{E}_{P_0}\ j$ and $i\ \mathbb{E}_{P_1}\ j$. Since $i\ \mathbb{L}_O\ k$, either $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, either ($i\ \mathbb{S}_{P_0}\ k$ and $i\ \mathbb{S}_{P_1}\ k$) or ($i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$). The three cases are considered separately.

  – Let us suppose that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and since $i\ \mathbb{E}_{P_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, hence $i\ \mathbb{L}\overline{\mathbb{S}}_{O}\ k$.

  – Let us suppose that $i\ \mathbb{S}_{P_0}\ k$ and $i\ \mathbb{S}_{P_1}\ k$. Since $i\ \mathbb{S}_{P_0}\ k$ and since $i\ \mathbb{E}_{P_0}\ j$, $j\ \mathbb{S}_{P_0}\ k$, hence $j\ \mathbb{L}_{P_0}\ k$.

  – Let us suppose that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and since $i\ \mathbb{E}_{P_0}\ j$, $j\ \mathbb{E}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$ and since $i\ \mathbb{E}_{P_1}\ j$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$. Since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$ and $j\ \mathbb{E}_{P_0}\ k$, by definition of O, $j\ \mathbb{L}_O\ k$.

- Let us consider Axiom (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible). Let us suppose that $i\ \mathbb{E}_O\ j$ holds. Since $i\ \mathbb{E}_O\ j$ by definition of O, $i\ \mathbb{E}_{P_0}\ j$ and $i\ \mathbb{E}_{P_1}\ j$, hence, by definition of O, $i\ \mathbb{L}_O\ j$ does not hold.

- Let us consider Axiom (12 - $\textsc{position}_{\mathcal{V}_\iota'(m)}$ and $\mathbb{L}$ compatible). Let us assume that [($i \in \mathbb{O}_O$ and $j \notin \mathbb{O}_O$) or ($i \notin \mathbb{B}_O$ and $j \in \mathbb{B}_O$)] and that $\mathbb{L}$ belongs to $I^2_{\mathcal{V}_\iota'}$. Let us prove that $i\ \mathbb{L}_O\ j$.

  Let us consider the case ($i \in \mathbb{O}_O$ and $j \notin \mathbb{O}_O$), the other one is similar. Since $i \in \mathbb{O}_O$, by definition of O, then $i \in \mathbb{O}_{P_0}$ and $i \in \mathbb{O}_{P_1}$.

  Two cases are considered, depending on whether $j \in \mathbb{O}_{P_0}$ or not.

– Let us suppose that $j \in \mathbb{O}_{P_0}$. Since $j \notin \mathbb{O}_O$, and $j \in \mathbb{O}_{P_0}$, by definition of O, $j \notin \mathbb{O}_{P_1}$. Since $j \in \mathbb{O}_{P_0}$ and since $i \in \mathbb{O}_{P_0}$, $i \mathbb{E}_{P_0} j$. Since $i \in \mathbb{O}_{P_1}$ and since $j \notin \mathbb{O}_{P_1}$, $i \mathbb{L}\overline{\mathbb{S}}_{P_1} j$. Since $i \mathbb{E}_{P_0} j$ and $i \mathbb{L}\overline{\mathbb{S}}_{P_1} j$, by definition of O, then $i \mathbb{L}_O j$.

– Let us suppose that $j \notin \mathbb{O}_{P_0}$. Since $i \in \mathbb{O}_{P_0}$ and since $j \notin \mathbb{O}_{P_0}$, $i \mathbb{L}\overline{\mathbb{S}}_{P_0} j$. Since $i \mathbb{L}\overline{\mathbb{S}}_{P_0} j$, by definition of O, $i \mathbb{L}_O j$.

- Let us consider Axiom (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$). Let us assume that $i \mathbb{S}_O j$ and $i \mathbb{L}_O k$ and let us prove that either $i \mathbb{E}_O k$ or $i \mathbb{L}_O k$. Since $i \mathbb{S}_O j$, it implies that $i \mathbb{S}_{P_0} j$ and $i \mathbb{S}_{P_1} j$. Since $i \mathbb{S}_{P_0} j$ it follows that $j \in \zeta$ and $i \in \beta$. Since $i \mathbb{L}_O k$, $i \mathbb{L}\overline{\mathbb{S}}_{P_0} k$ or ($i \mathbb{S}_{P_0} k$ and $i \mathbb{S}_{P_1} k$) or ($i \mathbb{E}\wr\mathbb{S}_{P_0} k$ and $i \mathbb{L}\overline{\mathbb{S}}_{P_1} k$). The three cases are considered separately.

  – Let us assume that $i \mathbb{L}\overline{\mathbb{S}}_{P_0} k$. Since $i \mathbb{L}\overline{\mathbb{S}}_{P_0} k$ and since $i \mathbb{S}_{P_0} j$, $j \mathbb{L}_{P_0} k$. Since $j \mathbb{L}_{P_0} k$ and since $j \in \zeta$, $j \mathbb{L}\overline{\mathbb{S}}_{P_0} k$. Since $j \mathbb{L}\overline{\mathbb{S}}_{P_0} k$, by definition of O, $j \mathbb{L}_O k$.

  – Let us assume that $i \mathbb{S}_{P_0} k$ and $i \mathbb{S}_{P_1} k$. Since $i \mathbb{S}_{P_0} k$ and since $i \mathbb{S}_{P_0} j$, $j \mathbb{E}_{P_0} k$. Since $i \mathbb{S}_{P_1} k$ and since $i \mathbb{S}_{P_1} j$, $j \mathbb{E}_{P_1} k$. Since $j \mathbb{S}_{P_0} k$ and $j \mathbb{S}_{P_1} k$, by definition of O, $i \mathbb{L}_O k$.

  – Finally, let us assume that $i \mathbb{E}\wr\mathbb{S}_{P_0} k$ and $i \mathbb{L}\overline{\mathbb{S}}_{P_1} k$. Since $i \mathbb{E}\wr\mathbb{S}_{P_0} k$ and since $i \mathbb{S}_{P_0} j$, $j \mathbb{E}\wr\mathbb{S}_{P_0} k$. Since $i \mathbb{L}\overline{\mathbb{S}}_{P_1} k$ and since $i \mathbb{S}_{P_1} j$ $j \mathbb{L}_{P_1} k$. Since $j \mathbb{L}_{P_1} k$ and since $j \in \zeta$, $j \mathbb{L}\overline{\mathbb{S}}_{P_1} k$. Since $j \mathbb{E}\wr\mathbb{S}_{P_0} k$ and $j \mathbb{L}\overline{\mathbb{S}}_{P_1} k$, by definition of O, $j \mathbb{L}_O k$.

Proving $Q_1, Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}'_\iota}$ Let us prove by induction on c in $\{0,1,2\}$ that $Q_c \in \mathbb{POP}^m_{\nu,\mathcal{V}'_\iota}$. For $c = 0$ it holds by hypothesis. Let us assume that c is 0 or 1 and that $Q_c \in \mathbb{POP}^m_{\nu,\mathcal{V}'_\iota}$ and let us prove that $Q_{c+1} \in \mathbb{POP}^m_{\nu,\mathcal{V}'_\iota}$. Let $i, j, k \in [d-1]$ such that $i \in \nu \Longleftrightarrow j \in \nu \Longleftrightarrow k \in \nu$.

- Let us consider Axiom (1 - $\mathbb{E}$ equivalence). Since $\mathbb{E}_{Q_{c+1}}$ is the intersection of the equivalence relations $\mathbb{E}_{Q_c}$ and $\mathbb{E}\wr\mathbb{S}_{P_c}$, then $\mathbb{E}_{Q_{c+1}}$ is an equivalence relation.

- Let us consider Axiom (2 - $i \mathbb{S}_T j \wedge i \mathbb{S}_T k \Longrightarrow j \mathbb{E}_T k$). Let us assume that $i \mathbb{S}_{Q_{c+1}} j$ and $i \mathbb{S}_{Q_{c+1}} k$ and let us prove that $j \mathbb{E}_{Q_{c+1}} k$, the other case is similar. Since $i \mathbb{S}_{Q_{c+1}} j$, by definition of Q_{c+1}, $i \in \mathbb{B}_{P_c}$ and $j \in \mathbb{O}_{P_c}$ and $i \mathbb{S}_{Q_c} j$. Since $i \mathbb{S}_{Q_{c+1}} k$, by definition of Q_{c+1}, $i \in \mathbb{B}_{P_c}$ and $k \in \mathbb{O}_{P_c}$ and $i \mathbb{S}_{Q_c} k$. Since $j \in \mathbb{O}_{P_c}$ and since $k \in \mathbb{O}_{P_c}$, $j \mathbb{E}_{P_c} k$. Since $i \mathbb{S}_{Q_c} j$ and since $i \mathbb{S}_{Q_c} k$, $j \mathbb{E}_{Q_c} k$. Since $j \mathbb{E}_{P_c} k$ and $j \mathbb{E}_{Q_c} k$, by definition of Q_{c+1}, $j \mathbb{E}_{Q_{c+1}} k$.

- Let us consider Axiom (3 - $i \mathbb{S}_T j \wedge i \mathbb{E}_T k \Longrightarrow j \mathbb{S}_T k$). Let us assume that $i \mathbb{E}_{Q_{c+1}} j$ and $i \mathbb{S}_{Q_{c+1}} k$ and let us prove that $j \mathbb{S}_{Q_{c+1}} k$, the other case is similar. Since $i \mathbb{E}_{Q_{c+1}} j$, by definition of Q_{c+1}, $i \mathbb{E}_{P_c} j$ and $i \mathbb{E}_{Q_c} j$. Since $i \mathbb{S}_{Q_{c+1}} k$, by definition of Q_{c+1}, $i \in \mathbb{B}_{P_c}$ and $k \in \mathbb{O}_{P_c}$ and $i \mathbb{S}_{Q_c} k$. Since$i \mathbb{E}_{P_c} j$ and since $k \in \mathbb{O}_{P_c}$, $j \in \mathbb{O}_{P_c}$. Since $i \mathbb{E}_{Q_c} j$ and since $i \mathbb{S}_{Q_c} k$, $j \mathbb{S}_{Q_c} k$. Since $j \in \mathbb{O}_{P_c}$ and $j \mathbb{S}_{Q_c} k$ and $k \in \mathbb{B}_{P_c}$, by definition of Q_{c+1}, $j \mathbb{S}_{Q_{c+1}} k$.

- Since $Q_c \in \mathbb{POP}^m_{\nu,\mathcal{V}'_\iota}$, $Q_{c+1} \overset{\mathbb{OESBL}}{\preccurlyeq} Q_c$, $Q_{c+1} \overset{\mathbb{M}}{\cong} Q_c$ and $\mathbb{L}_{Q_{c+1}} \subseteq \mathbb{L}_{Q_c}$, by Lemma 8.1.15, Q_{c+1} satisfies Axioms (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (7 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{S}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod), (19 - Rigid case) and (20 - ν).

- Since Q_c and P_c satisfy Axiom (6 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{E}$ compatible), and that the symbols $\mathbb{O}$ and $\mathbb{B}$ for Q_{c+1} is defined as the intersection of this relation on P_c and on Q_c, then the element Q_{c+1} satisfies Axiom (6 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{E}$ compatible).

- Let us consider Axioms (8 - $\mathbb{L}$ asymmetric) and (9 - $\mathbb{L}$ transitive). Since $\mathbb{L}_{Q_{c+1}}$ is defined as the lexicographical order generated by $\mathbb{L}_{Q_c}$ and $\mathbb{L}\overline{\mathbb{S}}_{P_c}$, it is an order, hence Q_{c+1} satisfies Axioms (8 - $\mathbb{L}$ asymmetric) and (9 - $\mathbb{L}$ transitive).

- Let us consider Axiom (10 - $i\ \mathbb{E}_T\ j, i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$). Let us suppose that $i\ \mathbb{E}_{Q_{c+1}}\ j$ and $i\ \mathbb{L}_{Q_{c+1}}\ k$ hold and let us prove that $j\ \mathbb{L}_{Q_{c+1}}\ k$ or $j\ \mathbb{E}_{Q_{c+1}}\ k$ hold. Since $i\ \mathbb{E}_{Q_{c+1}}\ j$, by definition of Q_{c+1}, $i\ \mathbb{E}_{Q_c}\ j$ and $i\ \mathbb{E}_{P_c}\ j$. Since $i\ \mathbb{L}_{Q_{c+1}}\ k$, by definition of Q_{c+1}, either $i\ \mathbb{L}_{Q_c}\ k$ or ($i\ \mathbb{E}_{Q_c}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$), both cases are consider separately.
  - Let us suppose that $i\ \mathbb{L}_{Q_c}\ k$. Since $i\ \mathbb{L}_{Q_c}\ k$ and since $i\ \mathbb{E}_{Q_c}\ j$, $j\ \mathbb{L}_{Q_c}\ k$, hence, by definition of Q_{c+1}, $j\ \mathbb{L}_{Q_{c+1}}\ k$.
  - Let us suppose that $i\ \mathbb{E}_{Q_c}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$. Having $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$ and $i \in \mathbb{B}_{P_c}$ is a contradiction.
- let us consider Axiom (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible). Let us suppose that $i\ \mathbb{E}_{Q_{c+1}}\ j$ holds. Since $i\ \mathbb{E}_{Q_{c+1}}\ j$ by definition of Q_{c+1}, $i\ \mathbb{E}_{Q_c}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_c}\ j$, hence, by definition of Q_{c+1}, $i\ \mathbb{L}_{Q_{c+1}}\ j$ does not hold.
- Let us consider Axiom (12 - $\text{POSITION}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{L}$ compatible). Let us assume that [($i \in \mathbb{O}_{Q_{c+1}}$ and $j \notin \mathbb{O}_{Q_{c+1}}$) or ($i \notin \mathbb{B}_{Q_{c+1}}$ and $j \in \mathbb{B}_{Q_{c+1}}$)] and that $\mathbb{L}$ belongs to $I^2_{\mathcal{V}'_\iota}$.

  Let us consider the case ($i \in \mathbb{O}_{Q_{c+1}}$ and $j \notin \mathbb{O}_{Q_{c+1}}$), the other case is similar. Since $i \in \mathbb{O}_{Q_{c+1}}$, by definition of Q_{c+1}, $i \in \mathbb{O}_{Q_c}$ and $i \in \mathbb{O}_{P_c}$. Two cases are considered, depending on whether $j \in \mathbb{O}_{Q_c}$ holds or not.
  - Let us suppose that $j \in \mathbb{O}_{Q_c}$. Since $j \notin \mathbb{O}_{Q_{c+1}}$ and $j \in \mathbb{O}_{Q_c}$, by definition of Q_{c+1}, $j \notin \mathbb{O}_{P_c}$. Since $i \in \mathbb{O}_{Q_c}$ and since $j \in \mathbb{O}_{Q_c}$, $i\ \mathbb{E}\wr\mathbb{S}_{Q_c}\ j$. Since $i \in \mathbb{O}_{P_c}$ and since $j \notin \mathbb{O}_{P_c}$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ j$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ j$ and since $i\ \mathbb{E}\wr\mathbb{S}_{Q_c}\ j$, by definition of Q_{c+1}, $i\ \mathbb{L}_{Q_{c+1}}\ j$.
  - Let us suppose that $j \notin \mathbb{O}_{Q_c}$. Since $i \in \mathbb{O}_{Q_c}$ and since $j \notin \mathbb{O}_{Q_c}$, $i\ \mathbb{L}_{Q_c}\ j$, and by definition of Q_{c+1}, $i\ \mathbb{L}_{Q_{c+1}}\ j$.
- Let us consider Axiom (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$). Let us suppose that $i\ \mathbb{S}_{Q_{c+1}}\ j$ and $i\ \mathbb{L}_{Q_{c+1}}\ k$ hold and let us prove that $j\ \mathbb{L}_{Q_{c+1}}\ k$ or $j\ \mathbb{E}_{Q_{c+1}}\ k$ hold. Since $i\ \mathbb{S}_{Q_{c+1}}\ j$, by definition of Q_{c+1}, $i\ \mathbb{S}_{Q_c}\ j$ and $i \in \mathbb{B}_{P_c}$ and $j \in \mathbb{O}_{P_c}$. Since $i\ \mathbb{L}_{Q_{c+1}}\ k$, by definition of Q_{c+1}, either $i\ \mathbb{L}_{Q_c}\ k$ or ($i\ \mathbb{E}_{Q_c}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$), both cases are consider separately.
  - Let us suppose that $i\ \mathbb{L}_{Q_c}\ k$. Since $i\ \mathbb{L}_{Q_c}\ k$ and $i\ \mathbb{S}_{Q_c}\ j$ then either $j\ \mathbb{E}_{Q_c}\ k$ or $j\ \mathbb{L}_{Q_c}\ k$, both cases are considered separately.
    - Let us suppose that $j\ \mathbb{E}_{Q_c}\ k$. Two cases must be considered, depending on whether $k \in \mathbb{O}_{P_c}$ or not.
      - Let us suppose that $k \in \mathbb{O}_{P_c}$. Since $k \in \mathbb{O}_{P_c}$ and $j \in \mathbb{O}_{P_c}$, then $\mathbb{E}\wr\mathbb{S}P_c jk$. Since $\mathbb{E}\wr\mathbb{S}P_c jk$ and since $j\ \mathbb{E}_{Q_c}\ k$, by definition of Q_{c+1} $j\ \mathbb{E}_{Q_{c+1}}\ k$.
      - Let us suppose that $k \notin \mathbb{O}_{P_c}$. Since $j \in \mathbb{O}_{P_c}$ and $k \notin \mathbb{O}_{P_c}$, then $j\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$. Since $j\ \mathbb{E}_{Q_c}\ k$ and $j\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$, by definition of Q_{c+1}, $j\ \mathbb{L}\overline{\mathbb{S}}_{Q_{c+1}}\ k$.
    - Let us suppose that $j\ \mathbb{L}_{Q_c}\ k$, by definition of Q_{c+1}, it implies $j\ \mathbb{L}_{Q_{c+1}}\ k$.
  - Let us suppose that $i\ \mathbb{E}_{Q_c}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$. Having $i\ \mathbb{L}\overline{\mathbb{S}}_{P_c}\ k$ and $i \in \mathbb{B}_{P_c}$ is a contradiction.

□

8.2.2 $\sim_\phi$ and $\overset{\mathbb{L}}{\preccurlyeq}$

The following proposition is similar to Lemma 8.2.2, except that it considers the order $\overset{\mathbb{L}}{\preccurlyeq}$ and not the order $\overset{\mathbb{OESB}}{\preccurlyeq}$.

Lemma 8.2.3. *Let $P_0, P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ and $P_0 \sim_\phi P_1$ and $P_0 \overset{\mathbb{L}}{\not\cong} P_1$.*

There exists $R \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $R \sim_\phi P_0$, and $R \sqsubset P_0$.

Intuitively, the proof consists in choosing a pair of distinct $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes (L, G) such that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ holds and $L\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ G$ does not, and proving that removing $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ from P_0 creates a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop R which is $\sim_\phi$-equivalent to P_0.

In order to prove Lemma 8.2.3, another lemma must first be proved.

Lemma 8.2.4. *Let $P_0, P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ and $P_0 \sim_\phi P_1$ hold and such that there exists L and G two distinct $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes such that:*

1. *$L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$,*
2. *For all $k \in [d-1]$: ($L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and $k \notin G$ imply $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$) and ($k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ and $k \notin L$ imply $k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ L$) and*
3. *$L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$.*

Let $O \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ be defined as follows, for all $i, j \in [d-1]$:

- *$O \overset{\mathbb{MOESB}}{\cong} P_0$,*
- *$i\ \mathbb{L}_O\ j$ holds if and only if [$i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$)] or ($i \in G$ and $j \in L$).*

Then $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $O \sim_\phi P_0$.

Intuitively, Condition (2) of Lemma 8.2.4 states that L and G satisfies exactly the same property when compared to other classes. The $(\nu,\mathcal{V}_\iota')^m$-pop O is P_0 where the order $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ has been reversed into $L\ \mathbb{G}\overline{\mathbb{P}}_O\ G$.

Note that Condition (2) implies that there are no $k \in [d-1]$ such that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$. Intuitively, G is a $\mathbb{L}\overline{\mathbb{S}}_{P_0}$-successor of L, note however that $L\ \mathbb{S}_{P_0}\ G$ does not hold. In fact, this notation is not definition for $\mathbb{E}\wr\mathbb{S}$-classes.

Lemma 8.2.4 is now proved.

Proof of Lemma 8.2.4. The proof is similar to the proof of Lemma 8.2.2. The two only differences are that the value of O is fixed and that the definition of Q_1 and Q_2 are different. The two statements of the lemma are proved separately.

Proving $O \sim_\phi P_0$. Let us prove that $O \sim_\phi P_0$, that is, let us prove that $(O^{-1}\phi)(Q_0)$ is equivalent to $(P_0^{-1}\phi)(Q_0)$ for all $Q_0 \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$.

Let $Q_0 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$. Let us first claim that there exists $Q_1, Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ such that $P_0 \cdot Q_0 = P_0 \cdot Q_1$, $P_1 \cdot Q_1 = P_1 \cdot Q_2$ and $P_0 \cdot Q_2 = O \cdot Q_0$. Then

$$\begin{aligned}
(P_0^{-1}\phi)(Q_0) &\iff (P_0^{-1}\phi)(Q_1) && \text{(using Corollary 8.1.25)}\\
&\iff (P_1^{-1}\phi)(Q_1) && \left(P_0 \sim_\phi P_1\right)\\
&\iff (P_1^{-1}\phi)(Q_2) && \text{(using Corollary 8.1.25)}\\
&\iff (P_0^{-1}\phi)(Q_2) && \left(P_0 \sim_\phi P_1\right)\\
&\iff (O^{-1}\phi)(Q_0) && \text{(using Corollary 8.1.25).}
\end{aligned}$$

Constructing Q_1 The first $(\nu,\mathcal{V}_\iota')^m$-pop $Q_1 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ is now defined. The construction of Q_1 is similar to the construction of Q_1 in Lemma 8.2.2. That is, Q_1 is similar to Q_0. The relation $\mathbb{O}$ and $\mathbb{B}$ in Q_1 are the intersection of those relations in P_0 and in Q_0. More generally, each relation $\mathbb{O},\mathbb{S},\mathbb{B}$ occur in Q_1 only if they occur in Q_0 and they are mandatory to obtain the equality $P_0 \cdot Q_1 = P_0 \cdot Q_0$. The case of $\mathbb{E}$ is slightly different, since $i\ \mathbb{E}_{Q_1}\ j$ holds if and only if, either it is mandatory to obtain the equality $P_0 \cdot Q_1 = P_0 \cdot Q_0$, or if $i,j \in L \cup G$.

Let us now define Q_1. For all $i,j \in [d-1]$:

- $\textsc{position}_{\mathcal{V}_\iota'(m)}[Q_1](i) = \textsc{position}_{\mathcal{V}_\iota'(m)}[Q_0](i) \cap \textsc{position}_{\mathcal{V}_\iota'(m)}[P_0](i)$,
- $i\ \mathbb{E}_{Q_1}\ j$ if and only if $i\ \mathbb{E}_{Q_0}\ j$ and $[i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i,j \in L \cup G]$,
- $i\ \mathbb{S}_{Q_1}\ j$ if and only if $i\ \mathbb{S}_{Q_0}\ j$ and $i \in \mathbb{B}_{P_0}$ and $j \in \mathbb{O}_{P_0}$.
- $i\ \mathbb{L}_{Q_1}\ j$ if and only if $i\ \mathbb{L}_{Q_0}\ j$ or $[i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $(i \notin L$ or $j \notin G)]$ and
- $Q_1 \overset{\mathbb{M}}{\cong} Q_0$.

Constructing Q_2 The $(\nu,\mathcal{V}_\iota')^m$-pop $Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ is now defined. Intuitively, Q_2 is Q_1 where, in each $\mathbb{E}_{Q_1}$-classes, the positions of G are lesser that the positions of L. Let us now define Q_2. For all $i,j \in [d-1]$:

- $Q_2 \overset{\mathbb{OSBM}}{\cong} Q_1$,
- $i\ \mathbb{E}_{Q_2}\ j$ if and only if $i\ \mathbb{E}_{Q_1}\ j$ and $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$,
- $i\ \mathbb{L}_{Q_2}\ j$ if and only if $i\ \mathbb{L}_{Q_1}\ j$ or $(i\ \mathbb{E}_{Q_1}\ j$ and $i \in G$ and $j \in L)$.

Hence $i\ \mathbb{L}\overline{\mathbb{S}}_{Q_2}\ j$ if and only if $i\ \mathbb{L}\overline{\mathbb{S}}_{Q_1}\ j$ or $(i\ \mathbb{E}_{Q_1}\ j$ and $i \in G$ and $j \in L)$.

It remains to prove that Q_1 and Q_2 satisfy the claims.

Proving that $P_0 \cdot Q_0 = P_0 \cdot Q_1$ Let us prove that $P_0 \cdot Q_0 = P_0 \cdot Q_1$. For all $i,j \in [d-1]$:

- Let us consider $\mathbb{E}$.

$$\begin{aligned}
i\ \mathbb{E}_{P_0\cdot Q_0}\ j &\Longleftrightarrow i\ \mathbb{E}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_0}\ j && \text{(using the definition of } P_0 \cdot Q_0\text{)}\\
&\Longleftrightarrow ((i \in \beta) \Longleftrightarrow (j \in \beta)) \wedge ((i \in \zeta) \Longleftrightarrow (j \in \zeta)) \wedge \\
&\quad\ i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_0}\ j && \text{(using Definition 7.3.17)}\\
&\Longleftrightarrow ((i \in \beta) \Longleftrightarrow (j \in \beta)) \wedge ((i \in \zeta) \Longleftrightarrow (j \in \zeta)) \wedge \\
&\quad\ i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_1}\ j && \text{(using the definition of } Q_1\text{)}\\
&\Longleftrightarrow i\ \mathbb{E}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_1}\ j && \text{(using Definition 7.3.17)}\\
&\Longleftrightarrow i\ \mathbb{E}_{P_0\cdot Q_1}\ j. && \text{(using the definition of } P_0 \cdot Q_1\text{)}
\end{aligned}$$

- Let us consider $\mathbb{S}$:

$$\begin{aligned}
i\ \mathbb{S}_{P_0\cdot Q_0}\ j &\Longleftrightarrow (i\ \mathbb{S}_{P_0}\ j\ \wedge i\ \mathbb{E}_{Q_0}\ j) \vee \\
&\qquad (j \in \mathbb{O}_{P_0} \wedge i \in \mathbb{B}_{P_0}\ \wedge i\ \mathbb{S}_{Q_0}\ j) && \text{(using the definition of } P_0 \cdot Q_0\text{)}\\
&\Longleftrightarrow (i\ \mathbb{S}_{P_0}\ j\ \wedge i\ \mathbb{E}_{Q_1}\ j) \vee \\
&\qquad (j \in \mathbb{O}_{P_0} \wedge i \in \mathbb{B}_{P_0}\ \wedge i\ \mathbb{S}_{Q_1}\ j) && \text{(using the definition of } Q_1\text{)}\\
&\Longleftrightarrow i\ \mathbb{S}_{P_0\cdot Q_1}\ j && \text{(using the definition of } P_0 \cdot Q_1\text{)}.
\end{aligned}$$

- Let us now consider $\mathbb{L}$.

  Let us first suppose that $i\ \mathbb{L}_{P_0\cdot Q_0}\ j$ and let us prove that $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$. Since $i\ \mathbb{L}_{P_0\cdot Q_0}\ j$, either ($i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_0}\ j$) or $i\ \mathbb{L}_{Q_0}\ j$. The two cases are considered separately.

  - Let us assume that $i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_0}\ j$ hold. Since $i\ \mathbb{L}_{P_0}\ j$, by hypothesis, (either $i \notin G$ or $j \notin L$). Two cases must be considered, depending on whether ($i \in L$ and $j \in G$) or not.
    * Let us suppose that $i \in L$ and $j \in G$. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i, j \in L \cup G$, by definition of Q_1, $i\ \mathbb{E}_{Q_1}\ j$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $i\ \mathbb{E}_{Q_1}\ j$, $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$.
    * Let us suppose that ($i \notin L$ or $j \notin G$). Since $i\ \mathbb{L}_{P_0}\ j$, either $i\ \mathbb{S}_{P_0}\ j$ or $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$, both cases are considered separately.
      · Let us suppose that $i\ \mathbb{S}_{P_0}\ j$, hence $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$, by definition of Q_1, $i\ \mathbb{E}_{Q_1}\ j$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $i\ \mathbb{E}_{Q_1}\ j$, $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$.
      · Finally, let us suppose that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$) it follows that $i\ \mathbb{L}_{Q_1}\ j$, hence $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$.

    Since $i\ \mathbb{E}_{Q_0}\ j$ by definition of Q_1, ($i\ \mathbb{E}_{Q_1}\ j$ or $i\ \mathbb{L}_{Q_1}\ j$). Both cases imply that $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$ holds.
  - Finally, let us assume that $i\ \mathbb{L}_{Q_0}\ j$ holds. By definition of Q_1, $i\ \mathbb{L}_{Q_1}\ j$ holds. Since $i\ \mathbb{L}_{Q_1}\ j$ holds, $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$ holds.

  Let us now suppose that $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$ and let us prove that $i\ \mathbb{L}_{P_0\cdot Q_0}\ j$. Since $i\ \mathbb{L}_{P_0\cdot Q_1}\ j$, either ($i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_1}\ j$) or $i\ \mathbb{L}_{Q_1}\ j$. The two cases are considered separately.

  - Let us first suppose that $i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_1}\ j$. Since $i\ \mathbb{E}_{Q_1}\ j$, by definition of Q_1, $i\ \mathbb{E}_{Q_0}\ j$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}_{P_0\cdot Q_0}\ j$.
  - Finally, let us suppose that $i\ \mathbb{L}_{Q_1}\ j$. By definition of Q_1, $i\ \mathbb{L}_{Q_0}\ j$ or [$i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$)]. The two cases are considered separately.
    * If $i\ \mathbb{L}_{Q_0}\ j$ then $i\ \mathbb{L}_{P_0\cdot Q_0}\ j$.
    * If $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$) then $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0\cdot Q_0}\ j$.

- Let us finally consider $\textsc{length}_{m,b}$ and $\textsc{modulo}_m$. Since $Q_0 \overset{\mathbb{M}}{\cong} Q_1$ and $\overset{\mathbb{M}}{\cong}$ is a congruence relation, then $P_0 \cdot Q_0 \overset{\mathbb{M}}{\cong} P_0 \cdot Q_1$.

- Let us consider $\mathbb{O}$, the case $\mathbb{B}$ is similar:

$$\begin{aligned}
i \in \mathbb{O}_{P_0\cdot Q_0} &\Longleftrightarrow i \in \mathbb{O}_{P_0} \wedge i \in \mathbb{O}_{Q_0} && \text{(using the definition of } P_0 \cdot Q_0\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_{P_0} \wedge i \in \mathbb{O}_{Q_1} && \text{(using the definition of } Q_1\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_{P_0\cdot Q_1}. && \text{(using the definition of } P_0 \cdot Q_1\text{)}
\end{aligned}$$

Proving $P_1 \cdot Q_1 = P_1 \cdot Q_2$ Let us prove that $P_1 \cdot Q_1 = P_1 \cdot Q_2$. For all $i, j \in [d-1]$:

- Let us consider $\mathbb{O}$, $\mathbb{S}$, $\mathbb{B}$, $\textsc{length}_{m,b}$ and $\textsc{modulo}_m$. Since $Q_1 \overset{\mathbb{OSBM}}{\cong} Q_2$ and $\overset{\mathbb{OSBM}}{\cong}$ is a congruence relation, then $P_1 \cdot Q_1 \overset{\mathbb{OSBM}}{\cong} P_1 \cdot Q_2$.

- Let us consider $\mathbb{E}$.

$$\begin{aligned}
i\ \mathbb{E}_{P_1\cdot Q_1}\ j &= i\ \mathbb{E}_{P_1}\ j \wedge i\ \mathbb{E}_{Q_1}\ j && \text{(using the definition of } P_1 \cdot Q_1\text{)}\\
&= ((i \in L) \Longleftrightarrow (j \in L)) \wedge ((i \in G) \Longleftrightarrow (j \in G))\\
&\quad \wedge i\ \mathbb{E}_{P_1}\ j \wedge i\ \mathbb{E}_{Q_1}\ j && \text{(using hypothesis about } P_1\text{)}\\
&= i\ \mathbb{E}_{P_1}\ j \wedge i\ \mathbb{E}_{Q_2}\ j && \text{(using the definition of } Q_2\text{)}\\
&= i\ \mathbb{E}_{P_1\cdot Q_2}\ j. && \text{(using the definition of } P_1 \cdot Q_2\text{)}
\end{aligned}$$

- Finally, let us consider $\mathbb{L}$.

  Let us first suppose that $i \mathbb{L}_{P_1 \cdot Q_1} j$ and let us prove that $i \mathbb{L}_{P_1 \cdot Q_2} j$. Since $i \mathbb{L}_{P_1 \cdot Q_1} j$, either ($i \mathbb{L}_{P_1} j$ and $i \mathbb{E}_{Q_1} j$) or $i \mathbb{L}_{Q_1} j$. The two cases are considered separately.

  - Let us assume that $i \mathbb{L}_{P_1} j$ and $i \mathbb{E}_{Q_1} j$ hold. Since $i \mathbb{L}_{P_1} j$, either $i \mathbb{S}_{P_1} j$ or $i \mathbb{L}\overline{\mathbb{S}}_{P_1} j$, both cases are considered separately.
    * Let us suppose that $i \mathbb{S}_{P_1} j$, $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$. Since $i \mathbb{E}_{Q_1} j$, $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$, by definition of Q_2, $i \mathbb{E}_{Q_2} j$. Since $i \mathbb{L}_{P_1} j$ and since $i \mathbb{E}_{Q_2} j$, $i \mathbb{L}_{P_1 \cdot Q_2} j$.
    * Let us now suppose that $i \mathbb{L}\overline{\mathbb{S}}_{P_1} j$. Since $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ and since $i \mathbb{E}\wr\mathbb{S}_{P_1} j$ does not hold, $i \mathbb{E}\wr\mathbb{S}_{P_0} j$ does not hold. Since $i \mathbb{E}_{Q_1} j$ and $i \mathbb{E}\wr\mathbb{S}_{P_0} j$ does not hold, by definition of Q_1, $i, j \in L \cup G$. Two cases must be considered, depending on whether $i \in L$ or $i \in G$.
      · Let us first suppose that $i \in L$. Since $i \in L$ and (either $i \notin L$ or $j \notin G$) $j \notin G$. Since $j \in L \cup G$ and since $j \notin G$, $j \in L$. Since $i \mathbb{E}_{Q_1} j$, $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$, by definition of Q_2, $i \mathbb{E}_{Q_2} j$. Since $i \mathbb{L}_{P_1} j$ and since $i \mathbb{E}_{Q_2} j$, $i \mathbb{L}_{P_1 \cdot Q_2} j$.
      · Let us now suppose that $i \in G$. Two cases must be considered, depending on whether $j \in L$ or $j \in G$.
        ◦ Let us suppose that $j \in L$. Since $i \mathbb{E}_{Q_1} j$ and $i \in G$ and $j \in L$, by definition of Q_2, $i \mathbb{L}_{Q_2} j$, hence $i \mathbb{L}_{P_1 \cdot Q_2} j$.
        ◦ Let us suppose that $j \in G$. Since $i \mathbb{E}_{Q_1} j$ and $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$,, by definition of Q_2, $i \mathbb{E}_{Q_2} j$. Since $i \mathbb{L}_{P_1} j$ and since $i \mathbb{E}_{Q_2} j$, $i \mathbb{L}_{P_1 \cdot Q_2} j$.
  - Finally, let us assume that $i \mathbb{L}_{Q_1} j$ holds. By definition of Q_2, $i \mathbb{L}_{Q_2} j$ holds, hence $i \mathbb{L}_{P_1 \cdot Q_2} j$ holds.

  Let us now suppose that $i \mathbb{L}_{P_1 \cdot Q_2} j$ and let us prove that $i \mathbb{L}_{P_1 \cdot Q_1} j$. Since $i \mathbb{L}_{P_1 \cdot Q_2} j$, either ($i \mathbb{L}_{P_1} j$ and $i \mathbb{E}_{Q_2} j$) or $i \mathbb{L}_{Q_2} j$. The two cases are considered separately.

  - Let us first suppose that $i \mathbb{L}_{P_1} j$ and $i \mathbb{E}_{Q_2} j$. Since $i \mathbb{E}_{Q_2} j$, by definition of Q_2, $i \mathbb{E}_{Q_1} j$. Since $i \mathbb{L}_{P_1} j$ and since $i \mathbb{E}_{Q_1} j$, $i \mathbb{L}_{P_1 \cdot Q_1} j$.
  - Finally, let us suppose that $i \mathbb{L}_{Q_2} j$. By definition of Q_2, either $i \mathbb{L}_{Q_1} j$ or ($i \mathbb{E}_{Q_1} j$ and $i \in G$ and $j \in L$). The two cases are considered separately.
    * Let us first suppose that $i \mathbb{L}_{Q_1} j$ holds, then $i \mathbb{L}_{P_1 \cdot Q_1} j$ holds.
    * Let us now suppose that $i \mathbb{E}_{Q_1} j$ and $i \in G$ and $j \in L$ hold. Since $i \in G$ and $j \in L$, by hypothesis about P_1, then $i \mathbb{L}_{P_1} j$. Since $i \mathbb{L}_{P_1} j$ and since $i \mathbb{E}_{Q_1} j$, $i \mathbb{L}_{P_1 \cdot Q_1} j$.

Characterizing Q_2 in term of Q_0, P_0 and P_1 Before proving that $P_0 \cdot Q_2$ is equal to $O \cdot Q_0$ let us characterizes Q_2 in terms of Q_0, P_0 and P_1. By replacing Q_1 by its definition in the definition of Q_2, it is seen that, for all $i, j \in [d-1]$:

- $i \mathbb{S}_{Q_2} j$ if and only if $i \mathbb{S}_{Q_0} j$ and $i \in \mathbb{B}_{P_0}$ and $j \in \mathbb{O}_{P_0}$.
- $\textsc{position}_{\mathcal{V}'_t(m)}[Q_2](i) = \textsc{position}_{\mathcal{V}'_t(m)}[Q_0](i) \cap \textsc{position}_{\mathcal{V}'_t(m)}[P_0](i)$,
- $i \mathbb{E}_{Q_2} j$ if and only if $\{i \mathbb{E}_{Q_0} j$ and $[i \mathbb{E}\wr\mathbb{S}_{P_0} j$ or $i, j \in L \cup G]\}$ and $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$,

- $i\ \mathbb{L}_{Q_2}\ j$ if and only if $\{i\ \mathbb{L}_{Q_0}\ j$ or $[i\ \mathbb{E}_{Q_0}\ j, i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $(i \notin L$ or $j \notin G)]\}$ or $\{i\ \mathbb{E}_{Q_0}\ j$ and $[i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G]$ and $i \in G$ and $j \in L\}$ and
- $Q_2 \overset{\mathbb{M}}{\cong} Q_0$.

Let us first prove that $i\ \mathbb{E}_{Q_2}\ j$ is equivalent to ($i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$). Let us first assume that $i\ \mathbb{E}_{Q_2}\ j$ and let us prove that $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}_{P_0}\ j$. Since $i\ \mathbb{E}_{Q_2}\ j$, $i\ \mathbb{E}_{Q_0}\ j$ and $[i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G]$ and $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$. It remains to prove that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Two cases are considered, depending on whether $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G$ holds. The first case is trivial, let us suppose that $i, j \in L \cup G$. Two cases are considered, depending on whether $i \in L$ or $i \notin L$.

- Let us suppose that $i \in L$, since $(i \in L) \Longleftrightarrow (j \in L)$, $j \in L$. Since L is an $\mathbb{E}\wr\mathbb{S}_{P_0}$-classes, and since $i, j \in L$, $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$.
- Let us suppose that $i \notin L$. Since $i \in L \cup G$ and since $i \notin L$, $i \in G$. Since $(i \in J) \Longleftrightarrow (j \in J)$, $j \in G$. Since G is an $\mathbb{E}\wr\mathbb{S}_{P_0}$-classes and since $i, j \in G$, $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$.

Let us now suppose that $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}_{P_0}\ j$ and let us prove that $i\ \mathbb{E}_{Q_2}\ j$. Since $i\ \mathbb{E}_{P_0}\ j$, and L and G are $\mathbb{E}\wr\mathbb{S}_{P_0}$-classes, it follows that $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in J) \Longleftrightarrow (j \in J)$. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}_{P_0}\ j$ and $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in J) \Longleftrightarrow (j \in J)$, by the above characterization of Q_2, $i\ \mathbb{E}_{Q_2}\ j$ holds.

Since $i \in G$ and $j \in L$ implies $i, j \in L \cup G$, the preceding characterization of $i\ \mathbb{L}_{Q_2}\ j$ is equivalent to: $\{i\ \mathbb{L}_{Q_0}\ j$ or $[i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $(i \notin L$ or $j \notin G)$ and $i\ \mathbb{E}_{Q_0}\ j]$ or $(i\ \mathbb{E}_{Q_0}\ j$ and $i \in G$ and $j \in L)\}$.

Proving that $P_0 \cdot Q_2 = O \cdot Q_0$ Let us finally prove that $P_0 \cdot Q_2$ is equal to $O \cdot Q_0$. Let $i, j \in [d-1]$:

- Let us consider $\mathbb{O}$, the case $\mathbb{B}$ is similar.

$$\begin{array}{rll} i \in \mathbb{O}_{P_0 \cdot Q_2} & \Longleftrightarrow i \in \mathbb{O}_{P_0} \wedge i \in \mathbb{O}_{Q_2} & \text{(using the definition of } P_0 \cdot Q_2) \\ & \Longleftrightarrow i \in \mathbb{O}_{P_0} \wedge i \in \mathbb{O}_{Q_0} & \text{(using the definition of } Q_2) \\ & \Longleftrightarrow i \in \mathbb{O}_{P_0 \cdot Q_0}. & \text{(using the definition of } P_0 \cdot Q_0) \end{array}$$

- Let us consider $\mathbb{E}$:

$$\begin{array}{rll} i\ \mathbb{E}_{P_0 \cdot Q_2}\ j & \Longleftrightarrow i\ \mathbb{E}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_2}\ j & \text{(using the definition of } P_0 \cdot Q_2) \\ & \Longleftrightarrow i\ \mathbb{E}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_0}\ j \wedge i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j & \text{(using the characterization of } Q_2) \\ & \Longleftrightarrow i\ \mathbb{E}_{P_0}\ j \wedge i\ \mathbb{E}_{Q_0}\ j & (i\ \mathbb{E}_{P_0}\ j \Longrightarrow i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j) \\ & \Longleftrightarrow i\ \mathbb{E}_{O}\ j \wedge i\ \mathbb{E}_{Q_0}\ j & \left(O \overset{\mathbb{OESB}}{\cong} P_0\right) \\ & \Longleftrightarrow i\ \mathbb{E}_{O \cdot Q_0}\ j & \text{(using the definition of } O \cdot Q_0). \end{array}$$

- Let us consider $\mathbb{S}$:

$$\begin{array}{rll} i\ \mathbb{S}_{P_0 \cdot Q_2}\ j & \Longleftrightarrow (i\ \mathbb{S}_{P_0}\ j \quad \wedge i\ \mathbb{E}_{Q_2}\ j) \vee & \\ & \quad (j \in \mathbb{O}_{P_0} \quad \wedge i \in \mathbb{B}_{P_0} \wedge i\ \mathbb{S}_{Q_2}\ j) & \text{(using the definition of } P_0 \cdot Q_2) \\ & \Longleftrightarrow (i\ \mathbb{S}_{P_0}\ j \quad \wedge i\ \mathbb{E}_{Q_0}\ j) & \\ & \quad \vee (j \in \mathbb{O}_{P_0} \wedge i \in \mathbb{B}_{P_0} \wedge i\ \mathbb{S}_{Q_0}\ j\ ) & \text{(using the characterization of } Q_2) \\ & \Longleftrightarrow (i\ \mathbb{S}_{O}\ j \quad \wedge i\ \mathbb{E}_{Q_0}\ j) & \\ & \quad \vee (j \in \mathbb{O}_{O} \wedge i \in \mathbb{B}_{O} \wedge i\ \mathbb{S}_{Q_0}\ j\ ) & \text{(using the definition of } O) \\ & \Longleftrightarrow i\ \mathbb{S}_{O \cdot Q_0}\ j & \text{(using the definition of } O \cdot Q_0). \end{array}$$

- Let us now consider $\mathbb{L}$. Let us assume that $i\ \mathbb{L}_{P_0 \cdot Q_2}\ j$ and let us prove that $i\ \mathbb{L}_{O \cdot Q_0}\ j$. Since $i\ \mathbb{L}_{P_0 \cdot Q_2}\ j$, either ($i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_2}\ j$), or $i\ \mathbb{L}_{Q_2}\ j$. The two cases are considered separately.

– Let us first suppose that $i\ \mathbb{L}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_2}\ j$. Since $i\ \mathbb{E}_{Q_2}\ j$, by the above characterization of Q_2, $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{R}\mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $i\ \mathbb{R}\mathbb{S}_{P_0}\ j$, $i\ \mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{S}_{P_0}\ j$ and since $O \overset{\text{MOESB}}{\cong} P_0$, $i\ \mathbb{S}_O\ j$. Since $i\ \mathbb{S}_O\ j$ and since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{S}_{O\cdot Q_0}\ j$, hence $i\ \mathbb{L}_{O\cdot Q_0}\ j$.
– Let us now suppose that $i\ \mathbb{L}_{Q_2}\ j$. Since $i\ \mathbb{L}_{Q_2}\ j$, by the above characterization of Q_2, either $i\ \mathbb{L}_{Q_0}\ j$, either [$i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$)] or [$i\ \mathbb{E}_{Q_0}\ j$ and $i \in G$ and $j \in L$]. The three cases are considered separately.
  * If $i\ \mathbb{L}_{Q_0}\ j$ then $i\ \mathbb{L}_{O\cdot Q_0}\ j$.
  * Let us now suppose that $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$). Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$) by definition of O, $i\ \mathbb{L}_O\ j$. Since $i\ \mathbb{L}_O\ j$ and since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}_{O\cdot Q_0}\ j$.
  * Let us finally suppose that $i\ \mathbb{E}_{Q_0}\ j$ and $i \in G$ and $j \in L$. Since $i \in G$ and $j \in L$ by definition of O, $i\ \mathbb{L}_O\ j$. Since $i\ \mathbb{L}_O\ j$ and since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}_{O\cdot Q_0}\ j$.

Let us now suppose that $i\ \mathbb{L}_{O\cdot Q_0}\ j$, and let us prove that $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$. Since $i\ \mathbb{L}_{O\cdot Q_0}\ j$, either ($i\ \mathbb{L}_O\ j$ and $i\ \mathbb{E}_{Q_0}\ j$), or $i\ \mathbb{L}_{Q_0}\ j$. The two cases are considered separately.

– Let us first suppose that $i\ \mathbb{L}_O\ j$ and $i\ \mathbb{E}_{Q_0}\ j$. Since $i\ \mathbb{L}_O\ j$, by definition of O, either [$i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$)] or ($i \in G$ and $j \in L$). The two cases are considered separately.
  * Let us first suppose that $i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$). Since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$), by the above characterization of Q_2, $i\ \mathbb{L}_{Q_2}\ j$. Hence $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.
  * Let us now suppose that $i \in G$ and $j \in L$ hold. Since $i\ \mathbb{E}_{Q_0}\ j$ and $i \in G$ and $j \in L$, by the above characterization of Q_2, $i\ \mathbb{L}_{Q_2}\ j$, hence $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.
– Let us finally suppose that $i\ \mathbb{L}_{Q_0}\ j$, then by definition of Q_2, $i\ \mathbb{L}_{Q_2}\ j$, and then $i\ \mathbb{L}_{P_0\cdot Q_2}\ j$.

- Let us consider $\mathbb{M}$. Since $P_0 \overset{\mathbb{M}}{\cong} O$ and $Q_0 \overset{\mathbb{M}}{\cong} Q_2$ and since $\overset{\mathbb{M}}{\cong}$ is a congruence relation, then $O \cdot Q_0 \overset{\mathbb{M}}{\cong} P_0 \cdot Q_2$.

Proving $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. It remains to prove that O belongs to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota}$ and Q_1 and Q_2 belong to $\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$. Let us now first that $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

- Since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $O \overset{\text{MOESB}}{\cong} P_0$, by Lemma 8.1.15, O satisfies Axioms (1 - $\mathbb{E}$ equivalence), (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$), (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible) (5 - $\mathbb{S}$ not cyclic), (6 - $\text{POSITION}_{\mathcal{V}_\iota'(m)}$ and $\mathbb{E}$ compatible), (7 - $\text{POSITION}_{\mathcal{V}_\iota'(m)}$ and $\mathbb{S}$ compatible), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod), (19 - Rigid case) and (20 - ν), and $O \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.
- Let us consider Axiom (8 - $\mathbb{L}$ asymmetric). Let us assume that $i\ \mathbb{L}_O\ j$ and let us prove that $j\ \mathbb{L}_O\ i$ does not hold. Since $i\ \mathbb{L}_O\ j$, by definition of O, either [$i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$)] or ($i \in G$ and $j \in L$). The two cases are considered separately.
  – Let us suppose that $i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$). Since $i\ \mathbb{L}_{P_0}\ j$, $j\ \mathbb{L}_{P_0}\ i$ does not hold. Since (either $i \notin L$ or $j \notin G$), ($i \in L$ and $j \in G$) does not hold. Since neither $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$ nor ($i \in L$ and $j \in G$) hold, by definition of O, $j\ \mathbb{L}_O\ i$ does not hold.
  – Let us suppose that $i \in G$ and $j \in L$. Since $L \cap G = \emptyset$ since and $i \in G$, $i \notin L$. Since $j \in L$ and since $L \cap G = \emptyset$, $j \notin G$. Since $i \in G$ and since $j \in L$, ($i \notin G$ and $j \notin L$) does not hold. Hence neither (either $j \notin L$ or $i \notin G$) nor ($j \in G$ and $i \in L$) hold, hence, by definition of O, $j\ \mathbb{L}_O\ i$ does not hold.

- Let us consider Axiom (9 - $\mathbb{L}$ transitive). Let us assume that $i\ \mathbb{L}_O\ j$ and that $j\ \mathbb{L}_O\ k$ and let us prove that $i\ \mathbb{L}_O\ k$. Since $i\ \mathbb{L}_O\ j$, by definition of O, either [$i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$)] or ($i \in G$ and $j \in L$). The two cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$). Since $j\ \mathbb{L}_O\ k$, either ($j\ \mathbb{L}_{P_0}\ k$ and (either $j \notin L$ or $k \notin G$)) or ($j \in G$ and $k \in L$). The two cases are considered separately.
    - Let us suppose that $j\ \mathbb{L}_{P_0}\ k$ and (either $j \notin L$ or $k \notin G$). Since $i\ \mathbb{L}_{P_0}\ j$ and since $j\ \mathbb{L}_{P_0}\ k$, $i\ \mathbb{L}_{P_0}\ k$. Let us claim that (either $i \notin L$ or $k \notin G$). Since and $i\ \mathbb{L}_{P_0}\ k$ (either $i \notin L$ or $k \notin G$) by definition of O it implies $i\ \mathbb{L}_O\ k$.
      Let us now prove that (either $i \notin L$ or $k \notin G$), for the sake of the contradiction, let us assume that $i \in L$ and $k \in G$. Since (either $i \notin L$ or $j \notin G$) and since $i \in L$, $j \notin G$. Since (either $j \notin L$ or $k \notin G$) and since $k \in G$, $j \notin L$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $i \in L$, $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and since $j \notin L$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $j \notin G$, by condition (2), $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $j\ \mathbb{L}_{P_0}\ k$ and since $k \in G$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$. Having both $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ is a contradiction.
    - Let us suppose that $j \in G$ and $k \in L$. Since (either $i \notin L$ or $j \notin G$) and since $j \in G$, $i \notin L$. Since $i\ \mathbb{L}_{P_0}\ j$ and since $j \in G$, $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$. Two cases must be considered, depending on whether $i \in G$ or not.
      - Let us suppose that $i \in G$. Since $i \in G$ and $k \in L$, by definition of O, $i\ \mathbb{L}_O\ k$.
      - Let us suppose that $i \notin G$. Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and since $i \notin G$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ and since $i \notin L$, by Condition (2), $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ L$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ L$ and since $k \in L$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and $i \notin L$, by definition of O, $i\ \mathbb{L}_O\ k$.
  - Let us suppose that $i \in G$ and $j \in L$. Since $j\ \mathbb{L}_O\ k$, by definition of O, either [$j\ \mathbb{L}_{P_0}\ k$ and (either $j \notin L$ or $k \notin G$)] or ($j \in G$ and $k \in L$). The two cases are considered separately.
    - Let us suppose that $j\ \mathbb{L}_{P_0}\ k$ and (either $j \notin L$ or $k \notin G$). Since $j\ \mathbb{L}_{P_0}\ k$ and since $j \in L$, $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Two cases must be considered, depending on whether $k \in L$ or not.
      - Let us suppose that $k \in L$. Since $k \in L$ and $i \in G$, by definition of O, $i\ \mathbb{L}_O\ k$.
      - Let us suppose that $k \notin L$. Since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$, and since $k \notin L$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and $k \notin G$, by Condition (2), $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and since $i \in G$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and since $k \notin G$, by definition of O, $i\ \mathbb{L}_O\ k$.
    - Let us suppose that $j \in G$ and $k \in L$. Since $j \in L$ and $j \in G$ and $L \cap G = \emptyset$, it is a contradiction.

- The element O easily satisfies Axioms (10 - $i\ \mathbb{E}_T\ j$,$i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$), (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible), (12 - $\textsc{position}_{\mathcal{V}_i'(m)}$ and $\mathbb{L}$ compatible), and (13 - $\mathbb{S}$ implies $\mathbb{L}$) since O is similar to P_0, apart on L and G which are two $\mathbb{E}_{P_0}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}$-classes.

- Let us consider Axiom (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$). Let us assume that $i\ \mathbb{S}_O\ j$ and $i\ \mathbb{L}_O\ k$ and let us prove that either $i\ \mathbb{E}_O\ k$ or $i\ \mathbb{L}_O\ k$. Since $i\ \mathbb{S}_O\ j$, by definition of O, $i\ \mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{L}_O\ k$, by definition of O, [$i\ \mathbb{L}_{P_0}\ k$ and (either $i \notin L$ or $k \notin G$)] or ($i \in G$ and $k \in L$). Both cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{P_0}\ k$ and (either $i \notin L$ or $k \notin G$). Since $i\ \mathbb{L}_{P_0}\ k$ and $i\ \mathbb{S}_{P_0}\ j$, either $j\ \mathbb{E}_{P_0}\ k$ or $j\ \mathbb{L}_{P_0}\ k$. Two cases are considered separately.
    - If $j\ \mathbb{E}_{P_0}\ k$ then $j\ \mathbb{E}_O\ k$.
    - Let us suppose that $j\ \mathbb{L}_{P_0}\ k$. Two cases must be considered depending on whether $i \notin L$ or $k \notin G$.

· If $k \notin G$, since $j\ \mathbb{L}_{P_0}\ k$, $j\ \mathbb{L}_O\ k$.

· Let us assume that $i \notin L$. Since $i \notin L$ and since $i\ \mathbb{S}_{P_0}\ j$, $j \notin L$. Since $j \notin L$ and $j\ \mathbb{L}_{P_0}\ k$ by definition of O, $j\ \mathbb{L}_O\ k$.

– Let us suppose that $i \in G$ and $k \in L$. Since $i \in G$ and $i\ \mathbb{S}_{P_0}\ j$, since G is an $\mathbb{E}\wr\mathbb{S}_{P_0}$-class, $j \in G$. Since $j \in G$ and $k \in L$, by definition of O, $j\ \mathbb{L}_O\ k$.

$Q_1 \in \mathbb{POP}^m_{\nu,\mathcal{V}'_t}$ Let us prove that $Q_1 \in \mathbb{POP}^m_{\nu,\mathcal{V}'_t}$. Let $i,j,k \in [d-1]$ such that $i \in \nu \Longleftrightarrow j \in \nu \Longleftrightarrow k \in \nu$.

- Let us consider Axiom (1 - $\mathbb{E}$ equivalence). Since $i\ \mathbb{E}_{Q_0}\ i$ and $i\ \mathbb{E}_{P_0}\ i$, by definition of Q_1, $i\ \mathbb{E}_{Q_1}\ i$. Let us assume that $i\ \mathbb{E}_{Q_0}\ j$, by symmetry of the definition $j\ \mathbb{E}_{Q_0}\ i$ clearly holds. Let us suppose that $j\ \mathbb{E}_{Q_0}\ k$ and let us prove that $i\ \mathbb{E}_{Q_0}\ k$. Since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $j\ \mathbb{E}_{Q_0}\ k$ it follows that $j\ \mathbb{E}_{Q_0}\ k$ and $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $i\ \mathbb{E}_{Q_0}\ j$ and it follows that $j\ \mathbb{E}_{Q_0}\ k$, $i\ \mathbb{E}_{Q_0}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $j\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_t}$ it follows that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $i\ \mathbb{E}_{Q_0}\ k$ and $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ k$, by definition of Q_1, $i\ \mathbb{E}_{Q_1}\ k$.

- Let us consider Axiom (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$). Let us assume that ($i\ \mathbb{S}_{Q_1}\ j$ and $i\ \mathbb{S}_{Q_1}\ k$) and let us prove that $j\ \mathbb{E}_{Q_1}\ k$. Since $i\ \mathbb{S}_{Q_1}\ j$, $i\ \mathbb{S}_{Q_0}\ j$ and $i \in \mathbb{B}_{P_0}$ and $j \in \mathbb{O}_{P_0}$. Similarly $i\ \mathbb{S}_{Q_0}\ k$ and $k \in \mathbb{O}_{P_0}$. Since $j \in \mathbb{O}_{P_0}$ and $k \in \mathbb{O}_{P_0}$ and $(j \in \nu) \Longleftrightarrow (k \in \nu)$, it follows that $j\ \mathbb{E}_{P_0}\ k$. Since $i\ \mathbb{S}_{Q_0}\ j$ and since $i\ \mathbb{S}_{Q_0}\ k$, $j\ \mathbb{E}_{Q_0}\ k$. Since $i\ \mathbb{E}_{P_0}\ j$ and $j\ \mathbb{E}_{Q_0}\ k$ by definition of Q_1, $i\ \mathbb{E}_{Q_0}\ k$.

- Since $Q_0 \in \mathbb{POP}^m_{\nu,\mathcal{V}'_t}$, $Q_1 \overset{\text{OESBL}}{\preccurlyeq} Q_0$, $Q_1 \overset{\text{M}}{\cong} Q_0$ and $\mathbb{L}_{Q_1} \supseteq \mathbb{L}_{Q_0}$, by Lemma 8.1.15, Q_1 satisfies Axioms (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (7 - $\text{POSITION}_{\mathcal{V}'_t(m)}$ and $\mathbb{S}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod), (19 - Rigid case) and (20 - ν).

- Let us consider Axiom (6 - $\text{POSITION}_{\mathcal{V}'_t(m)}$ and $\mathbb{E}$ compatible). Let us suppose that ($i,j \in \mathbb{O}_{Q_1}$ or $i,j \in \mathbb{B}_{Q_1}$), let us prove that $i\ \mathbb{E}_{Q_1}\ j$. Let us suppose that $i,j \in \mathbb{O}_{Q_1}$, the other case is similar. Since $i,j \in \mathbb{O}_{Q_1}$ it follows that $i,j \in \mathbb{O}_{P_0}$ and $i,j \in \mathbb{O}_{Q_0}$, hence $i\ \mathbb{E}_{P_0}\ j$ and $i\ \mathbb{E}_{Q_0}\ j$, and then $i\ \mathbb{E}_{Q_1}\ j$.

- Let us consider Axiom (8 - $\mathbb{L}$ asymmetric). Let us assume that $i\ \mathbb{L}_{Q_1}\ j$ and let us prove that $j\ \mathbb{L}_{Q_1}\ i$ does not hold. Since $i\ \mathbb{L}_{Q_1}\ j$, by definition of Q_1, $i\ \mathbb{L}_{Q_0}\ j$ or [$i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$)]. The two cases are considered separately.

  – Let us suppose that $i\ \mathbb{L}_{Q_0}\ j$. Since $i\ \mathbb{L}_{Q_0}\ j$, neither $j\ \mathbb{L}_{Q_0}\ i$ nor $j\ \mathbb{E}_{Q_0}\ i$ hold, hence, by definition of Q_1, $j\ \mathbb{L}_{Q_1}\ i$ does not hold.

  – Let us assume that $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$). Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ holds, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$ does not hold. Since $i\ \mathbb{E}_{Q_0}\ j$, $j\ \mathbb{L}_{Q_0}\ i$ does not hold. Since neither $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$ nor $j\ \mathbb{L}_{Q_0}\ i$ hold, by definition of Q_1, $j\ \mathbb{L}_{P_0}\ i$ does not hold.

- Let us consider Axiom (9 - $\mathbb{L}$ transitive). Let us assume that $i\ \mathbb{L}_{Q_1}\ j$ and that $j\ \mathbb{L}_{Q_1}\ k$ and let us prove that $i\ \mathbb{L}_{Q_1}\ k$. Since $i\ \mathbb{L}_{Q_1}\ j$, by definition of Q_1, $i\ \mathbb{L}_{Q_0}\ j$ or [$i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$)]. The two cases are considered separately.

  – Let us suppose that $i\ \mathbb{L}_{Q_0}\ j$. let us claim that $i\ \mathbb{L}_{Q_0}\ k$, by definition of Q_1, it implies $i\ \mathbb{L}_{Q_1}\ k$. Let us prove that $i\ \mathbb{L}_{Q_0}\ k$.

    Since $j\ \mathbb{L}_{Q_1}\ k$, either $j\ \mathbb{L}_{Q_0}\ k$ or [$j\ \mathbb{E}_{Q_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($j \notin L$ or $k \notin G$)]. The two cases are considered separately.

    * Let us suppose that $j\ \mathbb{L}_{Q_0}\ k$. Since $i\ \mathbb{L}_{Q_0}\ j$ and since $j\ \mathbb{L}_{Q_0}\ k$, $i\ \mathbb{L}_{Q_0}\ k$.

    * Let us suppose that $j\ \mathbb{E}_{Q_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($j \notin L$ or $k \notin G$). Since $i\ \mathbb{L}_{Q_0}\ j$ and since $j\ \mathbb{E}_{Q_0}\ k$, $i\ \mathbb{L}_{Q_0}\ k$.

– Let us assume that $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$). Since $j\ \mathbb{L}_{Q_1}\ k$, either $j\ \mathbb{L}_{Q_0}\ k$ or ($j\ \mathbb{E}_{Q_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($j \notin L$ or $k \notin G$)). The two cases are considered separately.

  * Let us suppose that $j\ \mathbb{L}_{Q_0}\ k$. Since $i\ \mathbb{E}_{Q_0}\ j$ and since $j\ \mathbb{L}_{Q_0}\ k$, $i\ \mathbb{L}_{Q_0}\ k$. Since $i\ \mathbb{L}_{Q_0}\ k$, by definition of Q_1, it implies $i\ \mathbb{L}_{Q_1}\ k$.
  * Let us suppose that $j\ \mathbb{E}_{Q_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($j \notin L$ or $k \notin G$). Since $i\ \mathbb{E}_{Q_0}\ j$ and since $j\ \mathbb{E}_{Q_0}\ k$, $i\ \mathbb{E}_{Q_0}\ k$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Let us claim that ($i \notin L$ or $k \notin G$). Since $i\ \mathbb{E}_{Q_0}\ k$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($i \notin L$ or $k \notin G$), by definition of Q_1, $i\ \mathbb{L}_{Q_1}\ k$.
    Let us prove that ($i \notin L$ or $k \notin G$). For the sake of contradiction, let us assume that $i \in L$ and $k \in G$. Since $i \in L$ and ($i \notin L$ or $j \notin G$) $j \notin G$. Since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and since $i \in L$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and $k \in G$, by Condition (2), $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ and $G\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$, it is a contradiction.

- Let us consider Axiom (10 - $i\ \mathbb{E}_T\ j$,$i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$). Let us suppose that $i\ \mathbb{E}_{Q_1}\ j$ and $i\ \mathbb{L}_{Q_1}\ k$ hold and let us prove that $j\ \mathbb{L}_{Q_1}\ k$ holds. Since $i\ \mathbb{E}_{Q_1}\ j$ by definition of Q_1, $i\ \mathbb{E}_{Q_0}\ j$ and [$i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G$]. Since $i\ \mathbb{L}_{Q_1}\ k$, by definition of Q_1, either $i\ \mathbb{L}_{Q_0}\ k$ or [$i\ \mathbb{E}_{Q_0}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($i \notin L$ or $k \notin G$)], both cases are considered separately.

  – Let us suppose that $i\ \mathbb{L}_{Q_0}\ k$. Since $i\ \mathbb{L}_{Q_0}\ j$ and $j\ \mathbb{E}_{Q_1}\ k$ then $i\ \mathbb{L}_{Q_0}\ k$, by definition of Q_1, it implies $i\ \mathbb{L}_{Q_1}\ j$.
  – Let us suppose that $i\ \mathbb{E}_{Q_0}\ k$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and ($i \notin L$ or $k \notin G$). Having $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{E}_{Q_0}\ k$ implies $j\ \mathbb{E}_{Q_0}\ k$. Two cases must be considered, depending on whether $i \notin L$ or $k \notin G$.
    * Let us suppose that $i \notin L$. Two cases must be considered, depending on whether $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G$.
      · Let us suppose that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$, since $i \notin L$ and since L is a $\mathbb{E}\wr\mathbb{S}_{P_0}$-class, $j \notin L$. Since $j\ \mathbb{E}_{Q_0}\ k$, since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and since $j \notin L$, by definition of Q_1, $j\ \mathbb{L}_{Q_1}\ k$
      · Let us suppose that $i, j \in L \cup G$. Since $i \notin L$ and since $i \in L \cup G$, $i \in G$. Since $i \in G$ and since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $k \notin G$. Since $j \in L \cup G$ and $i \in G$, $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ i$ and since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $j\ \mathbb{E}_{Q_0}\ k$, since $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and since $k \notin G$, by definition of Q_1, $j\ \mathbb{L}_{Q_1}\ k$.
    * Let us suppose that $k \notin G$ and that $i \in L$. Since $i \in L$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, by hypothesis about P_0, $G\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $G\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and since $k \notin G$, $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.
      Let us prove that $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, since $k \notin G$ and since $j\ \mathbb{E}_{Q_0}\ k$, by definition of Q_1, it implies $i\ \mathbb{L}_{Q_1}\ j$. Two cases must be considered, depending on whether $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G$.
      · Let us suppose that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and since $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$, since $i \in L$ and since L is a $\mathbb{E}\wr\mathbb{S}_{P_0}$-class, $j \in L$. Since $j \in L$ and $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ then $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.
      · Let us suppose that $i, j \in L \cup G$. Since $j \in L \cup G$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$. Since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and since $G\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $j\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$.

- let us consider Axiom (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible). For the sake of contradiction, let us suppose that $i\ \mathbb{E}_{Q_1}\ j$ and $i\ \mathbb{L}_{Q_1}\ j$ hold. Since $i\ \mathbb{E}_{Q_1}\ j$ it follows that $i\ \mathbb{E}_{Q_0}\ j$ and [$i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or $i, j \in L \cup G$]. Since $i\ \mathbb{L}_{Q_1}\ j$ and since $i\ \mathbb{E}_{Q_0}\ j$, $i\ \mathbb{E}_{Q_0}\ j$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and ($i \notin L$ or $j \notin G$). Note that $i\ \mathbb{E}\wr\mathbb{S}_{P_0}\ j$ contradicts $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and that $i, j \in L \cup G$ contradicts ($i \notin L$ or $j \notin G$), hence it is a contradiction.

- Let us consider Axiom (12 - $\textsc{position}_{\mathcal{V}'_t(m)}$ and $\mathbb{L}$ compatible). Let us assume that [($i \in \mathbb{O}_{Q_1}$ and $j \notin \mathbb{O}_{Q_1}$) or ($i \notin \mathbb{B}_{Q_1}$ and $j \in \mathbb{B}_{Q_1}$)] and that $\mathbb{L}$ belongs to $I^2_{\mathcal{V}'_t}$. Let us prove that $i\ \mathbb{L}_{Q_1}\ j$.

Let us consider the case ($i \in \mathbb{O}_{Q_1}$ and $j \notin \mathbb{O}_{Q_1}$), the other one is similar. Since $i \in \mathbb{O}_{Q_1}$, by definition of Q_1, $i \in \mathbb{O}_{Q_0}$ and $i \in \mathbb{O}_{P_0}$. Two cases are considered separately, depending on whether $j \in \mathbb{O}_{Q_0}$ holds or not.

- Let us suppose that $j \in \mathbb{O}_{Q_0}$. Since $j \in \mathbb{O}_{Q_0}$ and $j \notin \mathbb{O}_{Q_1}$, by definition of Q_1, $j \notin \mathbb{O}_{P_0}$. Since $j \in \mathbb{O}_{Q_0}$ and since $i \in \mathbb{O}_{Q_0}$, $i \; \mathbb{E}_{Q_0} \; j$. Since $i \in \mathbb{O}_{P_0}$ and since $j \notin \mathbb{O}_{P_0}$, $i \; \mathbb{L}\overline{\mathbb{S}}_{P_0} \; j$. Since L is an $\mathbb{E}\wr\mathbb{S}_{P_0}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}$-class and since $i \in \mathbb{O}_{P_0}$, $i \notin L$. Since $i \; \mathbb{E}_{Q_0} \; j$ and $i \; \mathbb{L}\overline{\mathbb{S}}_{P_0} \; j$ and $i \notin L$, by definition of Q_1, $i \; \mathbb{L}_{Q_1} \; j$.
- Let us suppose that $j \notin \mathbb{O}_{Q_0}$. Since $i \in \mathbb{O}_{Q_0}$ and since $j \notin \mathbb{O}_{Q_0}$ $i \; \mathbb{L}_{Q_0} \; j$. Since $i \; \mathbb{L}_{Q_0} \; j$, by definition of Q_1, $i \; \mathbb{L}_{Q_1} \; j$.

- Let us consider Axiom (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$). Let us assume that $i \; \mathbb{S}_{Q_1} \; j$ and $i \; \mathbb{L}_{Q_1} \; k$ and let us prove that either $i \; \mathbb{E}_{Q_1} \; k$ or $i \; \mathbb{L}_{Q_1} \; k$. Since $i \; \mathbb{S}_{Q_1} \; j$ it follows that $i \; \mathbb{S}_{Q_0} \; j$ and $i \in \mathbb{B}_{P_0}$ and $j \in \mathbb{O}_{P_0}$. Since $i \; \mathbb{L}_{Q_1} \; k$, $i \; \mathbb{L}_{Q_0} \; k$ or [$i \; \mathbb{E}_{Q_0} \; k$ and $i \; \mathbb{L}\overline{\mathbb{S}}_{P_0} \; k$ and ($i \notin L$ or $k \notin G$)]. Both cases are considered separately.
  - Let us suppose that $i \; \mathbb{L}_{Q_0} \; k$. Since $i \; \mathbb{L}_{Q_0} \; k$ and $i \; \mathbb{S}_{Q_0} \; j$, it follows that either $j \; \mathbb{E}_{Q_0} \; k$ or $j \; \mathbb{L}_{Q_0} \; k$, both cases are considered separately.
    - Let us suppose that $j \; \mathbb{E}_{Q_0} \; k$. Since $j \in \mathbb{O}_{P_0}$, either $j \; \mathbb{E}_{P_0} \; k$ or $j \; \mathbb{L}_{P_0} \; k$, both cases are considered separately.
      - If $j \; \mathbb{E}_{P_0} \; k$ since $j \; \mathbb{E}_{Q_0} \; k$ by definition of Q_1, $j \; \mathbb{E}_{Q_1} \; k$.
      - Let us suppose that $j \; \mathbb{L}_{P_0} \; k$. Since $j \in \mathbb{O}_{P_0}$ and G is an $\mathbb{E}\wr\mathbb{S}_{P_0}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}$-class, then $j \notin G$. Since $j \; \mathbb{E}_{Q_0} \; k$, $j \; \mathbb{L}_{P_0} \; k$ and $j \notin G$, by definition of Q_1, $j \; \mathbb{L}_{Q_1} \; k$.
    - If $j \; \mathbb{L}_{Q_0} \; k$, by definition of Q_1, $j \; \mathbb{L}_{Q_1} \; k$.
  - Let us suppose that $i \; \mathbb{E}_{Q_0} \; k$ and $i \; \mathbb{L}\overline{\mathbb{S}}_{P_0} \; k$ and ($i \notin L$ or $k \notin G$). Note that $i \in \mathbb{B}_{P_0}$ and $i \; \mathbb{L}\overline{\mathbb{S}}_{P_0} \; k$ is a contradiction.

$Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$ Let us prove that $Q_2 \in \mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$.

- Let us consider Axiom (1 - $\mathbb{E}$ equivalence). Since $\mathbb{E}_{Q_2}$ is the intersection of the equivalence relations $\mathbb{E}_{Q_1}$, belonging to L and belonging to G, then $\mathbb{E}_{Q_2}$ is an equivalence relation.

- Since $Q_2 \overset{\mathbb{OSBM}}{\cong} Q_1$, $Q_2 \overset{\mathbb{EL}}{\preccurlyeq} Q_1$, $\mathbb{L}_{Q_1} \subseteq \mathbb{L}_{Q_2}$, by Lemma 8.1.15, Q_2 satisfies Axioms (2 - $i \; \mathbb{S}_T \; j \wedge i \; \mathbb{S}_T \; k \Longrightarrow j \; \mathbb{E}_T \; k$), (3 - $i \; \mathbb{S}_T \; j \wedge i \; \mathbb{E}_T \; k \Longrightarrow j \; \mathbb{S}_T \; k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (7 - $\textsc{position}_{\mathcal{V}_\iota'(m)}$ and $\mathbb{S}$ compatible), (12 - $\textsc{position}_{\mathcal{V}_\iota'(m)}$ and $\mathbb{L}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod), (19 - Rigid case) and (20 - ν).

- The element Q_2 easily satisfies (6 - $\textsc{position}_{\mathcal{V}_\iota'(m)}$ and $\mathbb{E}$ compatible) since Q_1 satisfies these axioms, and that Q_2 is similar to Q_1 apart on some $\mathbb{E}_{Q_1}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}$-classes.

- Let us consider Axiom (8 - $\mathbb{L}$ asymmetric). Let us assume that $i \; \mathbb{L}_{Q_2} \; j$ and let us prove that $j \; \mathbb{L}_{Q_2} \; i$ does not hold. Since $i \; \mathbb{L}_{Q_2} \; j$, by definition of Q_2, either $i \; \mathbb{L}_{Q_1} \; j$ or ($i \; \mathbb{E}_{Q_1} \; j$ and $i \in G$ and $j \in L$) hold. The two cases are considered separately.
  - Let us suppose that $i \; \mathbb{L}_{Q_1} \; j$. Since $i \; \mathbb{L}_{Q_1} \; j$, neither $j \; \mathbb{L}_{Q_1} \; i$ nor $j \; \mathbb{E}_{Q_1} \; i$ hold, hence, by definition of Q_2, $j \; \mathbb{L}_{Q_2} \; i$ does not hold.
  - Let us assume that $i \; \mathbb{E}_{Q_1} \; j$ and $i \in G$ and $j \in L$. Since $i \; \mathbb{E}_{Q_1} \; j$, $j \; \mathbb{L}_{Q_1} \; i$ does not hold. Since $j \in L$ and since $L \cap G = \emptyset$, $j \notin G$. Since neither $j \; \mathbb{L}_{Q_1} \; i$ nor $j \in G$, by definition of Q_2, $j \; \mathbb{L}_{P_0} \; i$ does not hold.

- Let us consider Axiom (9 - $\mathbb{L}$ transitive). Let us assume that $i\ \mathbb{L}_{Q_2}\ j$ and that $j\ \mathbb{L}_{Q_2}\ k$ and let us prove that $i\ \mathbb{L}_{Q_2}\ k$. Since $i\ \mathbb{L}_{Q_2}\ j$, by definition of Q_2, $i\ \mathbb{L}_{Q_1}\ j$ or ($i\ \mathbb{E}_{Q_1}\ j$ and $i \in G$ and $j \in L$) hold. The two cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{Q_1}\ j$. It is claimed that $i\ \mathbb{L}_{Q_1}\ k$, by definition of Q_2, it implies $i\ \mathbb{L}_{Q_2}\ k$. Let us prove that $i\ \mathbb{L}_{Q_1}\ k$. Since $j\ \mathbb{L}_{Q_2}\ k$, either $j\ \mathbb{L}_{Q_1}\ k$ or ($j\ \mathbb{E}_{Q_1}\ k$ and $j \in G$ and $k \in L$). The two cases are considered separately.
    - Let us suppose that $j\ \mathbb{L}_{Q_1}\ k$. Since $i\ \mathbb{L}_{Q_1}\ j$ and since $j\ \mathbb{L}_{Q_1}\ k$, $i\ \mathbb{L}_{Q_1}\ k$.
    - Let us suppose that $j\ \mathbb{E}_{Q_1}\ k$ and $j \in G$ and $k \in L$. Since $i\ \mathbb{L}_{Q_1}\ j$ and since $j\ \mathbb{E}_{Q_1}\ k$, $i\ \mathbb{L}_{Q_1}\ k$.
  - Let us assume that $i\ \mathbb{E}_{Q_1}\ j$ and $i \in G$ and $j \in L$. Since $j\ \mathbb{L}_{Q_2}\ k$, either $j\ \mathbb{L}_{Q_1}\ k$ or ($j\ \mathbb{E}_{Q_1}\ k$ and $j \in G$ and $k \in L$). The two cases are considered separately.
    - Let us suppose that $j\ \mathbb{L}_{Q_1}\ k$. Since $i\ \mathbb{E}_{Q_1}\ j$ and since $j\ \mathbb{L}_{Q_1}\ k$ $i\ \mathbb{L}_{Q_1}\ k$. Since $i\ \mathbb{L}_{Q_1}\ k$, by definition of Q_2, it implies $i\ \mathbb{L}_{Q_2}\ k$.
    - Let us suppose that $j\ \mathbb{E}_{Q_1}\ k$ and $j \in G$ and $k \in L$. Since $j \in L$ and $j \in G$ and $L \cap G = \emptyset$, there is a contradiction.

- Let us consider Axiom (10 - $i\ \mathbb{E}_T\ j$,$i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$). Let us suppose that $i\ \mathbb{E}_{Q_2}\ j$ and $i\ \mathbb{L}_{Q_2}\ k$ hold and let us prove that $j\ \mathbb{L}_{Q_2}\ k$ holds. Since $i\ \mathbb{E}_{Q_2}\ j$, by definition of Q_2, $i\ \mathbb{E}_{Q_1}\ j$ and $(i \in L) \Longleftrightarrow (j \in L)$ and $(i \in G) \Longleftrightarrow (j \in G)$. Since $i\ \mathbb{L}_{Q_2}\ k$, by definition of Q_2, $i\ \mathbb{L}_{Q_1}\ k$ or ($i\ \mathbb{E}_{Q_1}\ k$ and $i \in G$ and $k \in L$), both cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{Q_1}\ k$. Since $i\ \mathbb{L}_{Q_1}\ k$ and since $i\ \mathbb{E}_{Q_1}\ j$, $j\ \mathbb{L}_{Q_1}\ k$, by definition of Q_2 it implies $j\ \mathbb{L}_{Q_2}\ k$.
  - Let us suppose that $i\ \mathbb{E}_{Q_1}\ k$ and $i \in G$ and $k \in L$. Since $i\ \mathbb{E}_{Q_1}\ j$ and since $j\ \mathbb{E}_{Q_1}\ k$, $j\ \mathbb{E}_{Q_1}\ k$. Since $i \in G$ and since $(i \in G) \Longleftrightarrow (j \in G)$, $j \in G$. Since $j\ \mathbb{E}_{Q_1}\ k$, $j \in G$, $k \in L$ by definition of Q_2 it implies $j\ \mathbb{E}_{Q_2}\ k$.

- let us consider Axiom (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible). Let us suppose that $i\ \mathbb{L}_{Q_2}\ j$ holds. Since $i\ \mathbb{L}_{Q_2}\ j$ by definition of Q_2, $i\ \mathbb{L}_{Q_1}\ j$ or ($i\ \mathbb{E}_{Q_1}\ j$ and $i \in G$ and $j \in L$), both cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{Q_1}\ j$ then $i\ \mathbb{E}_{Q_1}\ j$ does not hold.
  - Since $i \in G$ and since $L \cap G = \emptyset$, $i \notin G$. Since $i \in G$ and since $i \notin G$, $(i \in L) \Longleftrightarrow (j \in L)$ does not hold.

  In both case, by definition of Q_2, $i\ \mathbb{E}_{Q_2}\ j$ does not hold.

- Let us consider Axiom (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$). Let us suppose that $i\ \mathbb{S}_{Q_2}\ j$ and $i\ \mathbb{L}_{Q_2}\ k$ hold and let us prove that $j\ \mathbb{L}_{Q_2}\ k$ or $j\ \mathbb{E}_{Q_1}\ k$ hold. Since $i\ \mathbb{S}_{Q_2}\ j$, by definition of Q_2, $i\ \mathbb{S}_{Q_1}\ j$. Since $i\ \mathbb{L}_{Q_2}\ k$, by definition of Q_2, $i\ \mathbb{L}_{Q_1}\ k$ or ($i\ \mathbb{E}_{Q_1}\ k$ and $i \in G$ and $k \in L$), both cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{Q_1}\ k$. Since $i\ \mathbb{L}_{Q_1}\ k$ and $j\ \mathbb{E}_{Q_1}\ k$, either $j\ \mathbb{E}_{Q_1}\ k$ or $j\ \mathbb{L}_{Q_1}\ k$, both cases are considered separately.
    - Let us suppose that $j\ \mathbb{E}_{Q_1}\ k$, by definition of Q_2 it implies $j\ \mathbb{E}_{Q_2}\ k$.
    - Let us suppose that $j\ \mathbb{L}_{Q_1}\ k$, by definition of Q_2 it implies $j\ \mathbb{L}_{Q_2}\ k$.
  - Let us suppose that $i\ \mathbb{E}_{Q_1}\ k$ and $i \in G$ and $k \in L$. Since $i\ \mathbb{E}_{Q_1}\ k$, by definition of Q_2 it implies $j\ \mathbb{E}_{Q_2}\ k$.

□

Another lemma is needed, to reduce Lemma 8.2.3 to Lemma 8.2.4.

Lemma 8.2.5. *Let $P_0, P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_i'}$ such that $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ and $P_0 \sim_\phi P_1$ and $P_0 \overset{\mathbb{L}}{\not\leftarrow} P_1$. There exists two $\mathbb{ES}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes L and G such that:*

1. *$L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$,*
2. *there is no $k \in [d-1]$ such that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ and $k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ and*
3. *$L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$ or $L\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ G$.*

Intuitively, Condition 2 states that there is nothing $\mathbb{L}\overline{\mathbb{S}}_{P_0}$-between L and G, that is, G is the $\mathbb{L}\overline{\mathbb{S}}_{P_0}$-successor of L. Note however that $L\ \mathbb{S}_{P_0}\ G$ does not hold, as it is not defined.

Condition (3) states that $L\ \mathbb{L}\mathbb{E}\mathbb{S}_{P_1}\ G$ does not hold.

Proof. Since $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ then P_0 and P_1 have the same set of $\mathbb{ES}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes. Since $P_0 \overset{\mathbb{L}}{\not\leftarrow} P_1$, there exists L and G two distinct $\mathbb{ES}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes such that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ and ($L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$ or $L\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ G$). Let $\mathfrak{P}$ be the set of such pairs (L,G).

Let $\mathfrak{R}(L,G)$ be the set of $\mathbb{ES}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes K such that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ K$ and $K\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$. Let $(L,G) \in \mathfrak{P}$ such that $\mathfrak{R}(L,G)$ is $\subseteq$-minimal. Let us prove that $\mathfrak{R}(L,G) = \emptyset$, it implies that the lemma holds. For the sake of contradiction, let us assume that $\mathfrak{R}(L,G) \neq \emptyset$, that is that there exists an $\mathbb{ES}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-class K which belongs to $\mathfrak{R}(L,G)$, that is, such that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ K$ and $K\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$.

Two cases must be considered, depending on whether ($L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ K$ or $L\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ K$) or $L\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ K$.

- Let us suppose that ($L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ K$ or $L\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ K$) then $(L,K) \in \mathfrak{P}$. Let us prove that $\mathfrak{R}(L,K) \subsetneq \mathfrak{R}(L,G)$, it implies that $(L,K) \in \mathfrak{P}$ and $\mathfrak{R}(L,K) \subsetneq \mathfrak{R}(L,G)$, it contradicts the hypothesis that $\mathfrak{R}(L,G)$ is $\subseteq$-minimal.

  Let us first prove that $\mathfrak{R}(L,K) \subseteq \mathfrak{R}(L,G)$. Let $K' \in \mathfrak{R}(L,K)$, let us prove that $K' \in \mathfrak{R}(L,G)$. Since $K' \in \mathfrak{R}(L,K)$, by definition of $\mathfrak{R}(L,K)$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ K'$ and $K'\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ K$. Since $K'\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ K$ and since $K\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$, $K'\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ K'$ and $K'\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$, by definition on $\mathfrak{R}(L,G)$, $K' \in \mathfrak{R}(L,G)$. Since $K \notin \mathfrak{R}(L,K)$ and since $K \in (L,G)$, $\mathfrak{R}(L,K) \neq \mathfrak{R}(L,G)$. Since $\mathfrak{R}(L,K) \neq \mathfrak{R}(L,G)$ and since $\mathfrak{R}(L,K) \subseteq \mathfrak{R}(L,G)$, $\mathfrak{R}(L,K) \subsetneq \mathfrak{R}(L,G)$.

- Let us now suppose that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ K$. Similarly to the last disjunction, two cases must be considered, depending on whether ($G\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ K$ or $K\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ G$) or $K\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ G$.

  - Let us first suppose that $K\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ G$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ K$ and $K\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ G$ then $L\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ G$, which contradicts the fact that ($L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$ or $L\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ G$).
  - Let us now suppose that ($G\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ K$ or $K\ \overline{\mathbb{L}}\ \overline{\mathbb{E}}\ \overline{\mathbb{G}}_{P_1}\ G$). As in the preceding case, $(K,G) \in \mathfrak{P}$ and $\mathfrak{R}(K,G) \subsetneq \mathfrak{R}(L,G)$ which contradicts the minimality hypothesis.

□

Lemma 8.2.3 can now be proven.

Proof of Lemma 8.2.3. Since $P_0 \overset{\mathbb{OESB}}{\cong} P_1$, it follows that P_0 and P_1 have the same set of $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes. By Lemma 8.2.5, there exists L and G two distinct $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{P_0}$-classes which satisfy the three conditions of Lemma 8.2.5.

The proof consist in two parts, constructing the $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop R and proving that it satisfy the hypothesis.

Constructing R The $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop R is now constructed. It is then proved that R satisfies the property of the lemma.

Let $R \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be defined as follows, for all $i,j \in [d-1]$:

- $R \overset{\mathbb{MOESB}}{\cong} P_0$,
- $i\ \mathbb{L}_R\ j$ holds if and only if $i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$),

Note that: $i\ \mathbb{L}\overline{\mathbb{S}}_R\ j$ holds if and only if $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$).

Let us prove that $R \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$.

- Since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $R \overset{\mathbb{MOESB}}{\cong} P_0$ and $\mathbb{L}_R \subseteq \mathbb{L}_{P_0}$, by Lemma 8.1.15, R satisfies Axioms (1 - $\mathbb{E}$ equivalence), (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$), (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (6 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{E}$ compatible), (7 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{S}$ compatible), (8 - $\mathbb{L}$ asymmetric), (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod) and $R \in \mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$.
- Let us consider axiom (9 - $\mathbb{L}$ transitive). Let us assume that $i\ \mathbb{L}_R\ j$ and $j\ \mathbb{L}_R\ k$ and let us prove that $i\ \mathbb{L}_R\ k$. Since $i\ \mathbb{L}_R\ j$, it follows that $i\ \mathbb{L}_{P_0}\ j$ and (either $i \notin L$ or $j \notin G$). Since $j\ \mathbb{L}_R\ k$, it follows that $j\ \mathbb{L}_{P_0}\ k$ and (either $j \notin L$ or $k \notin G$). Since $i\ \mathbb{L}_{P_0}\ j$ and since $j\ \mathbb{L}_{P_0}\ k$, $i\ \mathbb{L}_{P_0}\ k$. Let us claim that ($i \notin L$ or $k \notin G$), by definition of R, it implies that $i\ \mathbb{L}_O\ k$.

  Let us prove that ($i \notin L$ or $k \notin G$). For the sake of contradiction, let us assume that $i \in L$ and $k \in G$. Since $i \in L$ and (either $i \notin L$ or $j \notin G$), it follows that $j \notin G$. Since $k \in G$ and since ($j \notin L$ or $k \notin G$), $j \notin L$.

  Since $i\ \mathbb{L}_{P_0}\ j$ and since $i \in L$ then $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$. Since $j\ \mathbb{L}_{P_0}\ k$ and since $k \in G$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$.

  Note that $j \notin L \cup G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ contradicts Condition 2 of Lemma 8.2.5.
- Since the only difference between P_0 and R are that some $\mathbb{L}$s are removed from P_0 to obtain R, and only from positions which neither belong to $\mathbb{O}_{P_0}$ nor $\mathbb{B}_{P_0}$, then R satisfies Axioms (10 - $i\ \mathbb{E}_T\ j, i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$), (12 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{L}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$) and (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$).

Proving that R satisfies the conditions of the proposition. Let us prove that $R \sim_\phi P_0$. Let us claim that there exists $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ such that:

- $O \sim_\phi P_0$ and
- for all $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ with $R \overset{\mathbb{L}}{\sqsubseteq} T$, either $P_0 \overset{\mathbb{L}}{\sqsubseteq} T$ or $O \overset{\mathbb{L}}{\sqsubseteq} T$.

Let us prove that it implies $R \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and $R \sim_\phi P_0$. It suffices to prove that, for all $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ such that $R \overset{\mathbb{L}}{\sqsubseteq} T$, one has $T \sim_\phi P_0$. By hypothesis, either $P_0 \overset{\mathbb{L}}{\sqsubseteq} T$, in this case $P_0 \sim_\phi T$, or $O \overset{\mathbb{L}}{\sqsubseteq} T$, and by hypothesis $P_0 \sim_\phi O \sim_\phi T$.

It remains to prove that $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ exists which satisfies the conditions. The $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop O is almost the one created by Lemma 8.2.4. Note that P_0 and P_1 does not satisfy the hypothesis of this lemma. Hence, a pair of $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop P'_0 and P'_1 are created such that:

- $P_0 \overset{\mathbb{L}}{\sqsubseteq} P'_0$ and $P_1 \overset{\mathbb{L}}{\sqsubseteq} P'_1$,
- P'_0 and P'_1 satisfy the hypothesis of Lemma 8.2.4,
- the O created in this lemma satisfies the hypothesis announced above.

Before constructing P'_0 and P'_1, let us first prove that $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $k\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ imply that $k \in L \cup G$ and let us call (*) this statement.

Two cases must be considered, depending on whether $k \in L$ or not. If $k \in L$ then (*) holds. Otherwise, let us assume that $k \notin L$ and let us prove that $k \in G$. Since $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and since $k \notin L$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, by Condition 2 of Lemma 8.2.5, $k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ does not hold. Since $k\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ holds and $k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ does not hold then $k\ \mathbb{E}\wr\mathbb{S}_{P_0}\ G$, hence $k \in G$.

Constructing P'_0 Let P'_0 be defined as follows. For all $i,j \in [d-1]$:

- $P'_0 \overset{\mathbb{MOESB}}{\cong} P_0$ and
- $i\ \mathbb{L}_{P'_0}\ j$ holds if and only if $i\ \mathbb{L}_{P_0}\ j$ or [$i\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and (i or j does not belong to $L \cup G$)].

Hence $i\ \mathbb{L}\overline{\mathbb{S}}_{P'_0}\ j$ holds if and only if $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ or [$i\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and (i or j does not belong to $L \cup G$)].

Similarly, $i\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P'_0}\ j$ holds if and only if $i\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ or [$i\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and (i or j does not belong to $L \cup G$)].

Let us prove that P'_0 satisfies the Condition (2) of Lemma 8.2.4. Let $k \in [d-1]$. Let us suppose that $L\ \mathbb{L}\overline{\mathbb{S}}_{P'_0}\ k$ and $k \notin G$ and let us prove that $G\ \mathbb{L}\overline{\mathbb{S}}_{P'_0}\ k$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P'_0}\ k$ by definition of P'_0, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$ or [$L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and ($L \not\subseteq L \cup G$ or $k \notin L \cup G$)], both cases are considered separately.

- Let us first suppose that $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $k \notin L$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ k$, $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$. Since $G\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P'_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and $k \notin L \cup G$, by definition of P'_0, $k\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P'_0}\ G$.
- Let us now suppose that $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and ($L \not\subseteq L \cup G$ or $k \notin L \cup G$). Since $L \subseteq L$ and since ($L \not\subseteq L \cup G$ or $k \notin L \cup G$), $k \notin L \cup G$. Since $G\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P'_0}\ G$ and $L\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P_0}\ k$, and $k \notin L \cup G$, by definition of P'_0, $k\ \mathbb{L}\lambda\mathbb{E}\wr\mathbb{S}_{P'_0}\ G$.

Proving that $k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ and $k \notin L$ implies $k\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ L$ is similar by symmetry.

In order to use Lemma 8.2.4, the case $L\ \overline{\mathbb{L}}\,\overline{\mathbb{E}}\,\overline{\mathbb{G}}_{P_1}\ G$ is reduced to the case $L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$, with the introduction of a $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop $P'_1 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ such that $P_1 \overset{\mathbb{L}}{\sqsubseteq} P'_1$ and such that P'_1 satisfies the conditions of Lemma 8.2.4. Since $P_1 \overset{\mathbb{L}}{\sqsubseteq} P'_1$ and $P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, by definition of $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $P'_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and $P'_1 \sim_\phi P_1$. Since $P'_1 \sim_\phi P_1 \sim_\phi P_0$, $P'_1 \sim_\phi P_0$. Intuitively P'_1 is similar to P_1, except that $\mathbb{L}_{P'_1}$ is the transitive closure of $\mathbb{L}_{P_1} \cup \{(j,i) \mid j \in G, i \in L\}$.

Constructing P'_1 The $(\zeta, \beta, \nu, \mathcal{V}'_\iota)^m$-pop P'_1 is defined as follows:

- $P'_1 \overset{\mathbb{MOESB}}{\cong} P_1$ and
- for all $i, j \in [d-1]$, $i \mathbb{L}_{P'_1} j$ holds if and only if $i \mathbb{L}_{P_1} j$ or ($i \mathbb{LIES}_{P_1} G$ and $L \mathbb{LIES}_{P_1} j$).

Constructing O Let $O \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be defined as follows, for all $i, j \in [d-1]$:

- $O \overset{\mathbb{MOESB}}{\cong} P'_0$,
- $i \mathbb{L}_O j$ holds if and only if [$i \mathbb{L}_{P'_0} j$ and (either $i \notin L$ or $j \notin G$)] or ($i \in G$ and $j \in L$).

Since P'_0, P'_1 and O satisfy the hypothesis of Lemma 8.2.4, $O \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, and $O \sim_\phi P'_0 \sim_\phi P_0$. It remains to prove that for all $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ with $R \overset{\mathbb{L}}{\sqsubseteq} T$, either $P_0 \overset{\mathbb{L}}{\sqsubseteq} T$ or $O \overset{\mathbb{L}}{\sqsubseteq} T$.

Characterizing O using R Let us first give a characterization of O in term of R. Note first that $O \overset{\mathbb{MOESB}}{\cong} P'_0 \overset{\mathbb{MOESB}}{\cong} P_0 \overset{\mathbb{MOESB}}{\cong} R$.

Let us now prove that $i \mathbb{L}_O j$ is equivalent to {[$i \mathbb{L}_{P_0} j$ and (either $i \notin L$ or $j \notin G$)] or [$i \mathbb{LIES}_{P_0} G$ and $L \mathbb{LIES}_{P_0} j$]}

Let us first assume that $i \mathbb{L}_O j$. Then [$i \mathbb{L}_{P'_0} j$ and (either $i \notin L$ or $j \notin G$)] or ($i \in G$ and $j \in L$).

Both cases are considered separately.

- Let us first suppose that $i \mathbb{L}_{P'_0} j$ and (either $i \notin L$ or $j \notin G$). Since $i \mathbb{L}_{P'_0} j$ by definition of P'_0, $i \mathbb{L}_{P_0} j$ or [$i \mathbb{LIES}_{P_0} G$ and $L \mathbb{LIES}_{P_0} j$ and (i or j does not belong to $L \cup G$)]. Both cases are considered separately.
  - If $i \mathbb{L}_{P_0} j$, since (either $i \notin L$ or $j \notin G$), the property holds.
  - Let us now suppose that $i \mathbb{LIES}_{P_0} G$ and $L \mathbb{LIES}_{P_0} j$, in this case, there is nothing to prove.
- Let us now suppose that $i \in G$ and $j \in L$. Since $i \in G$, $i \mathbb{LIES}_{P_0} G$. Since $j \in L$, $L \mathbb{LIES}_{P_0} j$.

Let us now suppose that [$i \mathbb{L}_{P_0} j$ and (either $i \notin L$ or $j \notin G$)] or [$i \mathbb{LIES}_{P_0} G$ and $L \mathbb{LIES}_{P_0} j$] and let us prove that $i \mathbb{L}_O j$. Both cases are considered separately.

- Let us suppose that $i \mathbb{L}_{P_0} j$ and (either $i \notin L$ or $j \notin G$). Since $i \mathbb{L}_{P_0} j$, by definition of P'_0, $i \mathbb{L}_{P'_0} j$. Since $i \mathbb{L}_{P'_0} j$ and (either $i \notin L$ or $j \notin G$), by definition of O, $i \mathbb{L}_O j$.
- Let us suppose that $i \mathbb{LIES}_{P_0} G$ and $L \mathbb{LIES}_{P_0} j$. Two cases must be considered, depending on whether ($i \in G$ and $j \in L$) or not.
  - if $i \in G$ and $j \in L$, by definition of O, $i \mathbb{L}_O j$.
  - Let us suppose that (i or j does not belong to $L \cup G$). Since $i \mathbb{LIES}_{P_0} G$ and $L \mathbb{LIES}_{P_0} j$ and (i or j does not belong to $L \cup G$), by definition of P'_0, $i \mathbb{L}_{P'_0} j$. Since $i \mathbb{L}_{P'_0} j$ and (i or j does not belong to $L \cup G$), by definition of O, $i \mathbb{L}_O j$.

Proving that O satisfies the conditions of the proposition. It is now proven that for all $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}$ with $R \overset{\mathbb{L}}{\sqsubseteq} T$, either $P_0 \overset{\mathbb{L}}{\sqsubseteq} T$ or $O \overset{\mathbb{L}}{\sqsubseteq} T$.

Let $T \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}$ such that $R \overset{\mathbb{L}}{\sqsubseteq} T$. Two cases must be considered, depending on whether $L\ \mathbb{L}\overline{\mathbb{S}}_T\ G$ or $G\ \mathbb{L}\overline{\mathbb{S}}_T\ L$.

- Let us first suppose that $L\ \mathbb{L}\overline{\mathbb{S}}_T\ G$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_T\ G$ and $R \overset{\mathbb{L}}{\sqsubseteq} T$, by construction of R, $P_0 \overset{\mathbb{L}}{\sqsubseteq} T$.
- Let us now suppose that $G\ \mathbb{L}\overline{\mathbb{S}}_T\ L$. Note that the only difference between O and R is that $\mathbb{L}_O$ is the transitive closure of $\mathbb{L}_R \cup \{(G,L)\}$. Since $G\ \mathbb{L}\overline{\mathbb{S}}_T\ L$ and $R \overset{\mathbb{L}}{\sqsubseteq} T$, by construction of R and of O, $O \overset{\mathbb{L}}{\sqsubseteq} T$.

$P_0' \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}$ $P_0' \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}$. It remains to prove that P_1' and P_1' belongs to $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}$. Let us first prove that then

- Since $P_0 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}$, $P_0' \overset{\text{MOESB}}{\cong} P_0$ and $\mathbb{L}_{P_0} \subseteq \mathbb{L}_{P_0'}$, by Lemma 8.1.15, P_0' satisfies Axioms (1 - $\mathbb{E}$ equivalence), (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$), (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (6 - $\text{POSITION}_{\mathcal{V}_t'(m)}$ and $\mathbb{E}$ compatible), (7 - $\text{POSITION}_{\mathcal{V}_t'(m)}$ and $\mathbb{S}$ compatible), (12 - $\text{POSITION}_{\mathcal{V}_t'(m)}$ and $\mathbb{L}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod) and (19 - Rigid case).
- Let us consider Axiom (8 - $\mathbb{L}$ asymmetric). Let us assume that $i\ \mathbb{L}_{P_0'}\ j$ and let us prove that $j\ \mathbb{L}_{P_0'}\ i$ does not hold. Since $j\ \mathbb{L}_{P_0'}\ i$, by definition of P_0', $i\ \mathbb{L}_{P_0'}\ j$ or ($i\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ j$ and i or j does not belong to $L \cup G$), both cases are considered separately.
  - Let us suppose that $i\ \mathbb{L}_{P_0}\ j$. Since $i\ \mathbb{L}_{P_0}\ j$, $j\ \mathbb{L}_{P_0}\ i$ does not hold. For the sake of contradiction, let us assume that $j\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ i$. Hence $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}i\mathbb{L}_{P_0}j\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$, then (*), $i, j \in L \cup G$.

    Since neither $j\ \mathbb{L}_{P_0}\ i$ nor ($j\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ i$ and i or j does not belong to $L \cup G$) hold, by definition of P_0', $j\ \mathbb{L}_{P_0'}\ i$ does not hold.
  - Let us suppose that $i\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ j$ and (i or j does not belong to $L \cup G$).

    For the sake of contradiction, let us suppose that $j\ \mathbb{L}_{P_0'}\ i$ holds. Let us claim that $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}i\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$ and $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}j\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$. Hence, by (*), $j \in L$ and $i \in G$, which contradicts the fact that (i or j does not belong to $L \cup G$).

    Let us prove that $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}i\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$ and $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}j\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$. Since $j\ \mathbb{L}_{P_0'}\ i$, either $j\ \mathbb{L}_{P_0'}\ i$ or whether ($j\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ i$ and i or j does not belong to $L \cup G$). The two cases are considered separately:
    - Let us suppose that $j\ \mathbb{L}_{P_0'}\ i$. Since $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ j$, $j\ \mathbb{L}_{P_0'}\ i$ and $i\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ it follows that $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}j\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$ and $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}i\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$.
    - Let us suppose $j\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ i$. Since $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ j$ and $j\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ it follows that $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}j\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$. Since $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ i$ and since $i\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$, $L\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}i\mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}G$.
- Let us consider Axiom (9 - $\mathbb{L}$ transitive).

  Let us assume that $i\ \mathbb{L}_{P_0'}\ j$ and that $j\ \mathbb{L}_{P_0'}\ k$ and let us prove that $i\ \mathbb{L}_{P_0'}\ k$. Since $i\ \mathbb{L}_{P_0'}\ j$, by definition of P_0', either $i\ \mathbb{L}_{P_0}\ j$ or [$i\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\partial\mathbb{E}\partial\mathbb{S}_{P_0}\ j$ and (i or j does not belong to $L \cup G$)]. Both cases are considered separately.

– Let us suppose that $i \, \mathbb{L}_{P_0} \, j$.

Since $j \, \mathbb{L}_{P'_0} \, k$ by definition of P'_0, either $j \, \mathbb{L}_{P_0} \, k$ or [$j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and (j or k does not belong to $L \cup G$)

∗ Let us suppose that $j \, \mathbb{L}_{P_0} \, k$. Since $i \, \mathbb{L}_{P_0} \, j$ and since $j \, \mathbb{L}_{P_0} \, k$, $i \, \mathbb{L}_{P_0} \, k$ hence by definition of P'_0, $i \, \mathbb{L}_{P'_0} \, k$.

∗ Let us suppose that $j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and (j or k does not belong to $L \cup G$). Since $i \, \mathbb{L}_{P_0} \, j$ and since $j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$, $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$. Two cases are considered, depending on whether $k \notin L \cup G$ or not.

· Let us suppose that $k \notin L \cup G$. Since $i \, \mathbb{L}_{P_0} \, G$, $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$. Since $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and $k \notin L \cup G$, by definition of P'_0, $i \, \mathbb{L}_{P'_0} \, k$.

· Let us suppose that $k \in L \cup G$. Since $k \in L \cup G$ and since (j or k does not belong to $L \cup G$), $j \notin L \cup G$. Since $j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and since $j \notin G$, $j \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, G$. Since $i \, \mathbb{L}_{P_0} \, j$ and since $j \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, G$, $i \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, G$, hence $i \notin G$ and $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, J$. Let us claim that $i \notin L$. Since $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and $i \notin L \cup G$, by definition of P'_0, $i \, \mathbb{L}\overline{\mathbb{S}}_{P'_0} \, k$.
Let us prove that $i \notin L$. For the sake of contradiction, let us claim that $i \in L$. Since $i \, \mathbb{L}_{P_0} \, j$ and since $i \in L$, $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, j$. Since $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, j$ and since $j \notin L$, $L \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, j$. Note that $L \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, j$ and $j \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, G$ contradicts Condition (2) of Lemma 8.2.5.

– Let us suppose that $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, j$ and (i or j does not belong to $L \cup G$).

Since $j \, \mathbb{L}_{P'_0} \, k$ by definition of P'_0, either $j \, \mathbb{L}_{P_0} \, k$ or [$j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and (j or k does not belong to $L \cup G$)]

∗ Let us suppose that $j \, \mathbb{L}_{P_0} \, k$. Since $j \, \mathbb{L}_{P_0} \, k$ and since $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, j$, $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$. Two cases are considered, depending on whether $i \notin L \cup G$ or not.

· Let us suppose that $i \notin L \cup G$. Since $L \, \mathbb{L}_{P_0} \, k$, $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$. Since $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$, $L \, \mathbb{L}_{P_0} \, k$ and $i \notin L \cup G$, by definition of P'_0, $i \, \mathbb{L}\overline{\mathbb{S}}_{P'_0} \, k$.

· Let us suppose that $i \in L \cup G$. Since $i \notin L \cup G$ and since (j or i does not belong to $L \cup G$), $j \notin L \cup G$. Since $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, j$ and since $j \notin L$, $L \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, j$. Since $j \, \mathbb{L}_{P_0} \, k$ and since $L \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, j$, $L \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, k$, hence $k \notin L$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$. Let us claim that $k \notin G$. Since $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$, $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and $k \notin L \cup G$, by definition of P'_0, $i \, \mathbb{L}\overline{\mathbb{S}}_{P'_0} \, k$.
Let us prove that $k \notin G$. For the sake of contradiction, let us claim that $k \in G$. Since $j \, \mathbb{L}_{P_0} \, k$ and since $k \in G$, $j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$. Since $j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and since $j \notin G$, $j \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, G$. Note that $j \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, G$ and $L \, \mathbb{L}\overline{\mathbb{S}}_{P_0} \, j$ contradicts Condition (2) of Lemma 8.2.5.

∗ Let us suppose that $j \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and (j or k does not belong to $L \cup G$). Since $L\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} j \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} G$, by (*), j belongs to L or to G. Since $j \in L \cup G$ and since (j or k does not belong to $L \cup G$), $k \notin L \cup G$. Since $i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and $k \notin L \cup G$, by definition of P'_0, $i \, \mathbb{L}_{P'_0} \, k$.

• Let us suppose that $i \, \mathbb{S}_{P'_0} \, j$ and $i \, \mathbb{L}_{P'_0} \, k$ hold and let us prove that $j \, \mathbb{L}_{P'_0} \, k$ or $j \, \mathbb{E}_{P'_0} \, k$ hold. Since $i \, \mathbb{S}_{P'_0} \, j$, by definition of P'_0, $i \, \mathbb{S}_{P_0} \, j$. Since $i \, \mathbb{L}_{P'_0} \, k$, either $i \, \mathbb{L}_{P_0} \, k$ or [$i \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, G$ and $L \, \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0} \, k$ and (i or k does not belong to $L \cup G$)], both cases are considered separately.

– Let us suppose that $i \, \mathbb{L}_{P_0} \, k$. Since $i \, \mathbb{L}_{P_0} \, k$ and since $i \, \mathbb{S}_{P_0} \, j$, either $j \, \mathbb{E}_{P_0} \, k$ or $j \, \mathbb{L}_{P_0} \, k$, both cases are considered separately.

∗ Let us suppose that $j \, \mathbb{E}_{P_0} \, k$, by definition of P'_0, it implies $j \, \mathbb{E}_{P'_0} \, k$.

∗ Let us suppose that $j \, \mathbb{L}_{P_0} \, k$, by definition of P'_0, it implies $j \, \mathbb{L}_{P'_0} \, k$.

– Let us suppose that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and (i or k does not belong to $L\cup G$). Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and since $i\ \mathbb{S}_{P_0}\ j$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$. Let us prove that j or k does not belong to $L\cup G$, since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$, by definition of P'_0, $j\ \mathbb{L}_{P'_0}\ k$.

Two cases must be considered, depending on whether i or whether k does not belong to $L\cup G$. If $k\notin L\cup G$, there is nothing to prove, let us suppose that i does not belong to $L\cup G$. Since L and G are $\mathbb{E}\wr\mathbb{S}_{P_0}$-classes, since $i\ \mathbb{S}_{P_0}\ j$ and since $i\notin L\cup G$, $j\notin L\cup G$.

- Let us consider Axiom (10 - $i\ \mathbb{E}_T\ j$,$i\ \mathbb{L}_T\ k\Longrightarrow j\ \mathbb{L}_T\ k$). Let us suppose that $i\ \mathbb{E}_{P'_0}\ j$, $i\ \mathbb{L}_{P'_0}\ k$ and let us prove that $j\ \mathbb{L}_{P'_0}\ k$. Since $i\ \mathbb{E}_{P'_0}\ j$, by definition of P'_0, $i\ \mathbb{E}_{P_0}\ j$. Since $i\ \mathbb{L}_{P'_0}\ k$, by definition of P'_0, $i\ \mathbb{L}_{P_0}\ k$ or [$i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and (i or k does not belong to $L\cup G$)], both cases are considered separately.

  – Let us suppose that $i\ \mathbb{L}_{P_0}\ k$. Since $i\ \mathbb{E}_{P_0}\ j$ and since $i\ \mathbb{L}_{P_0}\ k$, $j\ \mathbb{L}_{P_0}\ k$, by definition of P'_0, it implies $j\ \mathbb{L}_{P'_0}\ k$.

  – Let us suppose that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and (i or k does not belong to $L\cup G$). Since (i or k does not belong to $L\cup G$), since $i\ \mathbb{E}_{P_0}\ j$, and since L and G are $\mathbb{E}\wr\mathbb{S}_{P_0}$-classes, ($j$ or k does not belong to $L\cup G$). Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and since $i\ \mathbb{E}_{P_0}\ j$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$. Since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$, since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and since (j or k does not belong to $L\cup G$), by definition of P'_0, $i\ \mathbb{L}_{P'_0}\ j$.

- Let us consider Axiom (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible). For the sake of contradiction, let us suppose that $i\ \mathbb{E}_{P'_0}\ j$ and $i\ \mathbb{L}_{P'_0}\ j$ hold. Since $i\ \mathbb{E}_{P'_0}\ j$ by definition of P'_0, $i\ \mathbb{E}_{P_0}\ j$, hence $i\ \mathbb{L}_{P'_0}\ j$ does not hold. Since $i\ \mathbb{L}_{P'_0}\ j$ and $i\ \mathbb{L}_{P'_0}\ j$ does not hold, by definition of P'_0, $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$ and (i or j does not belong to $L\cup G$). Since $i\ \mathbb{E}_{P_0}\ j$, it follows that $(i\in L)\Longleftrightarrow(j\in L)$ and $(i\in G)\Longleftrightarrow(j\in G)$. Since $(i\in L)\Longleftrightarrow(j\in L)$, $(i\in G)\Longleftrightarrow(j\in G)$ and (i or j does not belong to $L\cup G$) it follows that $i,j\notin L\cup G$. Since $i\notin G$ and since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$, $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$. Since $j\notin L$ and since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ j$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$. Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ j$ and since $i\ \mathbb{E}_{P_0}\ j$, $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$. Having both $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ i$ and $i\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$ contradicts Condition 2 of the Lemma.

- Let us consider Axiom (14 - $(i\mathbb{S}j\wedge i\mathbb{L}k)\Longrightarrow(j\mathbb{E}k\vee i\mathbb{L}k)$). Let us suppose that $i\ \mathbb{S}_{P'_0}\ j$, $i\ \mathbb{L}_{P'_0}\ k$ and let us prove that $j\ \mathbb{E}_{P'_0}\ k$ or $j\ \mathbb{L}_{P'_0}\ k$. Since $i\ \mathbb{S}_{P'_0}\ j$, by definition of P'_0, $i\ \mathbb{S}_{P_0}\ j$. Since $i\ \mathbb{L}_{P'_0}\ k$, by definition of P'_0, $i\ \mathbb{L}_{P_0}\ k$ or [$i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and (i or k does not belong to $L\cup G$)], both cases are considered separately.

  – Let us suppose that $i\ \mathbb{L}_{P_0}\ k$. Since $i\ \mathbb{S}_{P_0}\ j$ and since $i\ \mathbb{L}_{P_0}\ k$, either $j\ \mathbb{E}_{P_0}\ k$ or $j\ \mathbb{L}_{P_0}\ k$, both cases are considered separately.

    * Let us suppose that $j\ \mathbb{E}_{P_0}\ k$, by definition of P'_0, it implies $j\ \mathbb{E}_{P'_0}\ k$.
    * Let us suppose that $j\ \mathbb{L}_{P_0}\ k$, by definition of P'_0, it implies $j\ \mathbb{L}_{P'_0}\ k$.

  – Let us suppose that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and (i or k does not belong to $L\cup G$). Since (i or k does not belong to $L\cup G$), since $i\ \mathbb{S}_{P_0}\ j$, and since L and G are $\mathbb{E}\wr\mathbb{S}_{P_0}$-classes, ($j$ or k does not belong to $L\cup G$). Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$ and since $i\ \mathbb{E}_{P_0}\ j$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$. Since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ G$, since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_0}\ k$ and since (j or k does not belong to $L\cup G$), by definition of P'_0, $i\ \mathbb{L}_{P'_0}\ j$.

- Let us consider Axiom (20 - ν). Since $L\ \mathbb{L}\overline{\mathbb{S}}_{P_0}\ G$, $L\subseteq\nu\Longleftrightarrow G\subseteq\nu$, the axiom easily follows.

$P'_1\in\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_i}$. Let us prove that $P'_1\in\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_i}$.

- Since $P_1 \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, P'_1 easily satisfies Axioms (1 - $\mathbb{E}$ equivalence), (2 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{S}_T\ k \Longrightarrow j\ \mathbb{E}_T\ k$), (3 - $i\ \mathbb{S}_T\ j \wedge i\ \mathbb{E}_T\ k \Longrightarrow j\ \mathbb{S}_T\ k$), (4 - $\mathbb{S}$ and $\mathbb{E}$ incompatible), (5 - $\mathbb{S}$ not cyclic), (6 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{E}$ compatible), (7 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{S}$ compatible), (10 - $i\ \mathbb{E}_T\ j, i\ \mathbb{L}_T\ k \Longrightarrow j\ \mathbb{L}_T\ k$), (12 - $\textsc{position}_{\mathcal{V}'_\iota(m)}$ and $\mathbb{L}$ compatible), (13 - $\mathbb{S}$ implies $\mathbb{L}$), (15 - $\mathbb{O}$ and mod), (16 - $\mathbb{E}$ and mod), (17 - $\mathbb{S}$ and mod), (18 - $\mathbb{B}$ and mod) and (19 - Rigid case).

- Let us consider Axiom (8 - $\mathbb{L}$ asymmetric).

  Let us assume that $i\ \mathbb{L}_{P'_1}\ j$ and let us prove that $j\ \mathbb{L}_{P'_1}\ i$ does not hold. Since $i\ \mathbb{L}_{P'_1}\ j$, by definition of P'_1, either $i\ \mathbb{L}_{P_1}\ j$ or ($i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$). The two cases are considered separately.

  - Let us suppose that $i\ \mathbb{L}_{P_1}\ j$. Since $i\ \mathbb{L}_{P_1}\ j$, $j\ \mathbb{L}_{P_1}\ i$ does not hold. Let us claim that ($j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$) does not hold. Since neither $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ i$ nor ($j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$) hold, by definition of P'_1, $j\ \mathbb{L}_{P'_1}\ i$ does not hold.
    For the sake of contradiction, let us assume that $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ i$. Hence $L\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1} i \mathbb{L}_{P_1} j \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1} G$, which contradicts the fact that $G\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ L$.
  - Let us suppose that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$. By hypothesis $L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$, hence $i\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1} G \mathbb{L}\overline{\mathbb{S}}_{P_1} L \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1} j$, hence $j\ \mathbb{L}_{P_1}\ i$ does not hold. Let us claim that ($j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$) does not hold. Since neither $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ i$ nor ($j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$) hold, by definition of P'_1, $j\ \mathbb{L}_{P'_1}\ i$ does not hold.
    For the sake of contradiction, let us assume that $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ i$. Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$, $L\ \mathbb{G}\overline{\mathbb{P}}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ i$, it follows that $i\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ i$ which is a contradiction.

- Let us consider Axiom (9 - $\mathbb{L}$ transitive).

  Let us assume that $i\ \mathbb{L}_{P'_1}\ j$ and that $j\ \mathbb{L}_{P'_1}\ k$ and let us prove that $i\ \mathbb{L}_{P'_1}\ k$. Since $i\ \mathbb{L}_{P'_1}\ j$, by definition of P'_1, either $i\ \mathbb{L}_{P_1}\ j$ or ($i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P'_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P'_1}\ j$). The two cases are considered separately.

  - Let us suppose that $i\ \mathbb{L}_{P_1}\ j$. Since $j\ \mathbb{L}_{P'_1}\ k$, either $j\ \mathbb{L}_{P_1}\ k$ or ($j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P'_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P'_1}\ k$). The two cases are considered separately.
    - Let us suppose that $j\ \mathbb{L}_{P_1}\ k$. Since $i\ \mathbb{L}_{P_1}\ j$ and since $j\ \mathbb{L}_{P_1}\ k$, $i\ \mathbb{L}_{P_1}\ k$ hence by definition of P'_1, $i\ \mathbb{L}_{P'_1}\ k$.
    - Let us suppose that $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ k$. Since $i\ \mathbb{L}_{P_1}\ j$ and since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$, $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$. Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ k$, by definition of P'_1, $i\ \mathbb{L}\overline{\mathbb{S}}_{P'_1}\ k$.
  - Let us suppose that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$. Since $j\ \mathbb{L}_{P'_1}\ k$, by definition of P'_1, either $j\ \mathbb{L}\overline{\mathbb{S}}_{P_1}\ k$ or ($j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P'_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P'_1}\ k$). The two cases are considered separately.
    - Let us suppose that $j\ \mathbb{L}_{P_1}\ k$. Since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$ and since $j\ \mathbb{L}_{P_1}\ k$, $L\ \mathbb{L}_{P_1}\ k$. Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}_{P_1}\ k$, by definition of P'_1, $i\ \mathbb{L}_{P'_1}\ k$.
    - Let us suppose that $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ k$. Since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$ and since $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$, $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$, which does not hold by hypothesis about P_1.

- let us consider Axiom (11 - $\mathbb{L}$ and $\mathbb{E}$ incompatible). For the sake of contradiction, let us suppose that $i\ \mathbb{E}_{P'_1}\ j$ and $i\ \mathbb{L}_{P'_1}\ j$ hold. Since $i\ \mathbb{E}_{P'_1}\ j$ by definition of P'_1, $i\ \mathbb{E}_{P_1}\ j$, hence $i\ \mathbb{L}_{P'_1}\ j$ does not hold. Since $i\ \mathbb{L}_{P'_1}\ j$ and $i\ \mathbb{L}_{P'_1}\ j$ does not hold, by definition of P'_1, $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$. Since $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ and since $i\ \mathbb{E}_{P_1}\ j$, $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$. Since $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ j$ and $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ it follows that $L\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{P_1}\ G$ which contradicts Condition 3 of the lemma.

- Let us consider Axiom (14 - $(i\mathbb{S}j \wedge i\mathbb{L}k) \Longrightarrow (j\mathbb{E}k \vee i\mathbb{L}k)$). Let us suppose that $i\ \mathbb{S}_{P'_1}\ j$ and $i\ \mathbb{L}_{P'_1}\ k$ hold and let us prove that $j\ \mathbb{L}_{P'_1}\ k$ or $j\ \mathbb{E}_{P'_1}\ k$ hold. Since $i\ \mathbb{S}_{P'_1}\ j$, by definition of P'_1, $i\ \mathbb{S}_{P_1}\ j$.

Since $i \mathbb{L}_{P_1'} k$, by definition of P_1', either $i \mathbb{L}_{P_1} k$ or ($i \mathbb{LER}\mathbb{S}_{P_1} G$ and $L \mathbb{LER}\mathbb{S}_{P_1} k$), both cases are considered separately.

- Let us suppose that $i \mathbb{L}_{P_1} k$. Since $i \mathbb{L}_{P_1} k$ and since $i \mathbb{S}_{P_1} j$, either $j \mathbb{E}_{P_1} k$ or $j \mathbb{L}_{P_1} k$, both cases are considered separately.
  - Let us suppose that $j \mathbb{E}_{P_1} k$, by definition of P_1', $j \mathbb{E}_{P_1'} k$.
  - Let us suppose that $j \mathbb{L}_{P_1} k$, by definition of P_1', $j \mathbb{L}_{P_1'} k$.
- Let us suppose that $i \mathbb{LER}\mathbb{S}_{P_1} G$ and $L \mathbb{LER}\mathbb{S}_{P_1} k$. Since $i \mathbb{S}_{P_1} j$, since $i \mathbb{LER}\mathbb{S}_{P_1} G$ and since G is an $\mathbb{ER}\mathbb{S}_{P_1}$-class then $j \mathbb{LER}\mathbb{S}_{P_1} G$. Since $j \mathbb{LER}\mathbb{S}_{P_1} G$ and $L \mathbb{LER}\mathbb{S}_{P_1} k$, by definition of P_1', $j \mathbb{L}_{P_1'} k$.

- Let us consider Axiom (20 - ν). Since $L \mathbb{G}\overline{\mathbb{P}}_{P_1} G$, $L \subseteq \nu \Longleftrightarrow G \subseteq \nu$, the axiom easily follows.

□

8.2.3 $\sim_\phi$ and $\sqsubseteq$

The following proposition is similar to Lemmas 8.2.2 and 8.2.3, except that it considers the order $\sqsubseteq$.

Lemma 8.2.6. *Let $P_0, P_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be such that $P_0 \sim_\phi P_1$. There exists $R \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $R \sqsubseteq P_0$, $R \sqsubseteq P_1$ and $R \sim_\phi P_0$.*

Proof. The proof is by induction on the pair $\{P_0, P_1\}$ for the $\sqsubseteq$-order. Since $\sqsubseteq$ is an order relation over a finite set, the induction is well funded.

Two cases must be considered, depending on whether $P_0 \overset{\mathbb{OESBL}}{\cong} P_1$ or not.

- Let us first suppose that $P_0 \overset{\mathbb{OESBL}}{\cong} P_1$. Since $P_0 \overset{\mathbb{OESBL}}{\cong} P_1$, either $P_0 \overset{\mathbb{M}}{\preccurlyeq} P_1$ or $P_1 \overset{\mathbb{M}}{\preccurlyeq} P_0$. Let us suppose that $P_0 \overset{\mathbb{M}}{\preccurlyeq} P_1$, the other case is symmetric. Since $P_0 \overset{\mathbb{M}}{\preccurlyeq} P_1$ and $P_0 \overset{\mathbb{OESBL}}{\cong} P_1$, $O = P_0$ satisfies the hypothesis.

- Let us now suppose that $P_0 \overset{\mathbb{OESBL}}{\ncong} P_1$. It is claimed that there exists $c \in \{0,1\}$ and a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop Q such that $Q \sqsubset P_c$ and $Q \sim_\phi P_c$. By induction on $\{Q, P_{1-c}\}$ there exists a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop O such that $O \sqsubseteq Q$, $O \sqsubseteq P_1$ and $O \sim_\phi Q$. Since $O \sqsubseteq Q$ and $Q \sqsubset P_c$, $O \sqsubset P_c$. Since $O \sim_\phi Q$ and since $P_c \sim_\phi Q$, $O \sim_\phi P_c$. Hence the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop O satisfies the condition of the property.

  Constructing Q. Two cases must be considered, depending on whether $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ or not.

  - Let us suppose that $P_0 \overset{\mathbb{OESB}}{\cong} P_1$. Since $P_0 \overset{\mathbb{OESBL}}{\ncong} P_1$ and since $P_0 \overset{\mathbb{OESB}}{\cong} P_1$, either $P_0 \overset{\mathbb{L}}{\not\prec} P_1$ or $P_1 \overset{\mathbb{L}}{\not\prec} P_0$. Let us suppose that $P_0 \overset{\mathbb{L}}{\not\prec} P_1$, the other case is similar. Since $P_0 \overset{\mathbb{OESB}}{\cong} P_1$ and $P_0 \sim_\phi P_1$, by Lemma 8.2.3, there exists $Q \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $Q \sim_\phi P_0$ and $Q \sqsubset P_0$.
  - Let us now suppose that $P_0 \overset{\mathbb{OESB}}{\ncong} P_1$. Since $P_0 \overset{\mathbb{OESB}}{\ncong} P_1$ either $P_0 \overset{\mathbb{OESB}}{\not\prec} P_1$ or $P_1 \overset{\mathbb{OESB}}{\not\prec} P_0$. Let us suppose that $P_0 \overset{\mathbb{OESB}}{\not\prec} P_1$, the other case is similar. Since $P_0 \sim_\phi P_1$, by Lemma 8.2.2, there exists $Q \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $Q \sim_\phi P_0$ and $Q \sqsubset P_0$.

□

Proposition 8.2.1 can finally be proven.

Proof. Let $O_0, O_1 \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be $\sqsubseteq$-minimal such that $O_0 \sim_\phi P$ and $O_1 \sim_\phi P$ and let us prove that $O_0 = O_1$. By Lemma 8.2.6, there exists $R \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $R \sqsubseteq O_0$, $R \sqsubseteq O_1$ and $R \sim_\phi O_0$. Since O_0 and O_1 are $\sqsubseteq$-minimal, $O_0 = R = O_1$. □

8.3 The minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$

In this section, the minimal automaton $\mathcal{A}_{\phi,\mathbb{N}}$ accepting $\overline{\phi}^{\mathbb{N}}$ is constructed. The set of states of $\mathcal{A}_{\phi,\mathbb{N}}$ is now defined.

Definition 8.3.1 ($\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$)**.** Let $\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \subseteq \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be the set of $P \in \mathbb{POP}^{m}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that, for all $Q \sqsubset P$, $Q \not\sim_\phi P$.

The transition function of $\mathcal{A}_{\phi,\mathbb{N}}$ is now introduced.

Definition 8.3.2 ($\Downarrow_\phi$, $\circ_\phi$)**.** For $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, let $\Downarrow_\phi P$ be the function which sends P to its $\sqsubset$-minimal $\sim_\phi$-equivalent $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop.
Then, for $\boldsymbol{a} \in A_b^d$, let $P \circ_\phi \boldsymbol{a} = \Downarrow_\phi (P \cdot \boldsymbol{a})$.

By Proposition 8.2.1, the function $\Downarrow_\phi$ is unambiguously defined.
The following lemma implies that $\circ_\phi$ is a transition function.

Lemma 8.3.3. *The function $\circ_\phi$ is a right-action of $\left(A_b^d\right)^*$ on $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.*

Proof. Let $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\boldsymbol{w},\boldsymbol{v} \in \left(A_b^d\right)^*$. By Proposition 8.2.1, the set $\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ contains exactly one $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop of each $\sim_\phi$-classes, hence it suffices to prove that $P \circ_\phi (\boldsymbol{w}\boldsymbol{v}) \sim_\phi (P \circ_\phi \boldsymbol{w}) \circ_\phi \boldsymbol{v}$.

By definition of $\Downarrow_\phi$, $P \circ_\phi \boldsymbol{w} \sim_\phi P \cdot \boldsymbol{w}$, hence, by Lemma 8.1.27, $\overline{(P \circ_\phi \boldsymbol{w}) \cdot \boldsymbol{v}}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}} = \overline{(P \cdot \boldsymbol{w}) \cdot \boldsymbol{v}}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$. Since $\cdot$ is a right action, $(P \cdot \boldsymbol{w}) \cdot \boldsymbol{v} = P \cdot (\boldsymbol{w}\boldsymbol{v})$.

By definition of $\Downarrow_\phi$, $(P \circ_\phi \boldsymbol{w}) \circ_\phi \boldsymbol{v} \sim_\phi (P \circ_\phi \boldsymbol{w}) \cdot \boldsymbol{v}$ and $P \cdot (\boldsymbol{w}\boldsymbol{v}) \sim_\phi P \circ_\phi (\boldsymbol{w}\boldsymbol{v})$. By transitivity:

$$P \circ_\phi (\boldsymbol{w}\boldsymbol{v}) \sim_\phi P \cdot (\boldsymbol{w}\boldsymbol{v}) = (P \cdot \boldsymbol{w}) \cdot \boldsymbol{v} \sim_\phi \left(P \circ_\phi \boldsymbol{w}\right) \cdot \boldsymbol{v} \sim_\phi (P \circ_\phi \boldsymbol{w}) \circ_\phi \boldsymbol{v}.$$

□

The preceding lemma admits the following corollary.

Corollary 8.3.4. *Let $\boldsymbol{w} \in \left(A_b^d\right)^*$, then $(\Downarrow_\phi T_{\zeta,\beta,\nu}) \circ_\phi \boldsymbol{w} = \Downarrow_\phi \textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$.*

A notation is now introduced for the set of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops which satisfy the formula ϕ.

Definition 8.3.5 ($\overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}}$)**.** Let $\overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}}$ denote the set of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops $P \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $\phi(P)$.

The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ is now constructed. It is then proven that it is minimal and accepts $\overline{\phi}^{\mathbb{N}}$.

Definition 8.3.6. Let:

$$\mathcal{A}_{\phi,\mathbb{N}} = \left(\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}, A_b^d, \circ_\phi, \Downarrow_\phi T_{\zeta,\beta,\nu}, \overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}} \cap \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}\right).$$

Theorem 8.3.7. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ is the minimal automaton which accepts $\overline{\phi}^{\mathbb{N}}$.*

Proof. The minimality follows directly from Proposition 8.2.1. Let us prove that $\mathcal{A}_{\phi,\mathbb{N}}$ accepts $\overline{\phi}^{\mathbb{N}}$. Let $\boldsymbol{n} \in \mathbb{N}^d$.

$$\begin{aligned}
\boldsymbol{n} \in \overline{\mathcal{A}_{\phi,\mathbb{N}}}^{\mathbb{N}} &\iff \Downarrow_\phi T_{\zeta,\beta,\nu} \circ_\phi \underline{\boldsymbol{n}}_{\mathbb{N}} \in \overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}} \\
&\iff \Downarrow_\phi \left(\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}\left(\underline{\boldsymbol{n}}_{\mathbb{N}}\right)\right) \in \overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}} && \text{(using Corollary 8.3.4)} \\
&\iff \text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}\left(\underline{\boldsymbol{n}}_{\mathbb{N}}\right) \in \overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_t'}} && \left(\text{using the definition of } \Downarrow_\phi\right) \\
&\iff \boldsymbol{n} \in \overline{\phi}^{\mathbb{N}} && \text{(using Lemma 7.3.32).}
\end{aligned}$$

□

Lemma 8.1.27 implies that $\Downarrow_\phi$ is a morphism of automaton from $\mathcal{A}'_{\phi,\nu}$ to $\mathcal{A}_{\phi,\mathbb{N}}$.

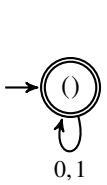
8.3.1 Examples

As in Section 7.3.3.1, the automata $\mathcal{A}_{\phi,\mathbb{N}}$ are now given for all atomic formulas ϕ considered in this part.

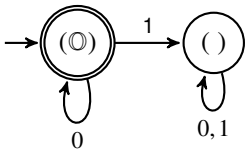
Let the basis b be equal to 2. Let the dimension d be the number of variables of the formula. Let $m = 1$ if there are no modular relation in a formula and let m be the modulus used in the formula otherwise. It is assumed in the examples that $\nu = \emptyset$.

The case of dimension $d = 1$. The automaton of Figure 8.1a is a quotient of the automata of Figure 7.6a, 7.6b and 7.6c, and it accepts the set $\mathbb{N}$.

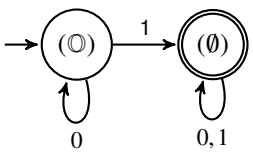
The automaton of Figure 8.1b is a quotient of the automaton of Figure 7.7, and it accepts $\{0\}$. The automaton of Figure 8.1c accepts $\mathbb{N}^{>0}$.



(a) Let ϕ be the formula True, $Label = ()$.



(b) Let ϕ be the formula $x_0 \doteq 0$, $Label = \left(\text{POSITION}_{\mathcal{V}_t'(m)}[T](0)\right)$.



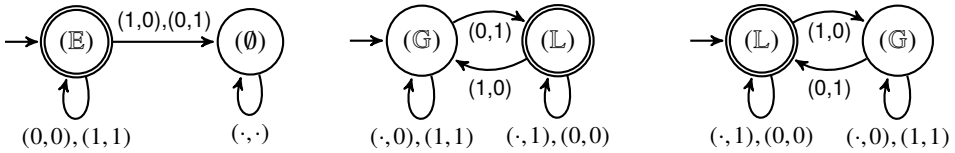
(c) Let ϕ be the formula $x_0 \not\doteq 0$, $Label = \left(\text{POSITION}_{\mathcal{V}_t'(m)}[T](0)\right)$.

Figure 8.1: Automata of dimension $d = 1$

Equality and Order. Let ϕ be the formula $x_0 \doteq x_1$ then the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ is given in Figure 7.8. It is a quotient of the automaton of Figure 7.8.

Let ϕ be the formula $x_0 < x_1$ (respectively, $x_0 \leq x_1$), then the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ is given in Figure 8.2b (respectively, Figure 8.2c). It is a quotient of the automaton of Figure 7.9a (respectively, 7.9b). The set of states and the transition function of those two automata are the same. The initial state differs.

Note that, in the automaton of Figure 8.2c, reading the word $(1, 1)$ leads to the state $(\mathbb{L})$ while 1 is not strictly less than 1. Intuitively the state $(\mathbb{E})$ should have been expected. This shows that, in some cases, $\mathbb{L}$ means "smaller" and in some other cases, $\mathbb{L}$ means "smaller or equal". The precise meaning depends on the formula ϕ and is discussed in Chapter 10.



(a) Let ϕ be the formula $x_0 \doteq x_1$. (b) Let ϕ be the formula $x_0 < x_1$. (c) Let ϕ be the formula $x_0 \leq x_1$.

Figure 8.2: $Label = \Big(\text{RELATION}_{\nu,\mathcal{V}'_t(m)}[T](0,1)\Big)$.

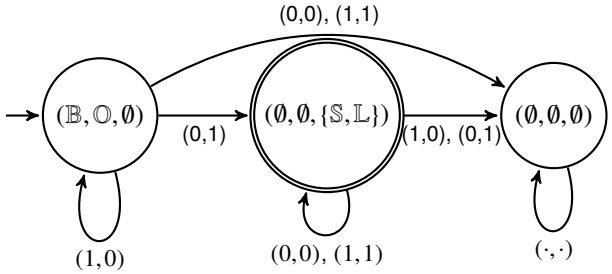


Figure 8.3: Let ϕ be the formula $x_0 + 1 \doteq x_1$, $Label = \Big(\text{POSITION}_{\mathcal{V}'_t(m)}[T](0), \text{POSITION}_{\mathcal{V}'_t(m)}[T](1), \text{RELATION}_{\nu,\mathcal{V}'_t(m)}[T](0,1)\Big)$.

A similar paradox appears in the automaton of Figure 8.4 which accepts the set defined by $x_0+1 \geq x_1$. But first, let us give the automaton $\mathcal{A}_{\phi,\mathbb{N}}$, for ϕ being the formulas $x_0 + 1 \doteq x_1$. This automaton is given in Figure 8.3. It is a quotient of the automaton of Figure 7.10.

Note that in the automaton of Figure 8.4, the letter $(0,1)$ leads to the state $(\emptyset,\emptyset,\mathbb{G})$. That is $0\mathbb{G}1$ while $0 < 1$. This is because $(0,1)^{-1}\phi$ is equal to $(5,1)^{-1}\phi$ and is different from $(1,5)^{-1}\phi$. Hence, intuitively, in this case, 0 in the 0th position should be treated as a number greater than the number 1 in the 1st position.

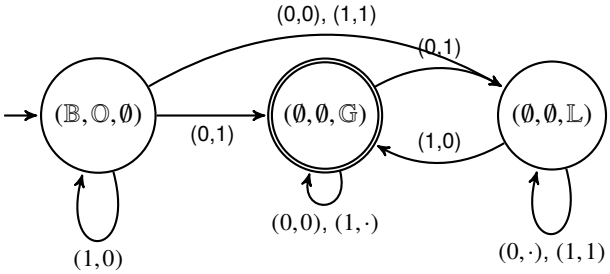


Figure 8.4: Let ϕ be the formula $x_0 + 1 \geq x_1$, $Label = \Big(\text{POSITION}_{\mathcal{V}'_t(m)}[T](0), \text{POSITION}_{\mathcal{V}'_t(m)}[T](1), \text{RELATION}_{\nu,\mathcal{V}'_t(m)}[T](0,1)\Big)$.

The modular case Let the modulus be $m = 3$, for a vocabulary with only the mod 3 predicate. Let the basis b be 5. Then the order of 2 modulo m is $\omega_{b,m} = 2$. Let ϕ be the formula $x_0 \equiv 0 \mod 3$, then $\mathcal{A}_{\phi,\mathbb{N}}$ is the automaton of Figure 8.5. It is a quotient of the automaton of Figure 7.11. For the sake of readability, the transitions by the letter 2 are omitted.

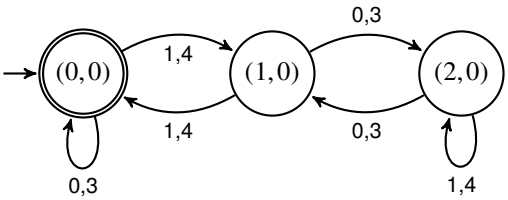


Figure 8.5: Let ϕ be the formula $x_0 \equiv 0 \mod 3$, $Label = (\textsc{modulo}_m[T]_0, \textsc{length}_{m,b}[T])$.

Chapter 9

The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$

Recall that the algorithms $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ was announced in Section 7.1. The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ takes as input an automaton $\mathcal{A}$ over A_b^d and accepts if and only if $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0[\mathcal{V}]/\nu$-definable. This algorithm is given in this chapter, in Section 9.4.

In the preceding chapter, a characterization of the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ was given. This characterization let us compute (inefficiently) the automaton $\mathcal{A}_{\phi,\mathbb{N}}$, assuming a formula ϕ was known. In this section, properties of $\mathcal{A}_{\phi,\mathbb{N}}$ are given, and those properties does not depend on the formula ϕ.

In order to introduce those properties, a set $\mathbb{A}_{\mathcal{V}_\iota'}$ of automata is introduced, it is simultaneously proven that:

- this set contains $\mathcal{A}_{\phi,\mathbb{N}}$ for $\phi \in \Sigma_0[\mathcal{V}_\iota']/\cdot,\cdot,\nu$,
- this set is closed by quotient,
- that each automaton $\mathcal{A}$ belonging to $\mathbb{A}_{\mathcal{V}_\iota'}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set, and
- it is decidable in linear time whether a minimal automaton over $\mathbb{N}$ accepts a $\Sigma_0[\mathcal{V}]/\nu$-definable set.

The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ then consists in checking whether $\mathcal{A}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota'}$, and those properties are sufficient to prove Theorem 9.4.8, which states that $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ indeed accepts the automata which accept $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable sets.

More precisely, some sets $\mathbb{A}_{\mathcal{V}_\iota',1}$, $\mathbb{A}_{\mathcal{V}_\iota',2}$, $\mathbb{A}_{\mathcal{V}_\iota',3}$, $\mathbb{A}_{\mathcal{V}_\iota',4}$, $\mathbb{A}_{\mathcal{V}_\iota',5}$ and $\mathbb{A}_{\mathcal{V}_\iota',6}$ of automata are introduced, such that $\mathbb{A}_{\mathcal{V}_\iota',6} = \mathbb{A}_{\mathcal{V}_\iota'}$. For each $i < 6$, the set $\mathbb{A}_{\mathcal{V}_\iota',i+1}$ is defined as the set of automata of $\mathbb{A}_{\mathcal{V}_\iota',i}$ which satisfy some property P_{i+1}. This sequence is necessary because properties P_{i+1} uses notions which are only defined for automata of $\mathbb{A}_{\mathcal{V}_\iota',i}$.

When $\mathbb{A}_{\mathcal{V}_\iota',i}$ is introduced:

- it is proven that, for all $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\cdot,\cdot,\nu$, the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',i}$ and
- an algorithm which decides whether a minimal automaton over $\mathbb{N}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',i+1}$ is given. This algorithm runs in time $O\left(nb^d 3^d d\right)$.
- Some properties implied by this definition are given.

A finite subset $\mathcal{L}$ of $\left(A_b^d\right)^*$ is introduced in Section 9.1, in order to restrict the study of a transition by any word $\boldsymbol{w} \in \left(A_b^d\right)^*$ to the study of words of $\mathcal{L}^*$.

The relations $\mathbb{O}_q$, $\mathbb{E}\mathbb{S}_q$, $\mathbb{L}\overline{\mathbb{S}}_q$ and $\mathbb{B}_q$ are associated to each state q in Section 9.2. Up to knowing ζ and β, it is equivalent to associating a $(\zeta, \beta, \nu, \mathcal{V}_\iota')$-pop to each state. It is then checked whether the transitions behaves as expected for $(\zeta, \beta, \nu, \mathcal{V}_\iota')$-pop.

In Section 9.3, it is shown that, given a state q, for each word $\boldsymbol{w} \in \left(A_b^d\right)^*$, there is a $\mathcal{L}$-word equivalent to $\boldsymbol{w}$. Finally, the algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ announced in this part are given in Section 9.4

9.1 New symbols

In this section, a set $\mathcal{L}$ of new *symbols* is introduced. Those symbols are intended to replace letters of A_b^d in the algorithms and in the proofs. Furthermore, the study of the right action of those symbols over $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is simpler than the right action of Definition 7.3.16.

It is assumed in the rest of the part that $b \geq 4$, because, some lemmas, such as Lemma 9.1.3, consider an A_b^d-letter $\boldsymbol{a}$ with at least 2 distinct components, a_i and a_j, for $i, j \in [d-1]$, such that $a_i > 0$ and $a_i + 1 < a_j$. If $b \leq 3$, those relations are unsatisfiable.

There is no loss of generality in assuming that $b \geq 4$, indeed, reading pairs of letters instead of letters transform any automaton $\mathcal{A}$ whose alphabet is $A_b^d = [b-1]^d$ into an automaton $\mathcal{A}'$ whose alphabet is $\alpha_{b^2}^d = \left[b^2 - 1\right]^d$, and $b^2 \geq 4$. An $\alpha_{b^2}^d$-word corresponds to an A_b^d-word of even length, but by Definition 2.3.6, the automaton $\mathcal{A}$ accepts a word $\boldsymbol{w}$ if and only if it accepts $\boldsymbol{w}\mathbf{0}$, hence it is correct to consider only the set of words of even length.

9.1.1 The set of symbols $\mathbb{P}^d$

The first set of symbols, denoted by $\mathbb{P}^d$, is now introduced. It contains the letters $\boldsymbol{a} \in A_b^d$ such that each component belongs to $\{0, 1, b-1\}$.

Definition 9.1.1 ($\mathbb{P}^d$)**.** Let $\mathbb{P}^d \subseteq A_b^d$ be the set of letters $\boldsymbol{a} \in A_b^d$ such that $a_i \in \{0, 1, b-1\}$ for all $i \in [d-1]$.

A notation for the letters of $\mathbb{P}^d$ is now introduced.

***Definition 9.1.2** ($\langle I; J\rangle$)**.** Let I, J be two disjoint subsets of $[d-1]$. Let $\langle I; J\rangle$ denote the unique letter $\boldsymbol{a} \in \mathbb{P}^d$ such that for all $i \in [d-1]$, $a_i = 1$ if $i \in I$, $a_i = b-1$ if $i \in J$, and $a_i = 0$ otherwise.

The transition by $\langle I; J\rangle$ in an arbitrary automaton over the alphabet A_b^d is straightforwardly defined since $\langle I; J\rangle \in A_b^d$. It is now shown that this transition is especially interesting over $\mathcal{A}_{\phi,\mathbb{N}}$, for this, the right-action of $\langle I; J\rangle$ over $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is now studied.

The principal difference between any letters $\boldsymbol{a}$ of A_b^d and a symbol $\langle I; J\rangle$ of $\mathbb{P}^d$ is that, for any $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, the pairs of position $(i, j) \in [d-1]$ such that ($i \ \mathbb{S}_{P\cdot\boldsymbol{a}} \ j$ holds and $i \ \mathbb{S}_P \ j$ does not hold) can be potentially any pair of positions, while the pairs $(i, j) \in [d-1]$ such that ($i \ \mathbb{S}_{P\cdot\langle I;J\rangle} \ j$ holds and $i \ \mathbb{S}_P \ j$ does not hold) are constrained such that $i \in I$ and $j \notin (I \cup J)$.

The value of $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\langle I; J\rangle)$ and the right action of $\langle I; J\rangle$ over $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ is now given. It is a straightforward application of the right-action Definition 7.3.11.

Lemma 9.1.3. *Let I, J be two disjoint subsets of $[d-1]$. Then $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\langle I; J\rangle)$ is such that, for all $i, j \in [d-1]$ with $(i \in \nu) \Longleftrightarrow (j \in \nu)$:*

- $\textsc{length}_{m,b}[\langle I;J\rangle] = 1$,
- $\textsc{modulo}_m[\langle I;J\rangle]_i = \begin{cases} 1 & \text{if } i \in I \\ (b-1) & \text{if } i \in J \\ 0 & \text{otherwise,} \end{cases}$
- $i \in \mathbb{O}_{\langle I;J\rangle}$ *if and only if* $i \notin I \cup J$,
- $i \in \mathbb{B}_{\langle I;J\rangle}$ *if and only if* $i \in J$,
- $i\ \mathbb{E}_{\langle I;J\rangle}\ j$ *if and only if* $(i \in I) \Longleftrightarrow (j \in I)$ *and* $(i \in J) \Longleftrightarrow (j \in J)$,
- $i\ \mathbb{S}_{\langle I;J\rangle}\ j$ *if and only if* $\{j \in I$ *and* $i \notin I \cup J\}$,
- $i\ \mathbb{E}\mathbb{S}_{\langle I;J\rangle}\ j$ *if and only if* $(i \in J) \Longleftrightarrow (j \in J)$.
- $i\ \mathbb{L}_{\langle I;J\rangle}\ j$ *if and only if* $\{i \notin J$ *and* $j \in J\}$ *or* $\{i \notin I \cup J$ *and* $j \in I\}$.
- $i\ \mathbb{L}\overline{\mathbb{S}}_{\langle I;J\rangle}\ j$ *if and only if* $\{i \notin J$ *and* $j \in J\}$.

Let $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ *The* $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$*-pop* $P \cdot \langle I;J\rangle$ *is equal to* $Q \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ *such that for all* $i,j \in [d-1]$*:*

- $\textsc{length}_{m,b}[Q] = \textsc{length}_{m,b}[P] + 1 \mod \omega_{b,m}$,
- $\textsc{modulo}_m[\langle I;J\rangle]_i = \begin{cases} \textsc{modulo}_m[P]_i + b^{\textsc{length}_{m,b}[P]} & \text{if } i \in I \\ \textsc{modulo}_m[P]_i + (b-1)b^{\textsc{length}_{m,b}[P]} & \text{if } i \in J \\ \textsc{modulo}_m[P]_i & \text{otherwise,} \end{cases}$
- $i \in \mathbb{O}_Q$ *if and only if* $i \in \mathbb{O}_P$ *and* $i \notin I \cup J$,
- $i \in \mathbb{B}_Q$ *if and only if* $i \in \mathbb{B}_P$ *and* $i \in J$,
- $i\ \mathbb{E}_Q\ j$ *if and only if* $i\ \mathbb{E}_P\ j$ *and* $(i \in I) \Longleftrightarrow (j \in I)$ *and* $(i \in J) \Longleftrightarrow (j \in J)$,
- $i\ \mathbb{S}_Q\ j$ *if and only if* $\{i\ \mathbb{S}_P\ j$, $(i \in I) \Longleftrightarrow (j \in I)$ *and* $(i \in J) \Longleftrightarrow (j \in J)\}$ *or* $\{i \in \mathbb{B}_P$ *and* $i \notin I \cup J$ *and* $j \in \mathbb{O}_P$ *and* $j \in I\}$,
- $i\ \mathbb{L}_Q\ j$ *if and only if* $\{i \notin J$ *and* $j \in J\}$ *or* $\{i \notin I \cup J$ *and* $j \in I\}$ *or* $\{i,j \notin I \cup J$ *and* $i\ \mathbb{L}_P\ j\}$.

Then, $P \circ_\phi \langle I;J\rangle = \Downarrow_\phi Q$.

9.1.2 The left-inverse symbols

For $J \subseteq [d-1]$, a symbol $\langle \emptyset;J\rangle^{-1}$ is introduced, which is intuitively the left-inverse of the symbol $\langle \emptyset;J\rangle$. Two definitions are given, one in term of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop and one in term of transitions in some automata. It is then shown that both definitions are equivalent over $\mathcal{A}_{\phi,\mathbb{N}}$.

Definition 9.1.4 ($\langle \emptyset;J\rangle^{-1}$)**.** Let $J \subseteq [d-1]$, let $\langle \emptyset;J\rangle^{-1}$ be the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop such that, for all $i,j \in [d-1]$ with $(i \in \nu) \Longleftrightarrow (j \in \nu)$:

- $\textsc{length}_{m,b}[Q] = -1$,
- $\textsc{modulo}_m[Q]_i$ is $-b+1 \mod m$ if $i \in J$ and is 0 otherwise,
- $i \in \mathbb{O}_Q$ if and only if $i \notin I \cup J$,

- $i \in \mathbb{B}_Q$ if and only if $i \in J$,
- $i \mathbb{E}_Q j$ if and only if $(i \in J) \Longleftrightarrow (j \in J)$,
- $i \mathbb{S}_Q j$ does not hold and
- $i \mathbb{L}_Q j$ if and only if $\{i \notin J \text{ and } j \in J\}$.

***Definition 9.1.5** ($\langle \emptyset; J\rangle^{-1}$)**.** Let $\mathcal{A}$ be an automaton of alphabet A_b^d. Let q be a state of $\mathcal{A}$. If there exists an integer $n \in \mathbb{N}^{>0}$ such that $\delta(q, \langle \emptyset; J\rangle^n) = P$, let $\delta(q, \langle \emptyset; J\rangle^{-1})$ denote $\delta(q, \langle \emptyset; J\rangle^{n-1})$.

It should be noted that if there exists $n \in \mathbb{N}^{>0}$ such that $P \cdot \langle \emptyset; J\rangle^n = P$, then there is an infinity of such n. It is trivial that the set of such n is of the form $q\mathbb{N}$ for $q \in \mathbb{N}^{>0}$. And then that for all $n, n' \in q\mathbb{N}$, the $(\zeta, \beta, \nu, \mathcal{V}_t')^m$-pop $P \cdot \langle \emptyset; J\rangle^{n-1}$ is equal to $P \cdot \langle \emptyset; J\rangle^{n'-1}$. Hence the precise value of n does not matter. Indeed, let $\mathcal{A} = (Q, A, \delta, q_0, F)$ be an automaton, and let $q \in Q$, then $\delta(q, \langle \emptyset; J\rangle^{-1})$ can also be defined as the only $q' \in Q$ such that $\delta(q', \langle \emptyset; J\rangle) = q$ and there exists $n \in \mathbb{N}$ such that $\delta(q, \langle \emptyset; J\rangle^n) = q'$.

When $d = 1$, the symbol $\langle \emptyset; \emptyset\rangle^{-1}$ is the "digit" 0^{-1} of [MS13]. It is denoted by $\langle \emptyset; J\rangle^{-1}$ because $P \cdot \langle \emptyset; J\rangle^{-1} \cdot \langle \emptyset; J\rangle = P$. Note that $P \cdot \langle \emptyset; J\rangle \cdot \langle \emptyset; J\rangle^{-1} = P$ does not hold in general. In this part, this notation is used only when $P \cdot \langle \emptyset; J\rangle^{-1}$ is defined.

The automata of Figure 7.10 and 8.5 are given in Figures 9.1 and 9.2 with the left-inverse symbols only.

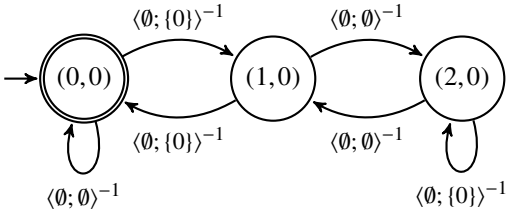


Figure 9.1: Automaton of Figures 8.5 with the inverse symbols.

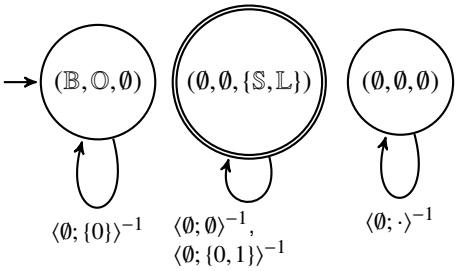


Figure 9.2: Automaton of Figures 7.10 with the inverse symbols.

In order to prove that both definitions coincide on some states, the definition of upper set is recalled.

***Definition 9.1.6** (Upper set, Lower set)**.** Let S be a set with a partial ordering relation. Then $R \subseteq S$ is an $\preccurlyeq$-upper (respectively, $\preccurlyeq$-lower) set if for all $x, y \in S$, $x \in R$ and $x \preccurlyeq y$ (respectively $y \preccurlyeq x$) imply $y \in R$.

For $x \in S$, let $\uparrow_{\preccurlyeq} x$ (respectively, $\downarrow_{\preccurlyeq} x$) denote the upper (respectively, lower) set $\{y \in S \mid x \preccurlyeq y\}$ (respectively, $\{y \in S \mid y \preccurlyeq x\}$) generated by x. It is the $\subseteq$-least upper (respectively, lower) set of S which contains x.

It is now proven that, on some states, both definitions coincides. Those states are the only one such that $\delta(q, \langle\emptyset; J\rangle^{-1})$ is considered.

Lemma 9.1.7. *Let $P \in \mathbb{POP}^{m,min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, let $J \subseteq [d-1]$ be a $\mathbb{LES}_P$-upper set which contains $\mathbb{B}_P$ and is disjoint from $\mathbb{O}_P$, then $\delta(P, \langle\emptyset; J\rangle^{-1})$ exists and is equal to $P \circ_\phi \langle\emptyset; J\rangle^{-1}$.*

Proof. Note that $\langle\emptyset; J\rangle^{-1} = \langle\emptyset; J\rangle^{\omega_{b,m} m-1}$ and that $\langle\emptyset; J\rangle^{\omega_{b,m} m}$ is such that, for all $i, j \in [d-1]$ with $(i \in \nu) \Longleftrightarrow (j \in \nu)$:

- $\textsc{length}_{m,b}\left[\langle\emptyset; J\rangle^{\omega_{b,m} m}\right] = 0$,
- $\textsc{modulo}_m\left[\langle\emptyset; J\rangle^{\omega_{b,m} m}\right]_i$ is 0
- $i \in \mathbb{O}_{\langle\emptyset;J\rangle^{\omega_{b,m} m}}$ if and only if $i \notin J$,
- $i \in \mathbb{B}_{\langle\emptyset;J\rangle^{\omega_{b,m} m}}$ if and only if $i \in J$,
- $i\ \mathbb{E}_{\langle\emptyset;J\rangle^{\omega_{b,m} m}}\ j$ if and only if $(i \in J) \Longleftrightarrow (j \in J)$,
- $i\ \mathbb{S}_{\langle\emptyset;J\rangle^{\omega_{b,m} m}}\ j$ does not hold and
- $i\ \mathbb{L}_{\langle\emptyset;J\rangle^{\omega_{b,m} m}}\ j$ if and only if $\{i \notin J \text{ and } j \in J\}$.

The hypothesis about J implies that $P \cdot \langle\emptyset; J\rangle^{\omega_{b,m} m} = P$. Having $P \in \mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and $P \cdot \langle\emptyset; J\rangle^{\omega_{b,m} m} = P$, imply $P \circ_\phi \langle\emptyset; J\rangle^{\omega_{b,m} m} = P$, that is $\delta(P, \langle\emptyset; J\rangle^{\omega_{b,m} m}) = P$, hence $\delta(P, \langle\emptyset; J\rangle^{-1}) = \delta(P, \langle\emptyset; J\rangle^{\omega_{b,m} m-1})$. It now remains to see that:

$$\begin{aligned}
\delta(P, \langle\emptyset; J\rangle^{-1}) &= \delta(P, \langle\emptyset; J\rangle^{\omega_{b,m} m-1}) \\
&= P \circ_\phi \langle\emptyset; J\rangle^{\omega_{b,m} m-1} \\
&\sim_\phi P \cdot \langle\emptyset; J\rangle^{\omega_{b,m} m-1} \\
&= P \cdot \langle\emptyset; J\rangle^{-1} \\
&\sim_\phi P \circ_\phi \langle\emptyset; J\rangle^{-1}.
\end{aligned}$$

Since each $\sim_\phi$-classes contains only one $(\zeta, \beta, \nu, \mathcal{V}'_\iota)^m$-pop of $\mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, and $\delta(P, \langle\emptyset; J\rangle^{-1}) \sim_\phi P \circ_\phi \langle\emptyset; J\rangle^{-1}$ then $\delta(P, \langle\emptyset; J\rangle^{-1}) = P \circ_\phi \langle\emptyset; J\rangle^{-1}$. □

The computation of the action of the inverse symbol is now studied.

***Lemma 9.1.8** (Computing $< \emptyset; J >$)**.** For all $J \subseteq [d-1]$, the set of actions of $\langle\emptyset; J\rangle^{-1}$ can be computed in time $O\left(n 2^d d\right)$.

Proof. The algorithm only consider cyclic states, because, in Section 7.2, it has been shown that it is enough to consider only the part of the automaton which are cyclic. The set of cyclic states is computed by Algorithm 7.2.11.

Let us prove that the computation time is $O\left(n 2^d d\right)$. For each of the 2^d sets $I \subseteq [d-1]$ considered in the loop of Line 1, the loops of Line 4 and of Line 7 are executed at most once for each of the n states. And each instructions takes at most time $O(d)$. Hence the computation time is correct. The space used is $O\left(n 2^d d\right)$ to save each transition by letters $\langle\emptyset; J\rangle^{-1}$. □

Algorithm 3: Computing the left-inverse transition.

```
for J ⊆ [d − 1] do
    Mark all cyclic states as "unvisited";
    for q a cyclic state do
        while q is marked as "unvisited" do
            Mark q as "processing";
            q := δ(q, ⟨∅; J⟩) ;
        end
        if q is marked as "processing" then
            while q is marked as "processing" do
                Add transition from δ(q, ⟨∅; J⟩) by ⟨∅; J⟩^{-1} to q;
                q := δ(q, ⟨∅; J⟩);
                Mark q as "processed";
            end
        end
    end
end
```

As announced in the beginning of the section, the first set of automata, $\mathbb{A}_{\mathcal{V}'_\iota,1}$, is now introduced. This definition asserts that some particular left-inverse symbols are defined on some states. It is then proved that $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to this set.

***Definition 9.1.9** ($\mathbb{A}_{\mathcal{V}'_\iota,1}$)**.** Let $\mathbb{A}_{\mathcal{V}'_\iota,1}$ be the set of automaton $\mathcal{A}$ over $\mathbb{N}$, as in Definition 2.3.6, such that, for each cyclic states q:

1. the automaton $\mathcal{A}_q$ is minimal and
2. for each $I, J \subseteq [d-1]$ disjoint, the state $\delta(q, \langle I; J\rangle)$ belongs to a $\langle\emptyset; J\rangle$-cycle.

Lemma 9.1.10. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota,1}$.*

Proof. By Theorem 8.3.7, the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ is a minimal automaton over $\mathbb{N}$. Let $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be a state of $\mathcal{A}_{\phi,\mathbb{N}}$, let $I, J \subseteq [d-1]$ disjoint.

Let $O = P \cdot \langle I; J\rangle$, let us prove that O satisfies the hypothesis of Lemma 9.1.7. By construction, J is a union of $\mathbb{E}\mathbb{S}_O$-equivalence classes such that $\mathbb{B}_O \subseteq J$ and J is disjoint from $\mathbb{O}_O$. Furthermore, the elements of J are $\mathbb{L}_O$-maximal. Hence the hypothesis of Lemma 9.1.7 are satisfied by O.

Since all of the hypothesis of Lemma 9.1.7 are closed under $\sqsubseteq$-decreasing, $\Downarrow_\phi O$ also satisfies those hypothesis, hence $\Downarrow_\phi O = P \circ_\phi \langle I; J\rangle$ belongs to a $\langle\emptyset; J\rangle$-cycle. □

***Lemma 9.1.11** (Deciding $\mathbb{A}_{\mathcal{V}'_\iota,1}$)**.** It is decidable in time $O\left(n3^d d\right)$ whether a minimal automaton $\mathcal{A}$ with n states belongs to $\mathbb{A}_{\mathcal{V}'_\iota,1}$.

Proof. Since $\mathcal{A}$ is assumed to be minimal, the algorithm does not check Property 1. By Lemma 2.3.7, it is decidable in time $O\left(nb^d\right)$ whether $\mathcal{A}$ satisfies definition 2.3.6.

The set of cyclic state of $\mathcal{A}$ is computed by Algorithm 7.2.11. The algorithm runs on each cyclic state q and each sets I and J disjoint. If $\delta(q, \langle I; J\rangle\langle\emptyset; J\rangle^{-1})$ is not defined for some q, I, J the algorithm rejects. Otherwise the algorithm accepts.

There are $O(n)$ cyclic states, and since I and J are disjoint, there are $O\left(d^3\right)$ values for I and J. Testing whether $\delta(q, \langle I; J\rangle\langle\emptyset; J\rangle^{-1})$ is defined takes time $O(d)$. Hence the algorithm runs in time $O\left(n3^d d\right)$. □

9.1.3 The set of symbols $\mathbb{C}^d$

The last set of symbols, $\mathbb{C}^d$, is introduced in this section.

Definition 9.1.12 ($\mathbb{C}^d$)**.** Let $\mathbb{C}^d$ be the set of words of the form $\langle I;J\rangle\langle\emptyset;J\rangle^{-1}$ for $I,J\subseteq[d-1]$ disjoint.

A notation for the letters of $\mathbb{C}^d$ is now introduced.

***Definition 9.1.13** ($[I;J]$)**.** Let I, J be two disjoint subsets of $[d-1]$. Let $[I;J]$ be the word $\langle I;J\rangle\langle\emptyset;J\rangle^{-1}$.

When $d=1$, the symbol $[0;\emptyset]$ is the "digit" g of [MS13]. By Definition 9.1.9, the transition by $[I;J]$ is defined for all cyclic states q of all automata $\mathcal{A}\in\mathbb{A}_{\mathcal{V}_\iota',1}$. By Lemma 9.1.7, for $P\in\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop $P\cdot[I;J]$ is well defined. Since $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}([I;J])=\textsc{top}^m_{\nu,\mathcal{V}_\iota'}(\langle I;J\rangle\cdot\langle\emptyset;J\rangle^{-1}$, both definition are equivalent over $\mathcal{A}_{\phi,\mathbb{N}}$. The state $\delta(q,[I;J])$ can also be defined as the unique state q' such that $\delta(q',\langle\emptyset;J\rangle)=\delta(q,\langle I;J\rangle)$ and such that there exists $n\in\mathbb{N}$ such that $\delta(q,\langle I;J\rangle\langle\emptyset;J\rangle^n)=q'$.

Intuitively, the right action of $[I;J]$ over a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop P corresponds to the right-action of an usual symbol, and then of a left-inverse. Hence this symbol is used to obtain a right-action rule which

- does not change the value of the $\textsc{length}_{m,b}$ function,
- does not change the modular values of positions belonging to J.
- In particular, the right action of $[I;J]^c$, for $c\in\mathbb{N}$, add $cb^{\textsc{length}_{m,b}[P]}$ to the modular values of positions in I.

Lemma 9.1.14. *Let I, J be two disjoint subsets of $[d-1]$. Then $\textsc{top}^m_{\nu,\mathcal{V}_\iota'}[I;J]$ is such that, for all $i,j\in[d-1]$ with $(i\in\nu)\Longleftrightarrow(j\in\nu)$:*

- $\textsc{length}_{m,b}[[I;J]]=0$,
- $\textsc{modulo}_m[[I;J]]_i$ *is* 1 *if* $i\in I$ *and is* 0 *otherwise,*
- $i\in\mathbb{O}_{[I;J]}$ *if and only if* $i\notin I\cup J$,
- $i\in\mathbb{B}_{[I;J]}$ *if and only if* $i\in J$,
- $i\ \mathbb{E}_{[I;J]}\ j$ *if and only if* $(i\in I)\Longleftrightarrow(j\in I)$ *and* $(i\in J)\Longleftrightarrow(j\in J)$,
- $i\ \mathbb{S}_{[I;J]}\ j$ *if and only if* $\{i\notin I\cup J$ *and* $j\in I\}$
- $i\ \mathbb{L}_{[I;J]}\ j$ *if and only if* $\{i\notin J$ *and* $j\in J\}$ *or* $\{i\notin I\cup J$ *and* $j\in I\}$.

Let $P\in\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop $P\cdot[I;J]$ is equal to Q such that for all $i,j\in[d-1]$:

1. $\textsc{length}_{m,b}[Q]=\textsc{length}_{m,b}[P]\mod\omega_{b,m}$,
2. $\textsc{modulo}_m[Q]_i$ *is* $\textsc{modulo}_m[P]_i+b^{\textsc{length}_{m,b}[P]}$ *if* $i\in I$ *and is* $\textsc{modulo}_m[P]_i$ *otherwise,*
3. $i\in\mathbb{B}_Q$ *if and only if* $i\in\mathbb{B}_P$ *and* $i\in J$,
4. $i\in\mathbb{O}_Q$ *if and only if* $i\in\mathbb{O}_P$ *and* $i\notin I\cup J$,
5. $i\ \mathbb{S}_Q\ j$ *if and only if* $\{i\ \mathbb{S}_P\ j$, $(i\in I)\Longleftrightarrow(j\in I)$ *and* $(i\in J)\Longleftrightarrow(j\in J)\}$ *or* $\{i\in\mathbb{B}_P$, $i\notin I\cup J$, $j\in\mathbb{O}_P$ *and* $j\in I\}$,
6. $i\ \mathbb{L}_Q\ j$ *if and only if* $\{i\notin J$ *and* $j\in J\}$, $\{i\notin I\cup J$ *and* $j\in I\}$ *or* $\{i,j\in I\cup J$ *and* $i\ \mathbb{L}_P\ j\}$,

Then, $P\circ_\phi[I;J]=\Downarrow_\phi Q$.

The main interest of those symbols concerns the modular predicates. The Figure 9.4 represents the automaton of Figure 7.11 for the formula $x_0 \equiv 0 \mod 3$, with the symbols of $\mathbb{C}^d$. The right-action of $[\{0\};\emptyset]$ on (n,m) is to increment m and the right action of $[\emptyset;\emptyset]$ is the identity action. Hence, the action of those letters seems more readable than the action of the A_b^d-letters in Automaton 7.11. Furthermore, the modulus value can be read in the length of the $[\{0\};\emptyset]$-cycles.

The automaton of Figure 7.10, which accepts the set defined by $x_0+1 \doteq x_1$ is represented in Figure 9.3 with the $\mathbb{C}^d$ letters.

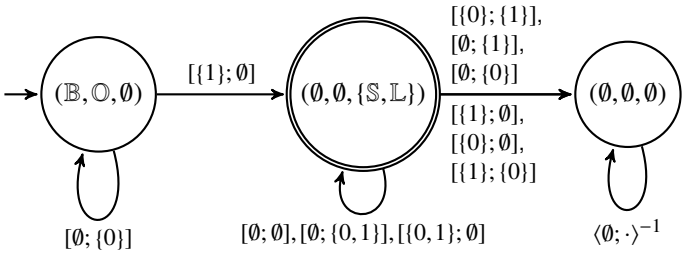


Figure 9.3: $x_0 + 1 \doteq x_1$, automaton of Figure 8.3 with the $\mathbb{C}^d$ symbols, $Label = \left(\text{POSITION}_{\mathcal{V}_\iota'(m)}[T](0), \text{POSITION}_{\mathcal{V}_\iota'(m)}[T](1), \text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[T](0,1)\right)$

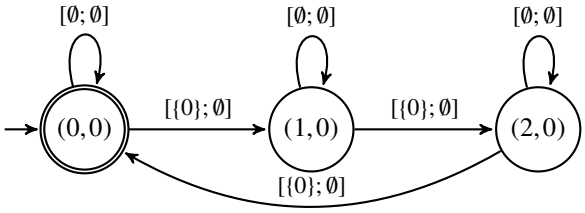


Figure 9.4: $x_0 \equiv 0 \mod 3$, automaton of Figure 8.5 with the $\mathbb{C}^d$ symbols, $Label = (\text{MODULO}_m[T]_0, \text{LENGTH}_{m,b}[T])$

9.2 Characterization of states

In this section, three properties satisfied by the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ are given. The subset $\mathbb{A}_{\mathcal{V}_\iota',5}$ of $\mathbb{A}_{\mathcal{V}_\iota',1}$, which contains the automata whose states satisfy those properties is then defined.

The two first properties, given in Section 9.2.1, are used to generalize the relations $\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{O}_P$ and $\mathbb{B}_P$ (defined on $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop P, which are states of the automaton $\mathcal{A}_{\phi,\mathbb{N}}$) to relations $\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{O}_q$ and $\mathbb{B}_q$ for any state q of any automaton of $\mathbb{A}_{\mathcal{V}_\iota',5}$.

The last property explain why it is only needed to consider symbols of $\mathcal{L}$ and not letters of A_b^d.

9.2.1 Studying loops.

In this section, it is proven that the non-modular values of the $(\zeta,\beta,\nu,\mathcal{V}_\iota')$-pop associated with a state q are precisely characterized by the symbols of $\mathbb{C}^d$ which leave the state q invariant, that is, by the sets $J \subseteq [d-1]$ such that $\delta(q,[\emptyset;J]) = q$.

In order to define the second set of automata, $\mathbb{A}_{\mathcal{V}_\iota',2}$, the following definition must be introduced.

***Definition 9.2.1** ($\mathfrak{F}^{\mathcal{A}}(q)$)**.** Let q be a cyclic state of $\mathcal{A}$. Let $\mathfrak{F}^{\mathcal{A}}(q)$ denote the set of sets $J \subseteq [d-1]$ such that $\delta(q,[\emptyset;J]) = q$.

***Lemma 9.2.2** (Computing $\mathfrak{F}^{\mathcal{A}}(q)$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,1}$ be an automaton with n states. The sets $\mathfrak{F}^{\mathcal{A}}(q)$, for all states q, are computable in time $O\left(n2^d d\right)$.

Proof. The set of cyclic states is computed by Algorithm 7.2.11. The algorithm runs on all cyclic states q and all sets $J \subseteq [d-1]$. For each state q and each set J, the algorithm computes $\mathfrak{F}^{\mathcal{A}}(q) = \{J \subseteq [d-1] \mid \delta(q,[\emptyset;J]) = q\}$. There are $O\left(2^d\right)$ values for J, there are $O(n)$ cyclic states and computing a step in the automaton takes time $O(d)$. Hence this part of the algorithm runs in time $O\left(n2^d d\right)$. □

The sets $\mathfrak{F}^{\mathcal{A}}(q)$ for q a cyclic state of $\mathcal{A}_{\phi,\mathbb{N}}$ is now characterized. More precisely, it is shown that the set of sets $J \subseteq [d-1]$ such that $P \cdot [\emptyset;J] = P$ gives some information about the $(\zeta,\beta,\nu,\mathcal{V}'_\iota)$-pop P. Hence, given some $P \in \mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, the following lemma characterizes those sets J.

Lemma 9.2.3. *Let $P \in \mathbb{POP}^{m,min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and a set $J \subseteq [d-1]$. The three following propositions are equivalent:*

1. *the equality $P \cdot [\emptyset;J] = P$ holds,*
2. *the equality $P \circ_\phi [\emptyset;J] = P$ holds,*
3. *the set J is a $\mathbb{LIRS}_P$-upper set such that $\mathbb{B}_P \subseteq J$ and $J \cap \mathbb{O}_P = \emptyset$.*

Proof. 1$\Longrightarrow$2 Since $P \in \mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $\Downarrow_\phi P = P$. Since $P \cdot [\emptyset;J] = P$:

$$\begin{array}{rcll} P \circ_\phi [\emptyset;J] & = & \Downarrow_\phi (P \cdot [\emptyset;J]) & \left(\text{using the definition of } \circ_\phi\right) \\ & = & \Downarrow_\phi P & (P \cdot [\emptyset;J] = P) \\ & = & P. & \left(\Downarrow_\phi P = P\right) \end{array}$$

2$\Longrightarrow$3 Let us suppose that $P \circ_\phi [\emptyset;J] = P$. Let $i,j \in [d-1]$. Then $i \in \mathbb{B}_P$ implies $i \in \mathbb{B}_{P\cdot[\emptyset;J]}$ and by Rule 3 of Lemma 9.1.14, i belongs to J, hence $\mathbb{B}_P \subseteq J$. Similarly, $i \in \mathbb{O}_P$ implies $i \in \mathbb{O}_{P\cdot[\emptyset;J]}$, hence by Rule 4 of Lemma 9.1.14, i does not belong to J, hence $\mathbb{O}_P \cap J = \emptyset$.

Finally, if $i \ \mathbb{LIRS}_P \ j$ then $i \ \mathbb{LIRS}_{P\cdot[\emptyset;J]} \ j$, hence by the Rule 6 of Lemma 9.1.14, either $i \notin J$ or $j \in J$.

3$\Longrightarrow$1 Let J be a $\mathbb{LIRS}_P$-upper set such that $\mathbb{B}_P \subseteq J$ and $J \cap \mathbb{O}_P = \emptyset$. The proof consists in a systematic application of the 6 rules of Lemma 9.1.14 with those hypothesis. □

The second set of automata announced in the introduction of this section, $\mathbb{A}_{\mathcal{V}'_\iota,2}$, is now introduced. It is then proved that $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to this set.

***Definition 9.2.4** ($\mathbb{A}_{\mathcal{V}'_\iota,2}$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,1}$ for all cyclic state q of $\mathcal{A}$.

The automaton $\mathcal{A}$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota,2}$ if:

1. the set $\mathfrak{F}^{\mathcal{A}}(q)$ is non-empty
2. the set $\mathfrak{F}^{\mathcal{A}}(q)$ is closed under taking union and intersection,
3. for all $\boldsymbol{a} \in A_b^d$, the state $\delta(q,s)$ is cyclic.

It should be noted that Definition 9.2.4 uses the letters of the form $[\emptyset; J]$ which are not necesserly defined for all cyclic states of all automata. This is why, only automata $\mathcal{A}$ belonging to $\mathbb{A}_{\mathcal{V}'_\iota,1}$ are considered. Indeed Definition 9.1.9 ensures that the action of these letters are correctly defined for all cyclic states.

Lemma 9.2.5. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota,2}$.*

Proof. By Lemma 9.1.10, $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota,1}$.

Let $P \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be a state of $\mathcal{A}_{\phi,\mathbb{N}}$. By Lemma 9.2.3, $\mathfrak{F}^{\mathcal{A}}(q)$ contains $\mathbb{B}_P$, hence is not empty. Note that the following sets are closed under taking union and intersection:

- the set of $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$-upper sets,
- the set of sets disjoint from $\mathbb{O}_q$ and
- the set of sets which contains $\mathbb{B}_q$.

Concerning Property 3 of Definition 9.2.4, it should be noted that, for each $\boldsymbol{a} \in A_b^d$, the $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop $P \cdot a$ belongs to $\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$. Since $P \cdot a$ belongs to $\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, as proven above $P \circ_\phi a$ is cyclic. □

***Lemma 9.2.6** (Deciding $\mathbb{A}_{\mathcal{V}'_\iota,2}$)**.** It is decidable in time $O\left(nb^d d\right)$ whether a minimal automaton with n states belongs to $\mathbb{A}_{\mathcal{V}'_\iota,2}$.

Proof. By Lemma 9.1.11, it is decidable in time $O\left(n3^d d\right)$ whether a minimal automaton belongs to $\mathbb{A}_{\mathcal{V}'_\iota,1}$, note that $b \geq 4$. An algorithm which checks properties 1 and 2 is now given.

If $\mathfrak{F}^{\mathcal{A}}(q) = \emptyset$, then the algorithm rejects. Otherwise, the algorithm runs on each J and J' in $\mathfrak{F}^{\mathcal{A}}(q)$. For each pair J and J', the algorithm checks whether $J \cup J'$ and $J \cap J'$ belongs to S, if it is not the case, the algorithm rejects.

There are $O\left(2^d\right)$ values for J and J', computing the union or intersection takes times $O(d)$, and there are $O(n)$ cyclic states. Hence this part of the algorithm runs in time $O\left(n4^d d\right)$.

An algorithm which checks Property 3 of Definition 9.2.4 is now given.

The algorithm only runs on each cyclic state q, each letter $\boldsymbol{a} \in A_b^d$. For each pair q and $\boldsymbol{a}$, the algorithm tests whether $\delta(q,a)$ is cyclic. If it is not the case the algorithm rejects.

If the algorithm has not already rejected, it accepts.

There are $O(n)$ states, $O\left(b^d\right)$ symbols and $\delta(q,s)$ is computable in time $O(d)$, hence this property is tested in time $O\left(nb^d d\right)$. □

From Lemma 9.2.3 and Definition 9.2.4, the following corollary is obtained about the sets $\mathbb{B}_q$ and $\mathbb{O}_q$ for q a state.

Corollary 9.2.7. *For $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$, for all cyclic states q of $\mathcal{A}$ there exists a $\subseteq$-smallest and a $\subseteq$-greatest subset J of $[d-1]$ such that $J \in \mathfrak{F}^{\mathcal{A}}(q)$.*

When $\mathcal{A} = \mathcal{A}_{\phi,\mathbb{N}}$, for $P \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, the smallest set J such that $P \cdot [\emptyset; J] = P$ is $\mathbb{B}_P$ and the greatest is $[d-1] \setminus \mathbb{O}_P$. By extension, the following notation is introduced.

***Definition 9.2.8** ($\mathbb{B}_q$, $\mathbb{O}_q$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$, let q be a cyclic state of $\mathcal{A}$. Then, let $\mathbb{B}_q$ be the $\subseteq$–smallest set $J \in \mathfrak{F}^{\mathcal{A}}(q)$ and $\mathbb{O}_q$ be the $\subseteq$-smallest set J such that $[d-1] \setminus J \in \mathfrak{F}^{\mathcal{A}}(q)$.

Note that, since $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$, $\mathbb{B}_q$ and $\mathbb{O}_q$ are unambiguously defined. In particular, the following equality hold:

$$\delta(q, \left[\emptyset; \mathbb{B}_q\right]) = q. \tag{9.1}$$

***Lemma 9.2.9** (Computing $\mathbb{O}_q$ and $\mathbb{B}_q$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$ with n states. The values $\mathbb{O}_q$ and $\mathbb{B}_q$ for each cyclic state q of $\mathcal{A}$ are computable in time $O\left(n2^d d\right)$.

Proof. The algorithm runs over each cyclic state q. For each q, the set $E = [d-1] \setminus \mathbb{O}_q$ and $M = \mathbb{B}_q$ are computed as the union and as the intersection of the $J \in \mathfrak{F}^{\mathcal{A}}(q)$ respectively. Then E is initialized as $\emptyset$ and M as $[d-1]$. The algorithm runs on each $J \in \mathfrak{F}^{\mathcal{A}}(q)$. For each J the algorithm sets E to $E \cup J$ and M to $M \cap J$. Finally, the algorithm sets $\mathbb{O}_q$ to $[d-1] \setminus m$.

There are $O(n)$ cyclic states q and, for each q, the cardinality of $\mathfrak{F}^{\mathcal{A}}(q)$ is $O\left(2^d\right)$. Comparing two sets takes time $O(d)$. Hence the whole algorithm runs in time $O\left(n2^d d\right)$. □

A similar process is now used to extend the definitions of $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{E}\wr\mathbb{S}_P$ and $\mathbb{L}\overline{\mathbb{S}}_P$ to $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{E}\wr\mathbb{S}_q$ and $\mathbb{L}\overline{\mathbb{S}}_q$ respectively, for any state q of any automaton of $\mathbb{A}_{\mathcal{V}'_\iota,2}$.

***Definition 9.2.10** ($i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ j$, $i\ \mathbb{E}\wr\mathbb{S}_q\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_q\ j$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$ and q a state of $\mathcal{A}$. Let $i, j \in [d-1]$, then let $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ j$ denote that for all $J \subseteq [d-1]$, if $i \in J$ and $J \in \mathfrak{F}^{\mathcal{A}}(q)$ then $j \in J$.

Then, let $i\ \mathbb{E}\wr\mathbb{S}_q\ j$ denote that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ j$ and $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ i$ and let $i\ \mathbb{L}\overline{\mathbb{S}}_q\ j$ denote that $j\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_i$ holds and not $i\ \mathbb{E}\wr\mathbb{S}_q\ j$.

It should be noted that $\mathbb{E}\wr\mathbb{S}_q$ is an equivalence relation, and that $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$ is a reflexive transitive relation. When the automaton $\mathcal{A}$ is $\mathcal{A}_{\phi,\mathbb{N}}$, the relations $\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{O}_P$ and $\mathbb{B}_P$ introduced in Definition 7.3.3 and the relations $\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{O}_q$ and $\mathbb{B}_q$ introduced in Definition 9.2.10 are equivalent, by Lemma 9.2.5, when $q = P$.

Two examples of formulas $\phi_0, \phi_1 \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, and of their minimal automata $\mathcal{A}_{\phi_0}$ and $\mathcal{A}_{\phi_1}$ are given. For each cyclic state q of $\mathcal{A}_{\phi_0}$ and $\mathcal{A}_{\phi_1}$, the values of $\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{O}_q$ and $\mathbb{B}_q$ are given.

Example 9.2.11. Consider $\nu = \emptyset$. Let ϕ_0 be the formula $x_0 + 1 \doteq x_1 \wedge x_1 + 1 \doteq x_2$. The automaton of Figure 9.5 represents the minimal automaton $\mathcal{A}_{\phi_0}$ in base 4 which accepts the set defined by ϕ. The transitions by letters of A_b^d and of $\mathbb{C}^d$ are given. The relations $\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$, $\mathbb{O}_q$ and $\mathbb{B}_q$ are given in each state as in Definitions 9.1.13 and 9.2.8.

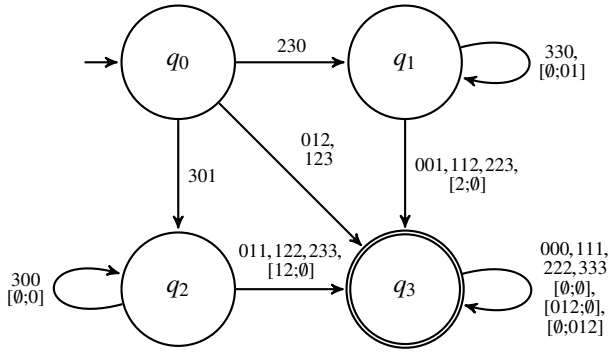
Let us consider the automata $\mathcal{A}_{q_1}$ and $\mathcal{A}_{q_2}$. They accept the sets defined by $x_0 + 1 \doteq x_1 + 1 \doteq x_2$ and $x_0 + 1 \doteq x_1 \doteq x_2$ respectively. For both of those automata, $0\ \mathbb{E}\wr\mathbb{S}_{q_3}\ 1$. More precisely, $i\ \mathbb{P}_{q_3}\ j$ if q_3 is considered as a state of $\mathcal{A}_{q_1}$, and $i\ \mathbb{S}_{q_3}\ j$ if q_3 is considered as a state of $\mathcal{A}_{q_2}$. This difference is caused by the fact that the automaton $\mathcal{A}_{q_1}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\zeta, \beta, \nu$-definable set for $\zeta = \{2\}$ and $\beta = \{0, 1\}$, while the automaton $\mathcal{A}_{q_1}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\zeta', \beta', \nu$-definable set for $\zeta' = \{1, 2\}$ and $\beta' = \{0\}$.

This shows why, the relation $\mathbb{E}\wr\mathbb{S}$ is considered in our algorithm, and not $\mathbb{E}$ and $\mathbb{S}$ separately.

Let ϕ_1 be the formula $x_0 \leq x_1 \leq x_2$. The automaton of Figure 9.6 is the minimal automaton in base 4 which accepts the set defined by ϕ_1. For the sake of readability, only transitions by symbols of the form $[\emptyset; J]$ are given. The set of words such that $\delta(q_0, w)$ is q_1 (respectively q_2, respectively q_3) is defined by the formula $x_0 \leq x_1 \wedge x_2 < x_1$ (respectively, $x_1 < x_0 \wedge x_1 \leq x_2$, respectively, $x_2 < x_1 < x_0$).

An algorithm to compute $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$, hence $\mathbb{E}\wr\mathbb{S}_q$ and $\mathbb{L}\overline{\mathbb{S}}_q$ is now given.

***Lemma 9.2.12** (Computing $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$. The relations $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$ for all cyclic states q of $\mathcal{A}$ are computable in time $O\left(nd^2 2^d\right)$.



State $q =$	q_1	q_2	q_3
$\text{POSITION}_{\mathcal{V}_\iota'(m)}[q](0)$	$\mathbb{B}$	$\mathbb{B}$	
$\text{POSITION}_{\mathcal{V}_\iota'(m)}[q](1)$	$\mathbb{B}$	$\mathbb{O}$	
$\text{POSITION}_{\mathcal{V}_\iota'(m)}[q](2)$	$\mathbb{O}$	$\mathbb{O}$	
$\text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[q](0,1)$	$\mathbb{E}\wr\mathbb{S}$	$\mathbb{G}$	$\mathbb{E}\wr\mathbb{S}$
$\text{RELATION}_{\nu,\mathcal{V}_\iota'(m)}[q](1,2)$	$\mathbb{G}$	$\mathbb{E}\wr\mathbb{S}$	$\mathbb{E}\wr\mathbb{S}$

Figure 9.5: $x_0 + 1 \doteq x_1 \wedge x_1 + 1 \doteq x_2$.

Proof. Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}_\iota',2}$ be an automaton with n states. Let q be a state of $\mathcal{A}$.

A matrix $(less_q[i,j])_{i,j\in[n-1]}$ of boolean is computed, which represents the pairs of positions (i,j) such that $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ j$. At initialization, each boolean is set to true. The algorithm runs on each $J \in \mathfrak{F}^{\mathcal{A}}(q)$. For each J, the algorithm runs on each $i \in J$ and each $j \notin J$. For each pair (i,j), the algorithm sets $less_q[i,j]$ to false.

At the end of the computation:

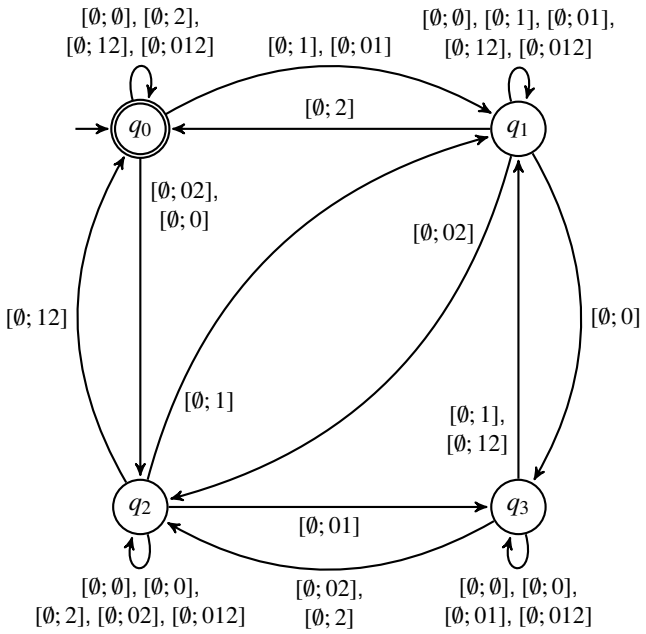
- $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ j$ holds if and only if $less_q[i,j]$ is equal to true,
- $i\ \mathbb{E}\wr\mathbb{S}_q\ j$ holds if and only if $less_q[i,j]$ and $less_q[j,i]$ are equal to true and
- $i\ \mathbb{L}\overline{\mathbb{S}}_q\ j$ holds if and only if $less_q[i,j]$ is equal to true and $less_q[j,i]$ is equal to false.

There are $O\left(2^d\right)$ values for J and $O(d)$ values for i and j, hence the total time of is $O\left(nd^2 2^d\right)$. □

A subset of $\mathbb{A}_{\mathcal{V}_\iota',2}$ is now introduced, it states that the right action by $\mathcal{L}$'s symbol over states of $\mathcal{A}$ behave similarly to their right action over $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$.

***Definition 9.2.13** ($\mathbb{A}_{\mathcal{V}_\iota',3}$)**.** Let $\mathbb{A}_{\mathcal{V}_\iota',3}$ be the set of automata $\mathcal{A} \in \mathbb{A}_{\mathcal{V}_\iota',2}$ such that, for all cyclic states q:

1. Let $J \subseteq [d-1]$ be an $\mathbb{L}_q$-upper set, containing $\mathbb{B}_q$ and disjoint from $\mathbb{O}_q$, then $J \in \mathfrak{F}^{\mathcal{A}}(q)$.
2. for all sets $I, J \subseteq [d-1]$ disjoint, for all integers $i, j \in [d-1]$, for $\boldsymbol{a}$ being $[I;J]$ or $\langle I;J\rangle$, $\delta(q,\boldsymbol{a}) \overset{\mathbb{OESBL}}{\preccurlyeq} q\cdot\langle I;J\rangle$.
3. For all $i,j \in [d-1]$ such that $i \in \nu \Longleftrightarrow j \notin \nu$, $i\ \mathbb{L}\wr\mathbb{E}_q\ j$ does not hold.
4. If $<$ does not belong to $\mathcal{V}_\iota^{\mathbb{N}}$, for all $i,j \in [d-1]$ such that $i \in \nu \Longleftrightarrow j \notin \nu$, $i\ \mathbb{L}\overline{\mathbb{S}}_q\ j$ does not hold.



State $q =$	q_0	q_1	q_2	q_3
$\textsc{relation}_{\nu,\mathcal{V}'_\iota(m)}[q](0,1)$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{G}$	$\mathbb{G}$
$\textsc{relation}_{\nu,\mathcal{V}'_\iota(m)}[q](0,2)$	$\mathbb{L}$			$\mathbb{G}$
$\textsc{relation}_{\nu,\mathcal{V}'_\iota(m)}[q](1,2)$	$\mathbb{L}$	$\mathbb{G}$	$\mathbb{L}$	$\mathbb{G}$

Figure 9.6: $x_0 \leq x_1 \leq x_2$.

It should be noted that Definition 9.2.13 uses the $\mathbb{O}_q$, $\mathbb{B}_q$, $\mathbb{BS}_q$ and $\mathbb{L}\overline{\mathbb{S}}_q$ symbols, which are not defined for all states of all automata. This is why, only automata $\mathcal{A}$ belonging to $\mathbb{A}_{\mathcal{V}'_\iota,2}$ are considered, indeed Definition 9.2.4 ensures that those symbols are defined on every cyclic states of automata in $\mathbb{A}_{\mathcal{V}'_\iota,2}$. It leads to the following definition.

***Definition 9.2.14** ($\textsc{top}_{\nu,\mathcal{V}'_\iota} q$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,3}$, let q be a state of $\mathcal{A}$. Let $\textsc{top}_{\nu,\mathcal{V}'_\iota}(q)$ be the elements of $\mathbb{PAIR}_{\nu,\mathcal{V}'_\iota}$ associated to q by $\mathbb{O}_q$, $\mathbb{BS}_q$, $\mathbb{L}_q$ and $\mathbb{B}_q$.

For $T \in \mathbb{PAIR}_{\nu,\mathcal{V}'_\iota}$, let $q \cdot T$ as in Definition 7.3.11.

Lemma 9.2.15. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota,3}$.*

Proof. By Lemma 9.2.5, the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota,2}$. Let $P \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be a state of $\mathcal{A}_{\phi,\mathbb{N}}$.

Let us first consider Condition 1. Let $J \subseteq [d-1]$ be an $\mathbb{L}_P$-upper set containing $\mathbb{B}_P$ and disjoint from $\mathbb{O}_P$. Then $P \overset{\mathbb{L}}{\sqsubseteq} P \cdot [\emptyset; J]$, and since $P \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $P \circ_\phi [\emptyset; J] = P$.

Let us now consider Condition 2, it follows from the definition of $\circ_\phi$.

Finally, Conditions 3 and 4 follows from the definition of $\textsc{top}^m_{\nu,\mathcal{V}'_\iota}$. □

***Lemma 9.2.16** (Deciding $\mathbb{A}_{\mathcal{V}'_\iota,3}$)**.** It is decidable in time $O\left(nb^d d\right)$ whether a minimal automaton with n states belongs to $\mathbb{A}_{\mathcal{V}'_\iota,3}$.

Proof. By Lemma 9.2.6, it is decidable in time $O\left(nb^d d\right)$ whether a minimal automaton belongs to $\mathbb{A}_{\mathcal{V}'_\iota,2}$. The algorithm runs over each cyclic state q and each disjoint pair of sets I and J. For each q, I and J,

the algorithm runs over $\boldsymbol{a}$ being $[I;J]$ or $\langle I;J\rangle$. For each $\boldsymbol{a}$ the algorithm checks whether $\delta(q,\boldsymbol{a}) \overset{\mathbb{OESBL}}{\not\in} q\cdot\langle I;J\rangle$, in this case the algorithm rejects.

If the algorithm has not rejected, it accepts.

There are $O(n)$ states q, $O\left(3^d\right)$ disjoint sets I and J, and computing $\delta(q,[I;J])$ and $\delta(q,\langle I;J\rangle)$ takes time $O(d)$. Checking each property takes time $O(1)$, hence this part of the algorithm runs in time $O\left(n3^d d\right)$. □

9.2.2 Studying $\mathbb{C}^d$-cycles and modular values

The preceding section deal with the symbols of the form $[\emptyset;J]$, this section considers the symbols of the form $[I;\emptyset]$ and the length of the $[I;\emptyset]$-cycles.

***Definition 9.2.17** ($\mathbb{A}_{\mathcal{V}_\iota',4}$)**.** Let $\mathbb{A}_{\mathcal{V}_\iota',4}$ be the set of automata $\mathcal{A}\in\mathbb{A}_{\mathcal{V}_\iota',3}$ such that, for all non-empty disjoint sets $I\subseteq[d-1]$, for all cyclic state q such that I is a $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$-upper-set:

1. There exists a positive integer m such that $q=\delta(q,[I;\emptyset]^m)$.

Let $\mathrm{LoopSize}(q,I)$ be the least such m.

2. $\mathrm{LoopSize}(q,I)$ is coprime with b.

Intuitively, the right action of $[I;\emptyset]$ change the order by setting I as $\mathbb{L}$-maximal position, and increment the position of I. Since I is a $\mathbb{L}$-upper set of q, the right-action by $[I;\emptyset]$ does not change the order, and since numbers are considered modulo m, the effect of the right action of $[I;\emptyset]$ on the number modulo m is canceled by $m-1$ other right-actions of the same letter. Furthermore, by hypothesis, m is coprime with b.

Example 9.2.18. In this example $\nu=\emptyset$ and the basis b is 7. Let ϕ be the formula $4x_0+6x_1\equiv 0 \mod 120$. Then, $\overline{\phi}^{\mathbb{N}}$ is accepted by an automaton $\mathcal{A}=(Q,A,\delta,q_0,F)$ with $Q=[119]$, $F=\{0\}$, $q_0=0$, and for all $i\in[119]$,

- $\delta(i,I)=i$, with $I=[\emptyset;\emptyset]$,
- $\delta(i,I)\equiv i+4 \mod 120$, with $I=[\{0\};\emptyset]$,
- $\delta(i,I)\equiv i+6 \mod 120$, with $I=[\{1\};\emptyset]$ and
- $\delta(i,I)\equiv i+10 \mod 120$ with $I=[\{01\};\emptyset]$.

A part of this automaton is shown in figure 9.7.

The automaton $\mathcal{A}$ has exactly one strongly connected component, which is $[119]$. There are two $\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{[119]}$-classes, which are $\{0\}$ and $\{1\}$. Then $\mathrm{LoopSize}([119],\{0\})=30$ and $\mathrm{LoopSize}([119],\{1\})=20$ which are coprime to 7. Then $\mathrm{LoopSize}([119],\{01\})=12$, which divides $\mathrm{lcm}(20,30)=60$.

Lemma 9.2.19. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',4}$.*

Proof. By Lemma 9.2.15, $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',3}$. Since $\phi\in\Sigma_0[\mathcal{V}_\iota']/\cdot,\cdot,\nu$, by definition of $\mathcal{V}_\iota'$, there exists $m\in\mathbb{C}_b$ such that $\phi\in\Sigma_0[\mathcal{V}_\iota'(m)]/\cdot,\cdot,\nu$.

Let I be a $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_C$-upper set, and let $P\in\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be a state of $\mathcal{A}_{\phi,\mathbb{N}}$. Let $P'_k=P\cdot[I;\emptyset]^k$ and $P_k=P\circ_\phi[I;\emptyset]^k$ for all $k\in\mathbb{N}$. By induction on $k\in\mathbb{N}$, by Lemma 9.1.14, P'_k is such that, for all $i,j\in[d-1]$,

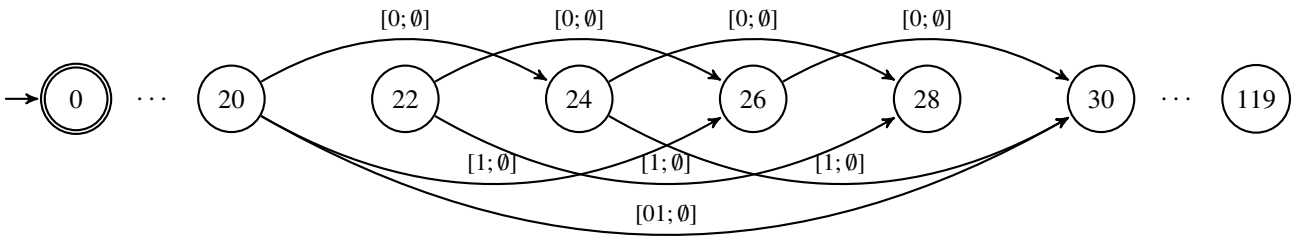


Figure 9.7: A part of the minimal automaton which accepts $x_0 \equiv 0 \mod 120$.

- $\text{LENGTH}_{m,b}\left[P'_k\right] = \text{LENGTH}_{m,b}[P]$,
- $\text{MODULO}_m\left[P'_k\right]_i$ is $\text{MODULO}_m[P]_i + b^{\text{LENGTH}_{m,b}[t]}k \mod m$ if $i \in I$ and is $\text{MODULO}_m[P]_i$ otherwise,
- $\text{POSITION}_{\mathcal{V}'_\iota(m)}\left[P'_k\right] = \text{POSITION}_{\mathcal{V}'_\iota(m)}[P]$ and
- $\text{RELATION}_{\mathcal{V},\mathcal{V}'_\iota(m)}\left[P'_k\right] = \text{RELATION}_{\mathcal{V},\mathcal{V}'_\iota(m)}[P]$.

In particular, if $k = m$, one has $\text{MODULO}_m\left[P'_m\right]_i = \text{MODULO}_m[P]_i + b^{\text{LENGTH}_{m,b}[t]}m \equiv \text{MODULO}_m[P]_i \mod m$ if $i \in [d-1] \setminus I$, and $\text{MODULO}_m[P_m]_i = \text{MODULO}_m[P]_i$ otherwise. Hence, $P'_m = P$, and then $P_m = P$. Hence Property 1 of Definition 9.2.17 is satisfied.

For all $k < m$, for all $i \in I$, $\text{MODULO}_m[P]_i + b^{\text{LENGTH}_{m,b}[t]}k \not\equiv \text{MODULO}_m[P]_i \mod m$, hence $P'_k \neq P$. Hence the length of the $[I;\emptyset]$-cycle for $\cdot$ is m. Since $\Downarrow_\phi$ sends $[I;\emptyset]$-cycle to $[I;\emptyset]$-cycle, the length of the $[I;\emptyset]$-cycle for the right-action $\circ_\phi$ divides m, hence is coprime to b. Hence Condition 2 of Definition 9.2.17 is satisfied by $\mathcal{A}_{\phi,\mathbb{N}}$. □

***Lemma 9.2.20** (Computing LoopSize(q,I))**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,3}$ be an automaton. The values LoopSize(q,I) is computable in time $O\left(n2^d d\right)$.

Proof. An algorithm which computes all LoopSize(q,I) is now given. The algorithm runs on each set $I \subseteq [d-1]$. For each I, the algorithm runs on each cyclic state q such that I is an $\mathbb{L}\mathbb{e}\mathbb{S}q$-upper-set and such that LoopSize(q,I) is not defined. The algorithm runs on each $q_i = q \cdot [I;\emptyset]^i$ for $i \in \mathbb{N}$, until q_k has already been visited. The algorithm assigns i to LoopSize(q',I) for all q' of the $[I;\emptyset]$-cycle of q.

There are $O\left(2^d\right)$ sets I and $O(n)$ states. The successor of each state by $[I;\emptyset]$ is computed in time $O(d)$. Hence this part of the algorithm runs in time $O\left(n2^d d\right)$. □

***Lemma 9.2.21** (Deciding $\mathbb{A}_{\mathcal{V}'_\iota,4}$)**.** It is decidable in time $O\left(nb^d d\right)$ whether a minimal automaton with n states belongs to $\mathbb{A}_{\mathcal{V}'_\iota,4}$.

Proof. By Lemma 9.2.16, it is decidable in time $O\left(nb^d d\right)$ whether a minimal automaton belongs to $\mathbb{A}_{\mathcal{V}'_\iota,3}$. The algorithm runs on each set $I \subseteq [d-1]$. For each I, the algorithm runs on each cyclic state q such that I is a $\mathbb{L}\mathbb{e}\mathbb{S}q$-upper-set and such that LoopSize(q,I) is not defined. The algorithm runs on each $q_i = q \cdot [I;\emptyset]^i$ for $i \in \mathbb{N}$, until q_k has already been visited. If $q_k \neq q$ or if i is not coprime to b, then the algorithm rejects.

There are $O\left(2^d\right)$ sets I and $O(n)$ states q. The successor of each state by $[I;\emptyset]$ is computed in time $O(d)$. Hence this part of the algorithm runs in time $O\left(n2^d d\right)$. □

Definition 9.2.17 admits the following straightforward lemma.

Lemma 9.2.22. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,4}$, let m be the least common multiple of all of the LoopSize(q,I)'s. Let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $I \subseteq [d-1]$. Let $n,n' > 0$ such that $n \equiv n' \mod m$. Then*

$$\delta(q,[I;\emptyset]^n) = \delta(q,[I;\emptyset]^{n'}).$$

Proof. Since $n,n' > 0$ and $n \equiv n' \mod m$, then there exists $i \in [m] \setminus \{0\}$ and $k,k' \in \mathbb{N}$ such that $n = i + km$ and $n' = i + k'm$.

Let $q' = \delta(q,[I;\emptyset]^i)$, having $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,2}$ and $\mathbb{B}_q = \emptyset$ imply that I is an $\mathbb{LRS}_{q'}$-upper set. Since I is a $\mathbb{LRS}_{q'}$-upper set, Property 1 of Definition 9.2.17 can be applied, hence $q' = \delta(q',[I;\emptyset]^m)$. It implies that $\delta(q,[I;\emptyset]^i) = \delta(q,[I;\emptyset]^{i+m})$. By an easy induction, for all k, $\delta(q,[I;\emptyset]^i) = \delta(q,[I;\emptyset]^{i+km})$. By transitivity of equality, $\delta(q,[I;\emptyset]^n) = \delta(q,[I;\emptyset]^{n'})$. □

9.3 From $\left(A_b^d\right)^*$ to $\mathcal{L}$-words

In this section, it is explained how it is possible to restrict the study of A_b^d-word to the study of $\mathcal{L}$-word. Let us recall that $\mathcal{L}$ is the set of symbols of the form $\langle I;J\rangle$ and $[I;J]$, as defined in Section 9.1. More precisely, for each cyclic state q and $\boldsymbol{w} \in \left(A_b^d\right)^*$, there exists a word $w' \in \mathcal{L}^*$ such that $\delta(q,\boldsymbol{w}) = \delta(q,w')$. Furthermore, w' only depends of $\mathbb{O}_q$, $\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w})$ and $|\boldsymbol{w}|$.

9.3.1 From A_b^d to $\mathcal{L}$-words

In this section, a set of automata $\mathbb{A}_{\mathcal{V}'_\iota,5}$ is introduced. It is such that, for each automata $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,5}$, for each cyclic state q of $\mathcal{A}$, and for each letter $\boldsymbol{a} \in A_b^d$, there exists a word $s \in \mathcal{L}^*$ such that $\delta(q,\boldsymbol{a}) = \delta(q,s)$. More precisely, the word s is constructed as a function of $\mathbb{O}_q$, and of $\boldsymbol{a}$.

Before giving Definition 9.3.4, it is reminded that, for $I \subseteq [d-1]$, the symbol $\langle I;\emptyset\rangle$ represents a letter belonging to A_b^d. Hence, $\boldsymbol{a}$ and $\langle I;\emptyset\rangle$ are d-tuples of integers. Then, $\boldsymbol{a} - \langle I;\emptyset\rangle$ is defined as the d-tuple of integers where the substraction is applied component-wise. Let $\boldsymbol{a} - I$ denote $\boldsymbol{a} - \langle I;\emptyset\rangle$. The following notation generalize this notation for A_b^d-words.

***Definition 9.3.1** ($\boldsymbol{w} - S$).* Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,5}$, let $\boldsymbol{w} \in \left(A_b^d\right)^*$ and let $S \subseteq [d-1]$ such that, for all $i \in S$, $w_i \notin 0^*$. Let $\boldsymbol{w} - S \in \left(A_b^d\right)^*$ be the only word such that:

- $|\boldsymbol{w} - S| = |\boldsymbol{w}|$ and
- $\overline{\boldsymbol{w} - S}^{\mathbb{N}} = \overline{w}^{\mathbb{N}} - \langle S;\emptyset\rangle$.

The value of $\boldsymbol{w} - S$ satisfies the inductive equation given in the following lemma whose proof is straightforward from the base b representation of integers.

Lemma 9.3.2. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,5}$, let $\boldsymbol{w} \in \left(A_b^d\right)^*$ and let $S \subseteq [d-1]$ such that, for all $i \in S$, $w_i \notin 0^*$.*

If $\boldsymbol{w} = \epsilon$, then $S = \emptyset$, hence $\boldsymbol{w} - S = \epsilon$. If $\boldsymbol{w} = \boldsymbol{a}\boldsymbol{v}$ with $\boldsymbol{a} \in A_b^d$ and $\boldsymbol{w}' \in \left(A_b^d\right)^*$, then $\boldsymbol{w} - S = \boldsymbol{a}'\boldsymbol{v}'$ where, for all i:

$$a'_i = \begin{cases} a_i & \text{if } i \notin S \\ a_i - 1 & \text{if } i \in S \text{ and } a_i > 0 \\ b-1 & \text{if } i \in S \text{ and } a_i = 0. \end{cases}$$

and $v = \boldsymbol{v} - \{i \in S \mid a_i = 0\}$.

In particular:

$$\begin{aligned} \overline{\boldsymbol{w} - S}^{\mathbb{N}} &= (\boldsymbol{a} - \{i \in S \mid a_i > 0\}) + \quad \langle \emptyset; \{i \in S \mid a_i = 0\}\rangle + b(\boldsymbol{v} - \{i \in S \mid a_i = 0\}) \\ &= (\boldsymbol{a} - \{i \in S \mid a_i > 0\}) + (b-1)\langle \{i \in S \mid a_i = 0\}; \emptyset\rangle + b(\boldsymbol{v} - \{i \in S \mid a_i = 0\}) \end{aligned}$$

Before giving the definition of $\mathbb{A}_{\mathcal{V}'_\iota,5}$, another notation must be given.

***Definition 9.3.3** ($\mathfrak{S}_{\mathcal{A}}(q,\boldsymbol{a})$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,4}$, let q be a state of $\mathcal{A}$ and let $\boldsymbol{a} \in \left(A_b^d\right)^*$.

Let $\mathfrak{S}_{\mathcal{A}}(q,\boldsymbol{a})$ be the set of sets $S \subseteq [d-1]$ such that:

1. for all $i \in S$, $a_i \notin 0^*$,
2. if $i \mathbb{E}_q j$ and $a_i = a_j$ then $(i \in S) \Longleftrightarrow (j \in S)$,
3. if $i \in S$ and $j \notin S$ and $a_i = a_j$ then $i \mathbb{G}_q j$ does not hold,
4. the set S is disjoint from $\mathbb{B}_{q\cdot\boldsymbol{a}}$ and
5. if $\mathbb{O}_{q\cdot\boldsymbol{a}} \subsetneq \mathbb{O}_q$, then S is a superset of $\mathbb{O}_q \setminus \mathbb{O}_{q\cdot\boldsymbol{a}}$ and is disjoint from $\mathbb{B}_q$.

The definition of $\mathbb{A}_{\mathcal{V}'_\iota,5}$ is now given.

***Definition 9.3.4** ($\mathbb{A}_{\mathcal{V}'_\iota,5}$)**.** Let $\boldsymbol{a} \in A_b^d$, q be a cyclic state, and $S \in \mathfrak{S}_{\mathcal{A}}(q,\boldsymbol{a})$. Let $\boldsymbol{a'}$ denote $S - \boldsymbol{a}$.

Let $\mathbb{A}_{\mathcal{V}'_\iota,5}$ be the set of automata $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,4}$ such that for each letter $\boldsymbol{a} \in A_b^d$, each cyclic state $q \in Q$ and each set $S \in \mathfrak{S}_{\mathcal{A}}(q,\boldsymbol{a})$, $\delta(q,\boldsymbol{a})$ is equal to $\delta(q, \left[s; \mathbb{B}_{q\cdot\boldsymbol{a}}\right]\boldsymbol{a'})$.

Intuitively, the right-action of $\boldsymbol{a}$ is decomposed in two successive right-actions. In the definition of $\delta(q,\boldsymbol{a})$, some position $i \in [d-1]$ are increased by a_i, while, in the definition of $\delta(q, \left[s; \mathbb{B}_{q\cdot\boldsymbol{a}}\right]\boldsymbol{a'})$, the value at position i is first incremented and then is increased by $a_i - 1$. The intuition for the conditions are now given.

The purpose of each of the 5 conditions of Definition 9.3.3 is the following:

- Condition 1 ensures that if $i \in I$ then $a_i - 1 \geq 0$. This inequality ensures that $\boldsymbol{a'} \in A_b^d$. It also ensures that that $\mathbb{O}_{\delta(q,\boldsymbol{a})} = \mathbb{O}_{\delta(q,[s;\mathbb{B}_{q\cdot\boldsymbol{a}}]\boldsymbol{a'})}$.
- Condition 2 ensures that $\mathbb{E}_{\delta(q,\boldsymbol{a})}$ is equal to $\mathbb{E}_{\delta(q,[s;\mathbb{B}_{q\cdot\boldsymbol{a}}]\boldsymbol{a'})}$.
- Condition 3 ensures that $\mathbb{L}_{\delta(q,\boldsymbol{a})}$ is a superset of $\mathbb{L}_{\delta(q,[s;\mathbb{B}_{q\cdot\boldsymbol{a}}]\boldsymbol{a'})}$.
- Condition 4 ensures that $\mathbb{B}_{\delta(q,\boldsymbol{a})} = \mathbb{B}_{\delta(q,[s;\mathbb{B}_{q\cdot\boldsymbol{a}}]\boldsymbol{a'})}$.
- Condition 5 ensures that the successor constraints which belong to $\delta(q,\boldsymbol{a})$ and not to q also belongs to $\delta(q, \left[I; \mathbb{B}_{\delta(q,\boldsymbol{a})}\right])$.

It should be noted that if $S \neq \emptyset$, then $\sum_{i=0}^{d-1} a'_i < \sum_{i=0}^{d-1} a_i$. This relation is used to generate by induction on $\sum_{i=0}^{d-1} a_i$, from any letter $\boldsymbol{a} \in A_b^d$, a word $w \in \mathcal{L}^*$ equivalent to $\boldsymbol{a}$.

Some examples of application of this lemma are now given, resuming Example 7.3.13. Those examples shows sequence of applications of Definition 9.3.4 for different states and letters. It is also an example of how to transform a letter of A_b^d into a word in $\mathcal{L}^*$ which have the same effect. The transformation is given in Proposition 9.3.10 in full generality.

Example 9.3.5. Consider the dimension d be 7, let ν be $\{0,1,2,3\}$. Let the base b be 4. Let the modulus be $m = 5$. Then the order of b modulo m is $\omega_{b,m} = 2$.

Let T_2 and T_3 be the $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pops of Example 7.3.13, let $\boldsymbol{a} = (0,1,2,3,0,0,3)$ as in Example 7.3.13. It is recalled that $T_2 \circ_\phi \boldsymbol{a} = T_3$.

In order to use Definition 9.3.4, a sets $S \subseteq [6]$ must be chosen, which satisfies the 5 conditions of the definition. Then in particular:

- By Condition 1, S does not contain 0, 4 and 5,

- by Condition 4, S is disjoint from $\mathbb{B}_{T_3} = \{3\}$,
- by Condition 5, since $\mathbb{O}_{T_2} \setminus \mathbb{O}_{T_3} = \{2,6\}$ is not empty, then S contains $\{2,6\}$,

Let S be $\{2,6\}$. It satisfies the three preceding conditions, and furthermore, $a_0 = a_4 = a_5 = 0$, and neither 1 nor 3 is $\mathbb{L}_O$-smaller than 2 or 6 and S is an $\mathbb{E}\mathbb{S}_{\delta(q,\boldsymbol{a})} \cap \mathbb{E}\mathbb{S}_q$-classes, then it satisfies Condition 3.

Then the 6-tuple $\boldsymbol{a}'$, as in the definition, is $\boldsymbol{a} - \langle \{2,6\}; \emptyset \rangle = (0,1,1,3,0,0,2)$. Let $P_4 = T_2 \circ_\phi [\{2,6\}; \{3\}]$, it is represented in Table 9.1. Furthermore, $T_3 = P_4 \circ_\phi \boldsymbol{a}'$.

Let us now consider a succession of application of Definition 9.3.4 with the $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-pop represented in Table 9.1. The difference between a $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-pop and its predecessor is written in color.

$$
\begin{array}{lllllllllllllll}
T_2 & & & & & & & & & & & \xrightarrow{(0,1,2,3,0,0,3)} & T_3 & \xrightarrow{[\emptyset;\emptyset]} & T_3 \\
T_2 & \xrightarrow{[\{2,6\};\{3\}]} & P_4 & & & & & & & & & \xrightarrow{(0,1,1,3,0,0,2)} & T_3 & \xrightarrow{[\emptyset;\emptyset]} & T_3 \\
T_2 & \xrightarrow{[\{2,6\};\{3\}]} & P_4 & \xrightarrow{[\{6\};\{3\}]} & P_5 & & & & & & & \xrightarrow{(0,1,1,3,0,0,1)} & T_3 & \xrightarrow{[\emptyset;\emptyset]} & T_3 \\
T_2 & \xrightarrow{[\{2,6\};\{3\}]} & P_4 & \xrightarrow{[\{6\};\{3\}]} & P_5 & \xrightarrow{[\{6\};\{3\}]} & P_6 & & & & & \xrightarrow{(0,1,1,3,0,0,0)} & T_3 & \xrightarrow{[\emptyset;\emptyset]} & T_3 \\
T_2 & \xrightarrow{[\{2,6\};\{3\}]} & P_4 & \xrightarrow{[\{6\};\{3\}]} & P_5 & \xrightarrow{[\{6\};\{3\}]} & P_6 & \xrightarrow{[\{1,2\};\{3\}]} & P_7 & \xrightarrow{(0,0,0,3,0,0,0)} & T_3 & \xrightarrow{[\emptyset;\emptyset]} & T_3 \\
T_2 & \xrightarrow{[\{2,6\};\{3\}]} & P_4 & \xrightarrow{[\{6\};\{3\}]} & P_5 & \xrightarrow{[\{6\};\{3\}]} & P_6 & \xrightarrow{[\{1,2\};\{3\}]} & P_7 & \xrightarrow{[\emptyset;\{3\}]} & T_3 & \xrightarrow{[\emptyset;\emptyset]} & T_3 &
\end{array}
$$

It is now proven that $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',5}$.

Lemma 9.3.6. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',5}$.*

The following proof easily follows from Lemma 9.1.14 and Definitions 7.3.11 and 9.3.4.

Proof. By Lemma 9.2.19, the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota',4}$.

Let $P \in \mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it is a state of $\mathcal{A}_{\phi,\mathbb{N}}$. Let $\boldsymbol{a} \in A_b^d$. Let $S \in \mathfrak{S}_{\mathcal{A}}(P, \boldsymbol{w})$. Let $\boldsymbol{a}'$ as in Definition 9.3.4. Let $R = P \cdot \boldsymbol{a}$, $Q' = P \cdot [S; \mathbb{B}_R]$ and $R' = Q' \cdot \boldsymbol{a}'$. Let us claim that $R' \overset{\mathbb{L}}{\sqsubseteq} R$, by definition of $\mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it implies that $R' \sim_\phi R$, hence $\Downarrow_\phi R' \sim_\phi \Downarrow_\phi R$. Hence the lemma holds.

Let us prove that $R \overset{\mathbb{L}}{\sqsubseteq} R'$. Let $i, j \in [d-1]$.

- Let us consider $\textsc{length}_{m,b}$.

$$\textsc{length}_{m,b}[R] = \textsc{length}_{m,b}[P] + 1 = \textsc{length}_{m,b}[Q'] + 1 = \textsc{length}_{m,b}[R'] + 1$$

- Let us consider $\textsc{modulo}_m$. Two cases must be considered, depending on whether $i \in S$ or $i \notin S$.

  If $i \in S$, then:

$$
\begin{aligned}
\textsc{modulo}_m[R]_i &= \textsc{modulo}_m[P]_i + a_i b^{\textsc{length}_{m,b}[P]} && \text{(using the definition of } R\text{)} \\
&= \textsc{modulo}_m[P]_i + (a_i' + 1) b^{\textsc{length}_{m,b}[P]} && \text{(using the definition of } \boldsymbol{a}'\text{)} \\
&= \textsc{modulo}_m[Q']_i + a_i' b^{\textsc{length}_{m,b}[P]} && \text{(using the definition of } Q'\text{)} \\
&= \textsc{modulo}_m[R']_i && \text{(using the definition of } R'\text{)}
\end{aligned}
$$

  Otherwise, if $i \notin S$:

$$
\begin{aligned}
\textsc{modulo}_m[R']_i &= \textsc{modulo}_m[P]_i + a_i b^{\textsc{length}_{m,b}[P]} && \text{(using the definition of } R'\text{)} \\
&= \textsc{modulo}_m[P]_i + a_i' b^{\textsc{length}_{m,b}[P]} && \text{(using the definition of } \boldsymbol{a}'\text{)} \\
&= \textsc{modulo}_m[Q']_i + a_i' b^{\textsc{length}_{m,b}[Q']} && \text{(using the definition of } Q'\text{)} \\
&= \textsc{modulo}_m[R']_i && \text{(using the definition of } R\text{)}
\end{aligned}
$$

0		$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{L}$			
0		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{S},\mathbb{L}$	$\mathbb{E}$			
1		$\mathbb{G}$	$\mathbb{P},\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$			
0, 0, $\mathbb{B}$,		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$	$\mathbb{E}$			
0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$
0						$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$
1						$\mathbb{G}$	$\mathbb{G}$	$\mathbb{E}$

(a) P_4 equal to $T_2 \circ_\phi [\{2,6\};\{3\}]$

0		$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{L}$			
0		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{S},\mathbb{L}$	$\mathbb{E}$			
1		$\mathbb{G}$	$\mathbb{P},\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$			
0, 0, $\mathbb{B}$,		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$	$\mathbb{E}$			
0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$
0						$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$
2						$\mathbb{G}$	$\mathbb{G}$	$\mathbb{E}$

(b) P_5 equal to $P_4 \circ_\phi [\{6\};\{3\}]$

0		$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{L}$			
0		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{S},\mathbb{L}$	$\mathbb{E}$			
1		$\mathbb{G}$	$\mathbb{P},\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$			
0, 0, $\mathbb{B}$,		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$	$\mathbb{E}$			
0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$
0						$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$
3						$\mathbb{G}$	$\mathbb{G}$	$\mathbb{E}$

(c) P_6 equal to $P_5 \circ_\phi [\{6\};\{3\}]$

0		$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{L}$			
1		$\mathbb{G}$	$\mathbb{E}$	$\mathbb{S},\mathbb{L}$	$\mathbb{G}$			
2		$\mathbb{G}$	$\mathbb{P},\mathbb{G}$	$\mathbb{E}$	$\mathbb{G}$			
0, 0, $\mathbb{B}$,		$\mathbb{G}$	$\mathbb{L}$	$\mathbb{L}$	$\mathbb{E}$			
0	$\mathbb{O}$					$\mathbb{E}$	$\mathbb{L}$	$\mathbb{L}$
0						$\mathbb{G}$	$\mathbb{E}$	$\mathbb{L}$
3						$\mathbb{G}$	$\mathbb{G}$	$\mathbb{E}$

(d) P_7 equal to $P_6 \circ_\phi [\{1,2\};\{3\}]$

Table 9.1: $(\zeta,\beta,\nu,\mathcal{V}_t')^m$-pops of Example 9.3.5

- Let us prove that $i \in \mathbb{O}_R \Longleftrightarrow i \in \mathbb{O}_{R'}$.

$$
\begin{aligned}
i \in \mathbb{O}_R &\Longleftrightarrow i \in \mathbb{O}_P \ \wedge a_i = 0 && \text{(using the definition of } R\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_P \ \wedge a_i = 0 \wedge i \notin S && \text{(using the definition of } S\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_{Q'} \wedge a_i = 0 \wedge i \notin S && \text{(using the definition of } Q'\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_{Q'} \wedge a_i' = 0 \wedge i \notin S && \text{(using the definition of } \boldsymbol{a'}\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_{Q'} \wedge a_i' = 0 && \text{(using the definition of } S\text{)}\\
&\Longleftrightarrow i \in \mathbb{O}_{R'} && \text{(using the definition of } R'\text{)}
\end{aligned}
$$

- Let us prove that $i \in \mathbb{B}_R \Longleftrightarrow i \in \mathbb{B}_{R'}$.

$$\begin{array}{lll}
i \in \mathbb{B}_R \Longleftrightarrow i \in \mathbb{B}_R & \wedge i \notin S & \text{(using Condition 4)} \\
\Longleftrightarrow i \in \mathbb{B}_P \wedge a_i = b-1 & \wedge i \notin S & \text{(using the definition of } R\text{)} \\
\Longleftrightarrow i \in \mathbb{B}_{Q'} \wedge a_i = b-1 & \wedge i \notin S & \text{(using the definition of } Q'\text{)} \\
\Longleftrightarrow i \in \mathbb{B}_{Q'} \wedge a'_i = 0 & & \text{(using the definition of } \boldsymbol{a'}\text{)} \\
\Longleftrightarrow i \in \mathbb{B}_{R'} & & \text{(using the definition of } R'\text{)}
\end{array}$$

- Let us prove the equivalence between $i \mathbb{E}_R j$ and $i \mathbb{E}_{R'} j$.

$$\begin{array}{lll}
i \mathbb{E}_R j & \Longleftrightarrow & i \mathbb{E}_P j \wedge a_i = a_j \qquad \text{(using the definition of } R\text{)} \\
& \Longleftrightarrow & i \mathbb{E}_P j \wedge a_i = a_j \wedge ((i \in S) \Longleftrightarrow (j \in S)) \qquad \text{(using Condition 2)} \\
& \Longleftrightarrow & i \mathbb{E}_P j \wedge a'_i = a'_j \wedge ((i \in S) \Longleftrightarrow (j \in S)) \qquad \text{(using the definition of } a'\text{)} \\
& \Longleftrightarrow & i \mathbb{E}_{Q'} j \wedge a'_i = a'_j \qquad \text{(using the definition of } Q'\text{)} \\
& \Longleftrightarrow & i \mathbb{E}_{R'} j \qquad \text{(using the definition of } R'\text{)}
\end{array}$$

- Let us consider $\mathbb{S}$. Let us first assume that $i \mathbb{S}_R j$ and let us prove that $i \mathbb{S}_{R'} j$. By the Definition of R, either ($i \in \mathbb{B}_P$, $j \in \mathbb{O}_P$ and $a_i + 1 = a_j$) or ($i \mathbb{S}_P j$ and $a_i = a_j$), both cases are studied separately.
  - Let us first suppose that $i \in \mathbb{B}_P$, $j \in \mathbb{O}_P$ and $a_i + 1 = a_j$. Since $i \mathbb{S}_R j$, $j \notin \mathbb{O}_R$. Since $i \in \mathbb{O}_P \setminus \mathbb{O}_R$, by Condition 5, $\mathbb{O}_P \setminus \mathbb{O}_R$ is not empty, hence Condition 5 can be applied. Since $j \in \mathbb{O}_P \setminus \mathbb{O}_R$, then $j \in S$ and since $i \in \mathbb{B}_P$, then $i \notin S$. Since $j \in S$, $i \notin S$ and $a_i + 1 = a_j$ then $a'_i = a'_j$. Since $j \in \mathbb{O}_P$, $i \in \mathbb{B}_P$, $i \in S$ and $j \notin S$ then $i \mathbb{S}_{Q'} j$. Since $i \mathbb{S}_{Q'} j$ and $a'_i = a'_j$ then $i \mathbb{S}_{R'} j$.
  - Now, let us suppose that $i \mathbb{S}_P j$ and that $a_i = a_j$. Since $i \mathbb{S}_P j$ and $a_i = a_j$, by Condition 3, $(i \in S) \Longleftrightarrow (j \in S)$. Since $i \mathbb{S}_P j$ and $(i \in S) \Longleftrightarrow (j \in S)$, by definition of Q', $i \mathbb{S}_{Q'} j$. Since $a_i = a_j$ and $(i \in S) \Longleftrightarrow (j \in S)$, by definition of $\boldsymbol{a'}$, $a'_i = a'_j$. Since $i \mathbb{S}_{Q'} j$ and $a'_i = a'_j$, by definition of R', then $i \mathbb{S}_{R'} j$.

  Let us now assume that $i \mathbb{S}_{R'} j$ and let us prove that $i \mathbb{S}_R j$. Since $i \mathbb{S}_{R'} j$, then either ($i \in \mathbb{B}_{Q'}$, $j \in \mathbb{O}_{Q'}$ and $a'_i + 1 = a'_j$) or ($i \mathbb{S}_{Q'} j$ and $a'_i = a'_j$), both cases are studied separately.
  - Let us suppose that $i \in \mathbb{B}_{Q'}$, $j \in \mathbb{O}_{Q'}$ and $a'_i + 1 = a'_j$. Since $j \in \mathbb{O}_{Q'}$, by definition of Q', then $j \in \mathbb{O}_P$ and $j \notin S$. Since $i \mathbb{S}_{R'} j$ then $j \notin \mathbb{O}_{R'}$, and it is proven above that it implies that $j \notin \mathbb{O}_R$. Since $j \in \mathbb{O}_P \setminus \mathbb{O}_R$ then $\mathbb{O}_P \setminus \mathbb{O}_R$ is not empty, hence Condition 5 can be used. Since $j \in \mathbb{O}_P \setminus \mathbb{O}_R$, by Condition 5, $j \in S$, which is a contradiction.
  - Now, let us suppose that $i \mathbb{S}_{Q'} j$ and $a'_i = a'_j$. Since $i \mathbb{S}_{Q'} j$, by definition of Q', either ($i \in \mathbb{B}_P$, $j \in \mathbb{O}_P$, $i \notin S$ and $j \in S$) or ($i \mathbb{S}_P j$ and $(i \in S) \Longleftrightarrow (j \in S)$), the two cases are studied separately.
    - Let us suppose that $j \in \mathbb{O}_P$, $i \in \mathbb{B}_P$, $i \notin S$ and $j \in S$. Having $i \notin S$, $j \in S$ and $a'_i = a'_j$ imply $a_i + 1 = a_j$. Since $j \in \mathbb{O}_P$, $i \in \mathbb{B}_P$ and $a_i + 1 = a_j$, by definition of R, $i \mathbb{S}_R j$ holds.
    - Now, let us suppose that $i \mathbb{S}_P j$ and $(i \in S) \Longleftrightarrow (j \in S)$. Having $a'_i = a'_j$ and $(i \in S) \Longleftrightarrow (j \in S)$ imply $a_i = a_j$. Since $a_i = a_j$ and $i \mathbb{S}_P j$, by definition of R, $i \mathbb{S}_R j$ holds.
- Finally, let us prove that $i \mathbb{L}_R j$ implies $i \mathbb{L}_{R'} j$.

  Let us assume that $i \mathbb{L}_R j$ and let us prove that $i \mathbb{L}_{R'} j$. Since $i \mathbb{L}_R j$, by definition of R, either $a_i < a_j$ or ($i \mathbb{L}_P j$ and $a_i = a_j$), both cases are studied separately.

– Let us first assume that $a_i < a_j$. Two cases must be considered, depending on whether ($j \in S$, $i \notin J$ and $a_i + 1 = a_j$) or not.
  * Let us suppose that $j \in S$, $i \notin J$ and $a_i + 1 = a_j$, hence $a'_i = a'_j$. Since $j \in S$, $i \notin J$, by definition of Q', then $i \mathbb{L}_{Q'} j$. Since $i \mathbb{L}_{Q'} j$ and $a'_i = a'_j$, by definition of R', then $i \mathbb{L}_{R'} j$.
  * Let us suppose that $j \notin S$ or $i \in J$ or $a_i + 1 < a_j$, hence $a'_i < a'_j$ and then, by definition of R', $i \mathbb{L}_{R'} j$.
– Let us assume now that $i \mathbb{L}_P j$ and $a_i = a_j$. Two cases must be considered, depending on whether $(i \in I) \Longleftrightarrow (j \in I)$ or not.
  * Let us suppose first that $(i \in I) \Longleftrightarrow (j \in I)$. Since $i \mathbb{L}_P j$ and $(i \in I) \Longleftrightarrow (j \in I)$, by definition of Q', $i \mathbb{L}_{Q'} j$. Since $a_i = a_j$ and $(i \in I) \Longleftrightarrow (j \in I)$, by definition of $\boldsymbol{a}'$, $a'_i = a'_j$. Since $i \mathbb{L}_{Q'} j$ and $a'_i = a'_j$, by definition of R', $i \mathbb{L}_{R'} j$.
  * By Condition 3, $i \notin S$ and $j \in S$ does not hold. Let us now suppose that $i \in S$ an $j \notin S$. Since $a_i = a_j$, $i \in S$ $j \notin S$, and $S \in \mathfrak{S}_{\mathcal{A}}(q, \boldsymbol{a})$, by definition of $\mathfrak{S}_{\mathcal{A}}(q, \boldsymbol{a})$, $a'_i < a'_j$. Since $a'_i < a'_j$ by definition of R', $i \mathbb{L}_{R'} j$.

□

***Lemma 9.3.7** (Deciding $\mathbb{A}_{\mathcal{V}'_\iota,5}$)**.** It is decidable in time $O\left(nb^d 3^d d\right)$ whether a minimal automaton belongs to $\mathbb{A}_{\mathcal{V}'_\iota,5}$.

Proof. By Lemma 9.2.21, it is decidable in time $O\left(nb^d d\right)$ whether a minimal automaton belongs to $\mathbb{A}_{\mathcal{V}'_\iota,4}$. The algorithm runs on each cyclic states q, each letter $\boldsymbol{a} \in A_b^d$ and each $I \subseteq [d-1]$. For each q, $\boldsymbol{a}$ and I, if the conditions of Definition 9.3.4 are satisfied and $q' \neq q''$, the algorithm rejects.

If the algorithm has not rejected, then the algorithm accepts.

There are $O(n)$ cyclic state, $O\left(b^d\right)$ letters and $O\left(3^d\right)$ sets, and testing the conditions and the equality can be done in time $O(d)$. Hence the algorithm runs in time $O\left(nb^d 3^d d\right)$. □

Two other notations are needed before stating the main proposition of this section. The notation $\mathbb{O}_{\boldsymbol{w}}$, of sets of position belonging to 0^* was introduced in Section 7.3.1.1. This notion is now extended in order to design the set of positions equal to any integer $f \in \mathbb{N}$.

Notation 9.3.8 ($(f)_{\boldsymbol{w}}$)**.** Let $f \in \mathbb{N}$ and $\boldsymbol{w} \in \left(A_b^d\right)^*$. Let $(f)_{\boldsymbol{w}}$ denote $\left\{i \in [d-1] \mid \overline{\boldsymbol{w}_i}^{\mathbb{N}} = f\right\}$.

The set of positions which belongs to $\mathbb{O}_q$ and not to $\mathbb{O}_{q \cdot \boldsymbol{w}}$, for a state q and a word $\boldsymbol{w}$, is considered in the following proposition. Let us introduce a notation for this set.

Definition 9.3.9. Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,5}$, q a state of $\mathcal{A}$ and $\boldsymbol{w}$ a word. Let $\mathbb{O}_{q \setminus w}$ denote $\mathbb{O}_q \setminus \mathbb{O}_{q \cdot w}$.

It is straightforward from the definition of $\cdot$ that $\mathbb{O}_{q \setminus w}$ is equivalently defined as $\mathbb{O}_q \setminus \mathbb{O}_w$.

The main proposition of the section is now stated.

Proposition 9.3.10. Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,5}$, let $\boldsymbol{a} \in A_b^d$, let q be a cyclic state of $\mathcal{A}$, let $q' = \delta(q, \boldsymbol{a})$. Then $q' = \delta(q, w)$ where:

$$w = \left[\mathbb{O}_{q \setminus \boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a} - \mathbb{O}_{q \setminus \boldsymbol{a}}}\right] \Pi_{f=1}^{b-2} \left[(f)_{\boldsymbol{a} - \mathbb{O}_{q \setminus \boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a} - \mathbb{O}_{q \setminus \boldsymbol{a}}}\right]^f \left\langle \emptyset; \mathbb{B}_{\boldsymbol{a} - \mathbb{O}_{q \setminus \boldsymbol{a}}} \right\rangle.$$

Note that $\mathbb{B}_{\boldsymbol{a} - \mathbb{O}_{q \setminus \boldsymbol{a}}} = (b-1)_{\boldsymbol{a} - \mathbb{O}_{q \setminus \boldsymbol{a}}}$.

An example of application of this proposition is now given, resuming Example 9.3.5.

Example 9.3.11. Let P_2 be the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop of Example 7.3.13, let let $\boldsymbol{a} = (0,1,2,3,0,0,3)$ as in Example 9.3.5. Then $O = P_2 \circ_\phi \boldsymbol{a}$ is the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop P_3 of this same example.

In this case, $\mathbb{B}_{P_3} = \{3\}$, hence $\boldsymbol{a} - \{2,6\}$ equals $(0,1,1,3,0,0,2)$.

Let

$$w = [\{2,6\};\{3\}][\{1,2\};\{3\}][\{6\};\{3\}]^2\langle\emptyset;\{3\}\rangle,$$

then

$$P_3 = P_2 \circ_\phi w.$$

To see that the right action of $\boldsymbol{a}$ and of w are the same, let us look, for example, at the seventh element. The right action of $\boldsymbol{a}$ add 3 to $\text{MODULO}_m[P_2]_3$, while the right-action of w add 1 three time. Furthermore, the right action of $\boldsymbol{a}$ ensures that the seventh position is maximal, it is also the case of w since 6 belongs to the last symbols of the form $[\cdot;\cdot]$.

Proposition 9.3.10 is now proved.

Proof of Proposition 9.3.10. For $f \in [b-2]$ and for $g \in [f]$, let $w^{f,g}$ be the prefix of w given by:

$$w^{f,g} = \left[\mathbb{O}_{q\backslash\boldsymbol{a}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]\Pi_{j=1}^{f-1}\left[(j)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]^j\left[(f)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]^g.$$

A sequence of letters $\boldsymbol{a}^{f,g}$ is now introduced. It is then proved by induction on f,g that $\delta(q,w^{f,g}\boldsymbol{a}^{f,g}) = q'$. For $f = g = b-2$, $\boldsymbol{a}^{f,g} = \left\langle\emptyset;\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right\rangle$, hence this equality is exactly the equality of the proposition.

Let $\boldsymbol{a}^{0,0} = \boldsymbol{a} - \mathbb{O}_{q\backslash\boldsymbol{a}}$ and let $\boldsymbol{a}^{f,g} \in A_b^d$ be such that, for all $i \in [d-1]$:

$$a_i^{f,g} = \begin{cases} a_i^{0,0} - g & \text{if } \boldsymbol{a}_i^{0,0} = f, \\ 0 & \text{if } \boldsymbol{a}_i^{0,0} < f, \\ a_i^{0,0} & \text{if } \boldsymbol{a}_i^{0,0} > f. \end{cases}$$

Note that $\boldsymbol{a}^{b-2,b-2} = \left\langle\emptyset;\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right\rangle$.

Let $q^{f,g}$ be equal to $\delta(q,w^{f,g})$. Those states satisfy the following equations:

$$q^{f,g} = \begin{cases} \delta(q, & \left[\mathbb{O}_{q\backslash\boldsymbol{a}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right] &) & \text{for } f = g = 0, \\ \delta(q^{f,g-1}, & \left[(f)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right] &) & \text{if } g > 0 \\ q^{f-1,f-1} & & & \text{for } f > 0 \text{ and } g = 0. \end{cases}$$

It is now proven by induction on (f,g) that $q^{f,g} \overset{\mathbb{OESB}}{\preccurlyeq} q\cdot\boldsymbol{a}$. The case $(0,0)$ holds by definition of $q^{0,0}$. The case $(f,0)$ for $f > 0$ is equivalent to the case $(f-1,f-1)$. Let us consider the case (f,g) for $f > 0$ and $g > 0$. Since

$$q^{f,g} = \delta(q^{f,g-1},\left[(f)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]),$$

the property holds.

Finally, let us prove by induction on (f,g) that $\delta(q,w^{f,g}\boldsymbol{a}^{f,g}) = q'$, that is, that $\delta(q^{f,g},\boldsymbol{a}^{f,g}) = q'$.

The case $(0,0)$ holds by Defintion 9.3.4 with $S = \mathbb{O}_{q\backslash\boldsymbol{a}}$. The case $(f,0)$ for $f > 0$, is equivalent to the case $(f-1,f-1)$. Let us consider the case (f,g), for $g > 0$. By induction hypothesis, $\delta(q^{f,g},\boldsymbol{a}^{f,g}) = q'$ and by Defintion 9.3.4 with $S = (f)_{\boldsymbol{w}-\mathbb{O}_{q\backslash\boldsymbol{a}}}$, the equality holds. □

This proposition, with Definition 9.2.13, admits the following corollary:

Corollary 9.3.12. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}_\iota',5}$, let q be a state of $\mathcal{A}$ and $\boldsymbol{a} \in A_b^d$, then $\delta(q,\boldsymbol{a}) \overset{\mathbb{OESBL}}{\preccurlyeq} q\cdot\boldsymbol{a}$.*

Proof. Let

$$w = \left[\mathbb{O}_{q\setminus \boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus \boldsymbol{a}}}\right] \Pi_{f=1}^{b-2} \left[(f)_{\boldsymbol{a}-\mathbb{O}_{q\setminus \boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus \boldsymbol{a}}}\right]^f \left\langle \emptyset; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus \boldsymbol{a}}} \right\rangle.$$

Note that, by construction, $q \cdot \boldsymbol{a} = q \cdot w$, therefore, it remains to prove

$$\delta(q, \boldsymbol{a}) \overset{\mathbb{OESBL}}{\preccurlyeq} q \cdot w.$$

Recall that $w[< i]$ denote the prefix of w' of length i. The lemma is the induction hypothesis for $w' = w$.

For $i = 0$, the $\delta(q, w[< 0]) = q \cdot w[< 0]$. Let $i > 0$ and let us assume that the induction hypothesis hold for $i - 1$. Then:

$$\begin{aligned} \delta(q, w[< i]w[i]) &\overset{\mathbb{OESBL}}{\preccurlyeq} \delta(q, w[< i]) \cdot w[i] && \text{(Definition 9.2.13)} \\ &\overset{\mathbb{OESBL}}{\preccurlyeq} (q \cdot w[< i])w[i] && \text{(By induction)}. \end{aligned} \tag{9.2}$$

□

The previous lemma admits an easy corollary.

Corollary 9.3.13. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}_\iota',5}$, let q a state of $\mathcal{A}$ and $\boldsymbol{w} \in \left(A_b^d\right)^*$, then*

$$\delta(q, \boldsymbol{w}) \overset{\mathbb{OESBL}}{\preccurlyeq} q \cdot \boldsymbol{w}.$$

Proof. The proof is by induction on the length of w. The case $w = \epsilon$ is trivial and the induction case is an application of Corollary 9.3.12. □

9.3.2 From $\left(A_b^d\right)^*$ to $\mathcal{L}$-words

In this section, a result similar to Proposition 9.3.10 is given in Proposition 9.3.17. The main difference between those two propositions is that the former considers letters of the alphabet A_b^d while the latter considers A_b^d-words. More precisely, Proposition 9.3.17 states that, for each automaton $\mathcal{A} \in \mathbb{A}_{\mathcal{V}_\iota',6}$, for each cyclic state q of $\mathcal{A}$, and for each word $\boldsymbol{w} \in \left(A_b^d\right)^*$, there exists a word $s \in \mathcal{L}^*$ such that $\delta(q, \boldsymbol{w}) = \delta(q, s)$. Furthermore, the word s is constructed as a function of $\mathbb{O}_q$, $\mathrm{TOP}^m_{\nu, \mathcal{V}_\iota'}(\boldsymbol{w})$ and $|\boldsymbol{w}|$.

Using Lemma 7.3.32, this property implies that $\mathcal{A}_q$ accepts a $\Sigma_0[\mathcal{V}_\iota']/\nu$-definable set. Then, using Proposition 7.2.10, it implies that $\mathcal{A}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

This section is the most technical of this part. The proof of Proposition 9.3.17 consists mostly in a sequence of equalities, which uses all properties of the definitions of the sets of automata $\mathbb{A}_{\mathcal{V}_\iota',1}$, $\mathbb{A}_{\mathcal{V}_\iota',2}$, $\mathbb{A}_{\mathcal{V}_\iota',3}$, $\mathbb{A}_{\mathcal{V}_\iota',4}$, $\mathbb{A}_{\mathcal{V}_\iota',5}$ and $\mathbb{A}_{\mathcal{V}_\iota',6}$. Some equalities of the proof of Proposition 9.3.17 are stated as separate lemma.

The last set of automata of this part is now introduced, restraining $\mathbb{A}_{\mathcal{V}_\iota',5}$ to the automata which satisfy some equalities. It is easy to show, using Lemmas 9.1.3 and 9.1.14, that those equalities are satisfied by $\mathcal{A}_{\phi,\mathbb{N}}$. Those 24 equalities satisfy the following properties:

- they hold on $\mathcal{A}_{\phi,\mathbb{N}}$,
- they are used by the proof of Proposition 9.3.17,
- they only deal with a word of length at most $b + 1$. Hence an algorithm can check them efficiently.

if:		then:	
$J \cap K = \emptyset$		$\delta(q, \langle \emptyset; J \rangle [K; \emptyset]) = \delta(q, [K; \emptyset][K \cup J; \emptyset]^{b-1} \langle \emptyset; \emptyset \rangle)$.	(9.3)
$(J \cup I) \cap K = \emptyset$		$\delta(q, [I; J][K; \emptyset]) = \delta(q, [I \cup K; \emptyset][\emptyset; K \cup J])$.	(9.4)
$\mathbb{B}_q \subseteq J$		$\delta(q, [\emptyset; J][K; \emptyset]) = \delta(q, [\emptyset; J][K \setminus J; \emptyset][J \cap K; \emptyset])$.	(9.5)
$J \cap K = \emptyset$	$I \cap \mathbb{O}_q = \emptyset$,	$\delta(q, [I; J][K; \emptyset]) = \delta(q, [K; \emptyset][I; \emptyset][\emptyset; K \cup J])$.	(9.6)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; K][K; \emptyset]) = \delta(q, [K; \emptyset])$.	(9.7)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [K; \emptyset][\emptyset; K]) = \delta(q, [K; \emptyset])$.	(9.8)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][\emptyset; J]) = \delta(q, [\emptyset; J][I; \emptyset][\emptyset; J])$.	(9.9)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][\emptyset; J]) = \delta(q, [\emptyset; J])$.	(9.10)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, \langle \emptyset; \emptyset \rangle [\emptyset; J]) = \delta(q, [\emptyset; J] \langle \emptyset; \emptyset \rangle)$.	(9.11)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][K; \emptyset]) = \delta(q, [K; \emptyset][\emptyset; J][\emptyset; K])$.	(9.12)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [K; \emptyset][I; \emptyset][\emptyset; K])$.	(9.13)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [I \setminus K; \emptyset][K \setminus I; \emptyset][K \cap I; \emptyset]^2)$.	(9.14)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][K; \emptyset]) = \delta(q, [\emptyset; J \setminus K][K \setminus J; \emptyset][K \cap J; \emptyset])$.	(9.15)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [I \setminus K; \emptyset][I \cap K; \emptyset][K; \emptyset])$.	(9.16)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][K; \emptyset]) = \delta(q, [\emptyset; J \setminus K][\emptyset; J \cap K][K; \emptyset])$.	(9.17)
$K \subseteq I$	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [I \setminus K; \emptyset][K; \emptyset]^2)$.	(9.18)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [K; \emptyset][I; \emptyset][\emptyset; K])$.	(9.19)
$I \subseteq K$	$\mathbb{B}_q = \emptyset$,	$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [K; \emptyset][I; \emptyset])$.	(9.20)
$K \subseteq J$	$\mathbb{B}_q = \emptyset$,	$\delta(q, [K; \emptyset][\emptyset; J]) = \delta(q, [\emptyset; J][K; \emptyset])$.	(9.21)
$J \cap K = \emptyset$	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][\emptyset; K]) = \delta(q, [\emptyset; K][\emptyset; K \cup J])$.	(9.22)
$J \cap K = \emptyset$	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][\emptyset; K]) = \delta(q, [\emptyset; J][\emptyset; J \cup K])$.	(9.23)
	$\mathbb{B}_q = \emptyset$,	$\delta(q, [\emptyset; J][\emptyset; K]) = \delta(q, [\emptyset; J \setminus K][\emptyset; K \setminus J][\emptyset; J \cap K])$.	(9.24)

Table 9.2: Equalities of Definition 9.3.14

***Definition 9.3.14** ($\mathbb{A}_{\mathcal{V}'_t,6}$)**.** Let $\mathbb{A}_{\mathcal{V}'_t,6}$ be the set of automata $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_t,5}$ such that for all cyclic states q, for all $I, J, J', K \subseteq [d-1]$ such that I is disjoint from J, the equalities of Table 9.2 are satisfied: Furthermore, if the vocabulary is $\mathcal{V}_2^{\mathbb{N}}$, for $\mathbb{B}_q = \emptyset$, then:

$$\delta(q, [I; \emptyset][K; \emptyset]) = \delta(q, [K; \emptyset][I; \emptyset]), \tag{9.25}$$

and

$$\delta(q, [\emptyset; J'][\emptyset; J]) = \delta(q, [\emptyset; J][\emptyset; J']). \tag{9.26}$$

Lemma 9.3.15. *The automaton $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_t,6}$.*

Proof. By Lemma 9.3.6, $\mathcal{A}_{\phi,\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}'_t,5}$. Let $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_t}$ be a cyclic state of $\mathcal{A}_{\phi,\mathbb{N}}$, let $9.3 \leq e \leq 9.26$ be the number of an equality of Definition 9.3.14. Let $I, J, J', K \subseteq [d-1]$ with $I \cap J = \emptyset$. If I, (respectively J, J', K) does not appear in the terms of Equality (e), let us assume that I (respectively J, J', K) is the empty set.

Let w and v be the words on the left and right side of equality (e), let $Q = \delta(P, w)$ and $R = \delta(P, v)$. It remains to prove that $Q = R$. Let $i, j \in [d-1]$.

- Let us consider $\text{LENGTH}_{m,b}$. Let c be 1 if $e = 9.3$ and 0 otherwise then

$$\begin{aligned} \text{LENGTH}_{m,b} Q &= \text{LENGTH}_{m,b}(P) + c && \text{(using the definition of } Q\text{)} \\ &= \text{LENGTH}_{m,b}(O). && \text{(using the definition of } O\text{)} \end{aligned}$$

- Let us consider MODULO_m. Let c be 1 if $i \in I$. Let c' be 1 if $i \in K$. Then

$$\begin{aligned} \text{MODULO}_m[Q]_i &= \text{MODULO}_m[P]_i + c + c' && \text{(using the definition of } Q\text{)} \\ &= \text{MODULO}_m[O]_i. && \text{(using the definition of } O\text{)} \end{aligned}$$

- Let us consider $\mathbb{O}$. Then $i \in \mathbb{O}_Q$ holds if and only if [$i \in \mathbb{O}_P$ and $i \notin I$ and $i \notin J$ and $i \notin J'$ and $i \notin K$], which is equivalent to $i \mathbb{E}_R j$.
- Let us consider $\mathbb{E}$. Then $i \mathbb{E}_Q j$ holds if and only if [$i \mathbb{E}_P j$ and $(i \in I) \Longleftrightarrow (j \in I)$ and $(i \in J) \Longleftrightarrow (j \in J)$ and $(i \in J') \Longleftrightarrow (j \in J')$ and $(i \in K) \Longleftrightarrow (j \in K)$], which is equivalent to $i \mathbb{E}_R j$.
- Let us consider $\mathbb{S}$. The relations $i \mathbb{S}_Q j$ and $i \mathbb{S}_O j$ holds exactly in one of those three cases:
  - either $e = 9.4$, $j \in I$ and $i \notin I \cup J \cup K$,
  - either e is 9.3, 9.4 or 9.6, $j \in K$ and $i \in J$,
  - or $i \mathbb{S}_P j$ holds and $(i \in I) \Longleftrightarrow (j \in I)$ and $(i \in J) \Longleftrightarrow (j \in J)$ and $(i \in J') \Longleftrightarrow (j \in J')$ and $(i \in K) \Longleftrightarrow (j \in K)$].
- Finally, let us consider $\mathbb{L}$. $i \mathbb{L}_Q j$ and $i \mathbb{L}_O j$ hold if and only if $\mathbb{L}$ belongs to $I^2_{\mathcal{V}'_t}$ and one of the following statements hold:
  - either $j \in K, i \notin K$,
  - either $j \in J, i \notin J$, and $(i \in K) \Longleftrightarrow (j \in K)$,
  - either $j \in I, i \notin I, i \notin J$ and $(i \in K) \Longleftrightarrow (j \in K)$,
  - or $i \mathbb{L}_P j$ and $(i \in I) \Longleftrightarrow (j \in I)$, $(i \in J) \Longleftrightarrow (j \in J)$ and $(i \in K) \Longleftrightarrow (j \in K)$.
- Finally, the case $\mathbb{B}$ is trivial, since neither $i \in \mathbb{B}_Q$ nor $i \in \mathbb{B}_O$ hold.

□

***Lemma 9.3.16** (Deciding $\mathbb{A}_{\mathcal{V}'_t,6}$)**.** It is decidable in time $O\left(nb^d 3^d d\right)$ whether a minimal automaton with n states belongs to $\mathbb{A}_{\mathcal{V}'_t,6}$.

Proof. By Lemma 9.3.7, it is decidable in time $O\left(nb^d 3^d d\right)$ whether a minimal automaton belongs to $\mathbb{A}_{\mathcal{V}'_t,5}$. The algorithm runs on each cyclic state q, and on each equality $9.3 \leq (e) \leq 9.26$. For each state q and each equality (e), the algorithms runs on each sets I, J and K which appear in the equality (e), such that $I \cap J = \emptyset$. The algorithm checks whether the conditions of Equality (e) are satisfied and whether the equality does not hold, if it is the case the algorithm rejects. Otherwise the algorithm accepts.

There are $O(n)$ cyclic states, $O\left(3^d\right)$ pair of sets (I, J) or (J, J') and $O\left(2^d\right)$ sets K, hence $O\left(6^d\right)$ 3-tuples of sets (I, J, K). Equality (9.3) can be checked in time $O(bd)$ and all other equalities can be checked in time $O(d)$. Hence the algorithms runs in time $O\left(n6^d db\right)$. Note that, since $b \geq 4$, then $6^d b \leq b^d 3^d$, hence the algorithms runs in time $O\left(nb^d 3^d d\right)$. □

The main proposition of this section is now given.

Proposition 9.3.17. Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$. Let m be the least common multiple of the $\mathrm{LoopSize}(q,I)$ for each cyclic state q and each $\mathbb{E}\circlearrowleft\mathbb{S}_q$-class I. Let q be a cyclic state of $\mathcal{A}$ and let $\boldsymbol{w},\boldsymbol{w}' \in \left(A_b^d\right)^+$ be two words such that:

- $|\boldsymbol{w}| = |\boldsymbol{w}'|$,
- $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}) = \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}')$ and
- their last letter is $\mathbf{0}$.

Then $\delta(q,\boldsymbol{w}) = \delta(q,\boldsymbol{w}')$.

The main idea of the proof of this proposition consists in proving that $\delta(q,\boldsymbol{w})$ and $\delta(q,\boldsymbol{w}')$ are both equal to $\delta(q,w'')$ where w'' is a word which only depends on $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w})$, $|\boldsymbol{w}|$ and on q. This is done in Corollary 9.3.36. In order to prove this corollary a sequence of equalities is first proved in the three following sections.

9.3.2.1 Moving symbols of the form $[\emptyset,K]$

Symbols of the form $[\emptyset;K]$ are considered in this section. It is explained how to rewrite words where this symbol occurs.

It should be reminded that, intuitively, the right-action of the letters $[\emptyset;K]$ ensures that K is a $\mathbb{L}\circlearrowleft\mathbb{E}\circlearrowleft\mathbb{S}_{q\cdot[\emptyset;K]}$-maximal class. Sequences of symbols of the form $[\emptyset;K]$ are studied in the two following lemmas and corollaries in order to show that different sequences have the same action. The following lemmas consider the interaction between symbols of the form $[\emptyset;J]$ and symbols of the form $[I;\emptyset]$.

Lemma 9.3.18. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$, let $K \subseteq [d-1]$ disjoint from the J_i's for $i \in [e-1]$. The following equality holds:*

$$\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[\emptyset;J_i]) = \delta(q,\Pi_{i=0}^{e-1}[\emptyset;J_i]\left[\emptyset;K\cup\bigcup_{i=0}^{e-1}J_i\right]). \tag{9.27}$$

For the sake of readability, as in Example 9.3.5, when an equality is used, the part of terms which is created by the equality appears in color in the equation. The main exception to this rule is the application of Equality (9.1), which removes $[\emptyset;\emptyset]$ from terms. Two easy examples are given in Table 9.3 with basic arithmetic properties. Note in the second case that +3 is colored while it did not move or change. This is because it is a part of the commutative operation.

$3+4-3=$ $3+1\quad=$ $4.$	$3+4-3=$ $4+3-\quad 3=$ $4+0\qquad=$ $4.$

Table 9.3: Examples of color

Proof. The proof is by induction on e. Note that if $e = 0$, then $\bigcup_{i=0}^{e-1} J_i = \emptyset$ and both sides of Equality (9.27) are syntactically equal. Let us assume that $e > 0$ and that the lemma holds for $e-1$.

$$
\begin{aligned}
&\delta(q, [\emptyset; K]\Pi_{i=0}^{e-1}[\emptyset; J_i]) && && && && \\
=&\delta(q, [\emptyset; K]\Pi_{i=0}^{e-2}[\emptyset; J_i] && && [\emptyset; J_{e-1}] && && \\
=&\delta(q, && \Pi_{i=0}^{e-2}[\emptyset; J_i] && \left[\emptyset; K \cup \textstyle\bigcup_{i=0}^{e-2} J_i\right] && [\emptyset; J_{e-1}] && && \text{(using induction)} \\
=&\delta(q, && \Pi_{i=0}^{e-2}[\emptyset; J_i] && && [\emptyset; J_{e-1}] && \left[\emptyset; K \cup \textstyle\bigcup_{i=0}^{e-2} J_i \cup J_{e-1}\right] && \text{(using Equality (9.22))} \\
=&\delta(q, && \Pi_{i=0}^{e-1}[\emptyset; J_i] && && && \left[\emptyset; K \cup \textstyle\bigcup_{i=0}^{e-1} J_i\right] && .
\end{aligned}
$$

□

Let us now prove a similar lemma, where K is not anymore assumed to be disjoint from the J_i's.

Lemma 9.3.19. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0, \ldots, J_{e-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $K \subseteq [d-1]$. The following equality holds:*

$$\delta(q, [\emptyset; K]\Pi_{i=0}^{e-1}[\emptyset; J_i]) = \delta(q, \left[\emptyset; K \setminus \textstyle\bigcup_{i=0}^{e-1} J_i\right]\Pi_{i=0}^{e-1}([\emptyset; J_i \setminus K][\emptyset; J_i \cap K])). \tag{9.28}$$

Proof. The proof is by induction on e. For $e = 0$ the two terms of Equation (9.28) are syntactically equal. Let us assume that $e > 0$ and that the lemma holds for $e-1$, then for all $K' \subseteq [d-1]$.

$$
\begin{aligned}
&\delta(q, [\emptyset; K'] && \Pi_{i=1}^{e-1}[\emptyset; J_i] && && \\
=&\delta(q, \left[\emptyset; K' \setminus \textstyle\bigcup_{i=1}^{e-1} J_i\right] && \Pi_{i=1}^{e-1}([\emptyset; J_i \setminus K'][\emptyset; J_i \cap K']) && && \text{(using induction)} \\
=&\delta(q, && \Pi_{i=1}^{e-1}([\emptyset; J_i \setminus K'][\emptyset; J_i \cap K'])\left[\emptyset; K' \cup \textstyle\bigcup_{i=1}^{e-1} J_i\right] && . && \text{(using Lemma 9.3.18)}
\end{aligned}
\tag{9.29}
$$

Note that, for all $K' \subseteq [d-1]$, the sets $J_i \setminus K'$, the sets $J_i \cap K'$ for $i \in \{1, \ldots, e-1\}$ and the set $K' \setminus \bigcup_{i=1}^{e-1} J_i$ are pairwise disjoint. Hence Lemma 9.3.18 can be used.

Then:

$$
\begin{array}{lll}
\delta(q,[\emptyset;K] & \Pi_{i=0}^{e-1}\ [\emptyset;J_i] &) \\
=\delta(q,[\emptyset;K][\emptyset;J_0] & \Pi_{i=1}^{e-1}\ [\emptyset;J_i] &) \\
=\delta(q,[\emptyset;K\setminus J_0][\emptyset;J_0\setminus K][\emptyset;K\cap J_0]\Pi_{i=1}^{e-1}[\emptyset;J_i] & &) \quad \text{(using Equality (9.24))} \\
=\delta(q,[\emptyset;K\setminus J_0][\emptyset;J_0\setminus K] & \Pi_{i=1}^{e-1}([\emptyset;J_i\setminus(K\cap J_0)][\emptyset;J_i\cap(K\cap J_0)] & \\
 & \left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Equality (9.29))} \\
=\delta(q,[\emptyset;K\setminus J_0][\emptyset;J_0\setminus K] & \Pi_{i=1}^{e-1}([\emptyset;J_i] & [\emptyset;\emptyset]) \\
 & \left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & (J_0\cap J_i=\emptyset) \\
=\delta(q,[\emptyset;K\setminus J_0][\emptyset;J_0\setminus K] & \Pi_{i=1}^{e-1}\ [\emptyset;J_i] & \\
 & \left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Equality (9.1))} \\
=\delta(q,[\emptyset;K\setminus J_0] & \Pi_{i=1}^{e-1}([\emptyset;J_i\setminus(J_0\setminus K)]\ [\emptyset;J_i\cap(J_0\setminus K)] & \\
 & \left[\emptyset;(J_0\setminus K)\cup\bigcup_{i=1}^{e-1}J_i\right]\left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Equality (9.29))} \\
=\delta(q,[\emptyset;K\setminus J_0] & \Pi_{i=1}^{e-1}([\emptyset;J_i] & [\emptyset;\emptyset]) \\
 & \left[\emptyset;(J_0\setminus K)\cup\bigcup_{i=1}^{e-1}J_i\right]\left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & (J_0\cap J_i=\emptyset) \\
=\delta(q,[\emptyset;K\setminus J_0] & \Pi_{i=1}^{e-1}\ [\emptyset;J_i] & \\
 & \left[\emptyset;(J_0\setminus K)\cup\bigcup_{i=1}^{e-1}J_i\right]\left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Equality (9.1))} \\
=\delta(q, & \Pi_{i=1}^{e-1}([\emptyset;J_i\setminus(K\setminus J_0)]\ [\emptyset;J_i\cap(K\setminus J_0)] & \\
\left[\emptyset;(K\setminus J_0)\cup\bigcup_{i=1}^{e-1}J_i\right] & \left[\emptyset;(J_0\setminus K)\cup\bigcup_{i=1}^{e-1}J_i\right]\left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Equality (9.29))} \\
=\delta(q, & \Pi_{i=1}^{e-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \\
\left[\emptyset;\left(K\setminus\bigcup_{i=0}^{e-1}J_i\right)\cup\bigcup_{i=1}^{e-1}\{(J_i\setminus K)\cup(J_i\cap K)\}\right] & & \\
 & \left[\emptyset;(J_0\setminus K)\cup\bigcup_{i=1}^{e-1}J_i\right]\left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & (J_0\cap J_i=\emptyset) \\
=\delta(q,\left[\emptyset;K\setminus\bigcup_{i=0}^{e-1}J_i\right] & \Pi_{i=1}^{e-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \\
 & \left[\emptyset;(J_0\setminus K)\cup\bigcup_{i=1}^{e-1}J_i\right]\left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Lemma 9.3.18)} \\
=\delta(q,\left[\emptyset;K\setminus\bigcup_{i=0}^{e-1}J_i\right][\emptyset;J_0\setminus K]\Pi_{i=1}^{e-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) & \\
 & \left[\emptyset;(K\cap J_0)\cup\bigcup_{i=1}^{e-1}J_i\right]) & \text{(using Lemma 9.3.18)} \\
=\delta(q,\left[\emptyset;K\setminus\bigcup_{i=0}^{e-1}J_i\right][\emptyset;J_0\setminus K] & & \\
\quad[\emptyset;K\cap J_0] & \Pi_{i=1}^{e-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \quad \text{(using Lemma 9.3.18)} \\
=\delta(q,\left[\emptyset;K\setminus\bigcup_{i=0}^{e-1}J_i\right] & \Pi_{i=0}^{e-1}\ [\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]\ ).
\end{array}
$$

□

The previous lemma admits the following corollary, where K is a union of some J_i's.

Corollary 9.3.20. *Let $\mathcal{A}\in\mathbb{A}_{\mathcal{V}',6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q=\emptyset$, let $J_0,\ldots,J_{e-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I\subseteq[d-1]$ be a union of J_i's for $i\in[e-1]$. The following equality holds:*

$$\delta(q,[\emptyset;I]\Pi_{i=0}^{e-1}[\emptyset;J_i])=\delta(q,\Pi_{i=0}^{e-1}[\emptyset;J_i]).$$

Proof. Note that $\{J_i\setminus I, J_{i,E}\cap I\}=\{\emptyset,J_i\}$. By Lemma 9.3.19:

$$
\begin{array}{lll}
\delta(q,[\emptyset;I] & \Pi_{i=0}^{e-1}[\emptyset;J_i] &) \\
=\delta(q,\left[\emptyset;I\setminus\bigcup_{i=0}^{e-1}J_i\right] & \Pi_{i=0}^{e-1}[\emptyset;J_i\setminus I][\emptyset;J_i\cap I]) & \text{(using Lemma 9.3.19)} \\
=\delta(q, & \Pi_{i=0}^{e-1}[\emptyset;J_i] &). \quad \text{(using Equality (9.1))}
\end{array}
$$

□

A result similar to the last lemma is now given, using also some symbols of the form $[I;\emptyset]$.

Lemma 9.3.21. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_{e-1}$ be a sequence of unions of J_i's for $i \in [e-1]$. Let $K \subseteq [d-1]$.*

$$\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset]\,\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) = \delta(q,\Pi_{i=0}^{e-1}[I_i;\emptyset][\emptyset;K]\,\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]).$$

Proof. The proof is by induction on e. For $e=0$, both terms are syntactically equal. Let us assume that $e>0$ and that the property holds for $e-1$. Then:

$$\begin{aligned}
&\delta(q,[\emptyset;K] && \Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \\
=&\delta(q,[\emptyset;K][I_0;\emptyset] && \Pi_{i=1}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \\
=&\delta(q, && [I_0;\emptyset][\emptyset;K][\emptyset;I_0] && \Pi_{i=1}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using Equation 9.12)}\\
=&\delta(q, && [I_0;\emptyset][\emptyset;K] && \Pi_{i=1}^{e-1}[I_i;\emptyset][\emptyset;I_0] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using induction)}\\
=&\delta(q, && [I_0;\emptyset][\emptyset;K] && \Pi_{i=1}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using Corollary 9.3.20)}\\
=&\delta(q, && [I_0;\emptyset] && \Pi_{i=1}^{e-1}[I_i;\emptyset][\emptyset;K] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using induction)}\\
=&\delta(q, && && \Pi_{i=0}^{e-1}[I_i;\emptyset][\emptyset;K] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]). &&
\end{aligned}$$

□

The preceding lemma admits the following corollary.

Corollary 9.3.22. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e''-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_{e-1}$ and $I'_0,\dots,I'_{e'-1}$ be two sequences of unions of J_i's for $i \in [e'-1]$. Let $K \subseteq [d-1]$.*

$$\begin{aligned}
&\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{i=0}^{e'-1}\begin{bmatrix}I'_i;\emptyset\end{bmatrix}\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]) =\\
&\delta(q, && \Pi_{i=0}^{e-1}[I_i;\emptyset][\emptyset;K]\Pi_{i=0}^{e'-1}\begin{bmatrix}I'_i;\emptyset\end{bmatrix}\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]).
\end{aligned}$$

Proof. The proof consists in a pair of applications of Lemma 9.3.21.

$$\begin{aligned}
&\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{i=0}^{e'-1}\begin{bmatrix}I'_i;\emptyset\end{bmatrix} && \Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]) && \\
=&\delta(q, && \Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{i=0}^{e'-1}\begin{bmatrix}I'_i;\emptyset\end{bmatrix}[\emptyset;K]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]) && \text{(using Lemma 9.3.21)}\\
=&\delta(q, && \Pi_{i=0}^{e-1}[I_i;\emptyset][\emptyset;K]\Pi_{i=0}^{e'-1}\begin{bmatrix}I'_i;\emptyset\end{bmatrix} && \Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]). && \text{(using Lemma 9.3.21)}
\end{aligned}$$

□

Lemmas 9.3.19 and 9.3.21 admit the two following corollaries.

Corollary 9.3.23. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_{e-1}$ be a sequence of unions of J_i's for $i \in [e'-1]$. Let $K \subseteq [d-1]$.*

$$\begin{aligned}
&\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right] &&)\\
=&\delta(q, && \Pi_{i=0}^{e-1}[I_i;\emptyset]\left[\emptyset;K\setminus\textstyle\bigcup_{i=0}^{e-1}J_i\right]\Pi_{i=0}^{e'-1}([\emptyset;J_i\setminus K][\emptyset;J_i\cap K])).
\end{aligned}$$

Proof.

$$\begin{aligned}
&\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right] &&) && \\
=&\delta(q, && \Pi_{i=0}^{e-1}[I_i;\emptyset][\emptyset;K] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right] &&) && \text{(using Lemma 9.3.21)}\\
=&\delta(q, && \Pi_{i=0}^{e-1}[I_i;\emptyset]\left[\emptyset;K\setminus\textstyle\bigcup_{i=0}^{e-1}J_i\right] && \Pi_{i=0}^{e-1}([\emptyset;J_i\setminus K][\emptyset;J_i\cap K])) && \text{(using Lemma 9.3.19).}
\end{aligned}$$

□

The following corollary is a special case of Corollary 9.3.23, where K is a union of J_i's.

Corollary 9.3.24. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_{e-1}$ be a sequence of unions of J_i's for $i \in [e'-1]$. Let K be a union of the J_i's for $i \in [e'-1]$. Then:*

$$\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset]\,\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) = \delta(q,\Pi_{i=0}^{e-1}[I_i;\emptyset]\Pi_{i=0}^{e-1}[\emptyset;J_i]).$$

Proof. Note that $\{J_i \setminus J_{i,E}, J_{i,E}\} = \{\emptyset, J_i\}$.

$$\begin{aligned}
&\delta(q,[\emptyset;K]\Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) \\
=&\delta(q, \quad \Pi_{i=0}^{e-1}[I_i;\emptyset][\emptyset;K]\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using Lemma 9.3.21)}\\
=&\delta(q, \quad \Pi_{i=0}^{e-1}[I_i;\emptyset] && \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) \quad \text{(using Corollary 9.3.20)}.
\end{aligned}$$

□

Finally, a lemma is given which deals with the vocabulary $\mathcal{V}_2^{\mathbb{N}}$.

Lemma 9.3.25. *Let the vocabulary be $\mathcal{V}'_\iota$ be $\mathcal{V}_2^{\mathbb{N}}$. Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e-1}$ be a sequence of subsets of $[d-1]$. Let $\sigma \in \mathbb{S}_e$ be a permutation of $[e-1]$, then:*

$$\delta(q,\Pi_{i=0}^{e-1}[\emptyset;J_i]) = \delta(q,\Pi_{i=0}^{e-1}[\emptyset;J_{\sigma(i)}]), \tag{9.30}$$

and

$$\delta(q,\Pi_{i=0}^{e-1}[J_i;\emptyset]) = \delta(q,\Pi_{i=0}^{e-1}[J_{\sigma(i)};\emptyset]). \tag{9.31}$$

Proof. Equality (9.32) is proven using Equation (9.26). The proof of Equality (9.31) is similar, using Equation (9.25).

The proof is by induction on e. For $e \le 1$, both side of the equality are syntactically equal. For $e = 2$, either both side of the equality are syntactically equal, or the equality holds by Equation (9.26). Let us assume that $e > 2$ and that Equation (9.32) holds for $e-1$. In this case, there exists two permutations $\sigma',\sigma'' \in \mathbb{S}_e$ such that $\sigma = \sigma' \circ \sigma''$, $\sigma'(0) = 0$ and $\sigma''(e-1) = e-1$. Let $\tau',\tau'' \in \mathbb{S}_{e-1}$ be the permutations σ' and σ'' without its 0-th and $(e-1)$-th component. By induction on e:

$$\begin{aligned}
&\delta(q,\Pi_{i=0}^{e-1}[\emptyset;J_i] &&) \\
=&\delta(q,\Pi_{i=0}^{e-2}[\emptyset;J_i] \quad [\emptyset;J_{e-1}] &&) \\
=&\delta(q,\Pi_{i=0}^{e-2}[\emptyset;J_{\tau''(i)}]\ [\emptyset;J_{e-1}] &&) \quad \text{(using induction)}\\
=&\delta(q,\Pi_{i=0}^{e-2}[\emptyset;J_{\sigma''(i)}]\ [\emptyset;J_{\sigma''(e-1)}] &&) \\
=&\delta(q,[\emptyset;J_{\sigma''(0)}] \quad \Pi_{i=1}^{e-2}[\emptyset;J_{\sigma''(i)}] &&) \\
=&\delta(q,[\emptyset;J_{\sigma''(0)}] \quad \Pi_{i=1}^{e-2}[\emptyset;J_{\tau'(\sigma''(i)-1)}] &&) \quad \text{(using induction)}\\
=&\delta(q,[\emptyset;J_{\sigma'(\sigma''(0))}]\ \Pi_{i=1}^{e-2}[\emptyset;J_{\sigma'(\sigma''(i))}] &&) \\
=&\delta(q,[\emptyset;J_{\sigma(0)}] \quad \Pi_{i=1}^{e-2}[\emptyset;J_{\sigma(i)}] &&) \quad (\sigma = \sigma' \circ \sigma'')\\
=&\delta(q,\delta(q, \quad \Pi_{i=0}^{e-1}[\emptyset;J_{\sigma(i)}] &&).)
\end{aligned} \tag{9.32}$$

□

9.3.2.2 Moving symbols of the form $[K;\emptyset]$

Moving symbols of the form $[\emptyset;K]$ are considered in the previous section. Similarly moving symbols of the form $[K;\emptyset]$ are considered in this section.

The following lemma is similar to Corollary 9.3.22, with $[K;\emptyset]$ instead of $[\emptyset;K]$. It states that, in some cases, a symbol $[K;\emptyset]$ can be moved around some $[\bigcup_{n\in E'} J_n;\emptyset]$'s.

Lemma 9.3.26. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_e$ be a sequence of unions of J_i's for $i \in [e'-1]$. Let $K \subseteq [d-1]$.*

$$\begin{aligned}&\delta(q,[K;\emptyset][I_0;\emptyset] \quad \Pi_{i=1}^{e}[I_i;\emptyset]\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right])\\ =&\delta(q, \quad [I_0;\emptyset][K;\emptyset]\Pi_{i=1}^{e}[I_i;\emptyset]\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]).\end{aligned}$$

Proof.

$$\begin{aligned}&\delta(q,[K;\emptyset][I_0;\emptyset] \quad \Pi_{i=1}^{e}[I_i;\emptyset]\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right])\\ =&\delta(q, \quad [I_0;\emptyset][K;\emptyset][\emptyset;I_0]\Pi_{i=1}^{e}[I_i;\emptyset]\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]) \quad \text{(using Equality (9.13))}\\ =&\delta(q, \quad [I_0;\emptyset][K;\emptyset] \quad \Pi_{i=1}^{e}[I_i;\emptyset]\Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right]). \quad \text{(using Corollary 9.3.24)}\end{aligned}$$

□

The preceding lemma admits the following corollary where instead of moving $[K;\emptyset]$ by one step, it is moved by many steps. The following corollary is similar to Corollary 9.3.23, apart that it uses $[K;\emptyset]$ and not $[\emptyset;K]$.

Corollary 9.3.27. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e''-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_{e-1}$ and $I'_0,\dots,I'_{e'-1}$ be two sequences of unions of J_i's for $i \in [e''-1]$. Let $K \subseteq [d-1]$.*

$$\begin{aligned}&\delta(q,[K;\emptyset]\Pi_{i=0}^{e-1}[I_i;\emptyset] \quad \Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right])\\ =&\delta(q, \quad \Pi_{i=0}^{e-1}[I_i;\emptyset][K;\emptyset]\Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]).\end{aligned}$$

Proof. The proof is by induction on e. For $e = 0$, both terms are syntactically equal. Let us assume that $e > 0$ and that the property holds for $e-1$.

$$\begin{aligned}&\delta(q,[K;\emptyset] \quad \Pi_{i=0}^{e-1}[I_i;\emptyset] \quad \Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right])\\ =&\delta(q,[K;\emptyset][I_0;\emptyset] \quad \Pi_{i=1}^{e-1}[I_i;\emptyset] \quad \Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right])\\ =&\delta(q, \quad [I_0;\emptyset][K;\emptyset]\Pi_{i=1}^{e-1}[I_i;\emptyset] \quad \Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]) \quad \text{(using Lemma 9.3.26)}\\ =&\delta(q, \quad [I_0;\emptyset] \quad \Pi_{i=1}^{e-1}[I_i;\emptyset][K;\emptyset]\Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]) \quad \text{(using induction)}\\ =&\delta(q, \quad \Pi_{i=0}^{e-1}[I_i;\emptyset][K;\emptyset]\Pi_{i=0}^{e'-1}\left[I'_i;\emptyset\right]\Pi_{j=0}^{e''-1}\left[\emptyset;J_j\right]).\end{aligned}$$

□

9.3.2.3 Partitioning the J_i's

In the preceding section, it is shown how to move symbols of the form $[K;\emptyset]$ in some words w. In the preceding results, moving this symbol does not change the other symbols. In this section, it is shown how moving $[K;\emptyset]$ or $[\emptyset;K]$ can be done in order to partition the sets J_i into $\{J_i \cap K, J_i \setminus K\}$ and K into $\left\{K \setminus \bigcup_{i=0}^{e'-1} J_i\right\} \cup \{K \cap J_i \mid i \in [e'-1]\}$.

The following lemma consider repetition of symbols.

Lemma 9.3.28. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $K \subseteq I \subseteq [d-1]$ and $c \in \mathbb{N}^{>0}$. The following equalities hold:*

$$\delta(q,[K;\emptyset][I;\emptyset]^c) = \delta(q,[I \setminus K;\emptyset]^c[K;\emptyset]^{c+1}), \tag{9.33}$$

and

$$\delta(q,[\emptyset;K][I;\emptyset]^c) = \delta(q,[I \setminus K;\emptyset]^c[K;\emptyset]^c). \tag{9.34}$$

Proof. Equality (9.33) is proven using Equality (9.14), the proof of Equality (9.34) is similar, using Equality (9.15).

The proof is by induction on c. Let us first assume that $c = 1$, then:

$$\begin{aligned}
\delta(q,[K;\emptyset][I;\emptyset]) &= \delta(q,[K\setminus I;\emptyset][I\setminus K;\emptyset][I\cap K;\emptyset]^2) && \text{(using Equality (9.14))}\\
&= \delta(q,[\emptyset;\emptyset]\quad [I\setminus K;\emptyset][K;\emptyset]^2) && (K\subseteq I)\\
&= \delta(q,\quad\quad [I\setminus K;\emptyset][K;\emptyset]^2). && \text{(using Equality (9.1))}
\end{aligned}$$

Let us now assume that $c > 1$ and that the lemma holds for $c-1$.

$$\begin{aligned}
&\delta(q,a[I;\emptyset]^c) &&&&&)\\
&= \delta(q,a[I;\emptyset]^{c-1} &&[I;\emptyset] &&&)\\
&= \delta(q,\quad [I\setminus K;\emptyset]^{c-1} &&[K;\emptyset]^c &[I;\emptyset] &&) && \text{(using induction)}\\
&= \delta(q,\quad [I\setminus K;\emptyset]^{c-1} &&[I;\emptyset] &&[K;\emptyset]^c) && \text{(using Equality (9.20))}\\
&= \delta(q,\quad [I\setminus K;\emptyset]^{c-1} &&[I;\emptyset] &[K;\emptyset] &[K;\emptyset]^{c-1}) &&\\
&= \delta(q,\quad [I\setminus K;\emptyset]^{c-1} &&[I\setminus K;\emptyset][K;\emptyset]^2 &[K;\emptyset]^{c-1}) && \text{(using Equality (9.18))}\\
&= \delta(q,\quad [I\setminus K;\emptyset]^{c} &&&[K;\emptyset]^{c+1}). &&
\end{aligned}$$

□

The previous lemma admits the following Corollary, where K is not anymore supposed to be a subset of I.

Corollary 9.3.29. *Let $\mathcal{A}\in\mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q=\emptyset$, let K,I be two subsets of $[d-1]$ and let $c\in\mathbb{N}^{>0}$. The following equalities hold:*

$$\delta(q,[K;\emptyset][I;\emptyset]^c) = \delta(q,[K\setminus I;\emptyset][I\setminus K;\emptyset]^c[I\cap K;\emptyset]^{c+1}), \tag{9.35}$$

and

$$\delta(q,[\emptyset;K][I;\emptyset]^c) = \delta(q,[\emptyset;K\setminus I][I\setminus K;\emptyset]^c[I\cap K;\emptyset]^c). \tag{9.36}$$

Proof. Equality (9.35) is proved, using Equality (9.16), the proof of Equality (9.36) is similar, using Equality (9.17).

Let $e_{[K;\emptyset]}$ = (9.16) and $e_{[\emptyset;K]}$ = (9.17). The proof is direct, using Equality (e_a) and Lemma 9.3.28.

$$\begin{aligned}
&\delta(q,[K;\emptyset] &&[I;\emptyset]^c &&)\\
&= \delta(q,[K\setminus I;\emptyset][K\cap I;\emptyset] &&[I;\emptyset]^c &&) && \text{(using Equality } e_a)\\
&= \delta(q,[K\setminus I;\emptyset][I\setminus(K\cap I);\emptyset]^c &&[I\cap(K\cap I);\emptyset]^{c+e} &&) && \text{(using Lemma 9.3.28)}\\
&= \delta(q,[K\setminus I;\emptyset][I\setminus K;\emptyset]^c &&[I\cap K;\emptyset]^{c+e} &&).
\end{aligned}$$

□

The followings lemma is, intuitively, a mix of Corollaries 9.3.27 and 9.3.29. It considers both symbols of the form $[\emptyset;J_i]$, and the $[I;\emptyset]$'s, with I being a union of J_i's.

Lemma 9.3.30. *Let $\mathcal{A}\in\mathbb{A}_{\mathcal{V}'_\iota,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q=\emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $c_0,\dots,c_{e-1}$ be a sequence of positive integers and let $I_0,\dots,I_{e-1}$ be a sequence of pairwise disjoint unions of J_i's for $i\in[e'-1]$. Let $K\subseteq[d-1]$.*

Then the following equality holds:

$$\begin{aligned}
&\delta(q,[K;\emptyset] && \textstyle\Pi_{i=0}^{e-1}[I_i;\emptyset]^{c_i}\\
&\quad\left[\emptyset;K\setminus\textstyle\bigcup_{j=0}^{e'-1}J_j\right] && \textstyle\Pi_{j=0}^{e'-1}([\emptyset;J_i\setminus K]\ [\emptyset;J_i\cap K]) &&)\\
&= \delta(q,\left[K\setminus\textstyle\bigcup_{i=0}^{e-1}I_i;\emptyset\right] && \textstyle\Pi_{i=0}^{e-1}([I_i\setminus K;\emptyset]^{c_i}\ [I_i\cap K;\emptyset]^{c_i+1}) && (9.37)\\
&\quad\left[\emptyset;K\setminus\textstyle\bigcup_{j=0}^{e'-1}J_j\right] && \textstyle\Pi_{j=0}^{e'-1}([\emptyset;J_i\setminus K]\ [\emptyset;J_i\cap K]) &&).
\end{aligned}$$

Proof. The proof is by induction on e. For $e = 0$, both sides of the equality are syntactically equal. Let us assume that $e > 0$ and that the property holds for $e - 1$.

$$
\begin{aligned}
&\delta(q, \quad [K;\emptyset] \\
&\quad \Pi_{i=0}^{e-1}[I_i;\emptyset]^{c_i} \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \\
&= \delta(q, \quad [K;\emptyset] \quad [I_0;\emptyset]^{c_0} \\
&\quad \Pi_{i=1}^{e-1}[I_i;\emptyset]^{c_i} \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \\
&= \delta(q, \quad [K \setminus I_0;\emptyset] \quad [I_0 \setminus K;\emptyset]^{c_0} \quad [I_0 \cap K;\emptyset]^{c_0+1} \\
&\quad \Pi_{i=1}^{e-1}[I_i;\emptyset]^{c_i} \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \quad \text{(using Corollary 9.3.29)} \\
&= \delta(q, \quad [I_0 \setminus K;\emptyset]^{c_0} \quad [I_0 \cap K;\emptyset]^{c_0+1} \\
&\quad [K \setminus I_0;\emptyset] \\
&\quad \Pi_{i=1}^{e-1}[I_i;\emptyset]^{c_i} \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \quad \text{(using Corollary 9.3.27)} \\
&= \delta(q, \quad [I_0 \setminus K;\emptyset]^{c_0} \quad [I_0 \cap K;\emptyset]^{c_0+1} \\
&\quad \left[(K \setminus I_0) \setminus \bigcup_{i=1}^{e-1} I_i;\emptyset\right] \Pi_{i=1}^{e-1}([I_i \setminus (K \setminus I_0);\emptyset]^{c_i} \; [I_i \cap (K \setminus I_0);\emptyset]^{c_i+1}) \\
&\quad \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \quad \text{(using induction)} \\
&= \delta(q, \quad [I_0 \setminus K;\emptyset]^{c_0} \quad [I_0 \cap K;\emptyset]^{c_0+1} \\
&\quad \left[K \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right] \Pi_{i=1}^{e-1}([I_i \setminus K^{c_i};\emptyset] \quad [I_i \cap K;\emptyset]^{c_i+1}) \\
&\quad \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \quad \left(I_j \cap I_0 = \emptyset\right) \\
&= \delta(q, \quad \left[K \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right] [I_0 \setminus K;\emptyset]^{c_0} \quad [I_0 \cap K;\emptyset]^{c_0+1} \\
&\quad \Pi_{i=1}^{e-1}([I_i \setminus K;\emptyset]^{c_i} \quad [I_i \cap K;\emptyset]^{c_i+1}) \\
&\quad \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_i\right] \Pi_{j=0}^{e'-1}(\left[\emptyset; J_j \setminus K\right] \quad \left[\emptyset; J_j \cap K\right]) \quad) \quad \text{(using Corollary 9.3.27)} \\
&= \delta(q, \quad \left[K \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right] \Pi_{i=0}^{e-1}([I_i \setminus K;\emptyset]^{c_i} \quad [I_i \cap K;\emptyset]^{c_i+1}) \\
&\quad \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_i\right] \Pi_{j=0}^{e'-1}(\left[\emptyset; J_j \setminus K\right] \quad \left[\emptyset; J_j \cap K\right]) \quad).
\end{aligned}
$$

□

The following lemma is similar to the preceding one, with $[\emptyset; K]$ instead of $[K;\emptyset]$.

Lemma 9.3.31. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_t,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0, \ldots, J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $c_0, \ldots, c_{e-1}$ be a sequence of positive integers and let $I_0, \ldots, I_{e-1}$ be a sequence of pairwise disjoint unions of J_i's for $i \in [e'-1]$. Let $K \subseteq [d-1]$.*

Then the following equality holds:

$$
\begin{aligned}
&\delta(q, [\emptyset; K] \quad \Pi_{i=0}^{e-1}[I_i;\emptyset]^{c_i} \\
&\quad \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad) \\
&= \delta(q, \quad \Pi_{i=0}^{e-1}([I_i \setminus K;\emptyset]^{c_i} \quad [I_i \cap K;\emptyset]^{c_i+1}) \\
&\quad \left[\emptyset; K \setminus \bigcup_{j=0}^{e'-1} J_j\right] \Pi_{j=0}^{e'-1}([\emptyset; J_i \setminus K] \quad [\emptyset; J_i \cap K]) \quad).
\end{aligned}
\tag{9.38}
$$

Proof. The proof is by induction on e. The induction property for $e = 0$ holds by Lemma 9.3.19. Let us

assume that $e > 0$ and that the property holds for $e-1$.

$$
\begin{array}{lll}
\delta(q, & [\emptyset;K] & \\
\quad \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \\
= \delta(q, & [\emptyset;K] & [I_0;\emptyset]^{c_0} \\
\quad \prod_{i=1}^{e-1}[I_i;\emptyset]^{c_i} & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \\
= \delta(q, & [\emptyset;K\setminus I_0] & [I_0\setminus K;\emptyset]^{c_0} \quad [I_0\cap K;\emptyset]^{c_0} \\
\quad \prod_{i=1}^{e-1}[I_i;\emptyset]^{c_i} & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \quad \text{(using Corollary 9.3.29)} \\
= \delta(q, & [I_0\setminus K;\emptyset]^{c_0} & [I_0\cap K;\emptyset]^{c_0}[\emptyset;K\setminus I_0] \\
\quad \prod_{i=1}^{e-1}[I_i;\emptyset]^{c_i} & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \quad \text{(using Corollary 9.3.22)} \\
= \delta(q, & [I_0\setminus K;\emptyset]^{c_0} & [I_0\cap K;\emptyset]^{c_0} \\
 & \prod_{i=1}^{e-1}([I_i\setminus(K\setminus I_0);\emptyset]^{c_i} & [I_i\cap(K\setminus I_0);\emptyset]^{c_i}) \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \quad \text{(using induction)} \\
= \delta(q, & [I_0\setminus K;\emptyset]^{c_0} & [I_0\cap K;\emptyset]^{c_0} \\
 & \prod_{i=1}^{e-1}([I_i\setminus K^{c_i};\emptyset] & [I_i\cap K;\emptyset]^{c_i}) \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad) \quad \left(I_j\cap I_0=\emptyset\right) \\
= \delta(q, & [I_0\setminus K;\emptyset]^{c_0} & [I_0\cap K;\emptyset]^{c_0} \\
 & \prod_{i=1}^{e-1}([I_i\setminus K;\emptyset]^{c_i} & [I_i\cap K;\emptyset]^{c_i}) \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_i\right] \prod_{j=0}^{e'-1}(\left[\emptyset;J_j\setminus K\right] & \left[\emptyset;J_j\cap K\right]) \quad) \quad \text{(using Corollary 9.3.27)} \\
= \delta(q, & \prod_{i=0}^{e-1}([I_i\setminus K;\emptyset]^{c_i} & [I_i\cap K;\emptyset]^{c_i}) \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_i\right] \prod_{j=0}^{e'-1}(\left[\emptyset;J_j\setminus K\right] & \left[\emptyset;J_j\cap K\right]) \quad).
\end{array}
$$

□

This lemma admits the following corollary.

Corollary 9.3.32. *Let $\mathcal{A}\in\mathbb{A}_{\mathcal{V}'_t,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q=\emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $c_0,\dots,c_{e-1}$ be a sequence of positive integers and let $I_0,\dots,I_{e-1}$ be a sequence of pairwise disjoint unions of J_i's for $i\in[e'-1]$. Let $K\subseteq[d-1]$.*

Then the following equality holds:

$$
\begin{array}{lll}
\delta(q,[\emptyset;K] & \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \\
 & \prod_{j=0}^{e'-1}[\emptyset;J_i] \quad) & \\
= \delta(q, & \prod_{i=0}^{e-1}([I_i\setminus K;\emptyset]^{c_i} & [I_i\cap K;\emptyset]^{c_i+1}) \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] & [\emptyset;J_i\cap K]) \quad).
\end{array}
\tag{9.39}
$$

Proof.

$$
\begin{array}{lll}
\delta(q,[\emptyset;K] & \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \\
 & \prod_{j=0}^{e'-1}[\emptyset;J_i] \quad) & \\
= \delta(q,[\emptyset;K][\emptyset;K] & \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \\
 & \prod_{j=0}^{e'-1}[\emptyset;J_i] \quad) & \text{(using Equality (9.10))} \\
= \delta(q,[\emptyset;K] & \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] \quad [\emptyset;J_i\cap K]) \quad) & \text{(using Corollary 9.3.23)} \\
= \delta(q, & \prod_{i=0}^{e-1}([I_i\setminus K;\emptyset]^{c_i} & [I_i\cap K;\emptyset]^{c_i+1}) \\
 & \left[\emptyset;K\setminus\bigcup_{j=0}^{e'-1}J_j\right] \prod_{j=0}^{e'-1}([\emptyset;J_i\setminus K] \quad [\emptyset;J_i\cap K]) \quad). & \text{(using Lemma 9.3.31)}
\end{array}
\tag{9.40}
$$

□

The following lemma is similar to Lemma 9.3.30, with repetitions of the symbol $[K;\emptyset]$. Contrary to the preceding lemmas, no version with $[\emptyset;K]$ are given. Indeed, since $\delta(q,[\emptyset;K]^2) = \delta(q,[\emptyset;K])$ there is no reason to consider repetition of the symbol $[\emptyset;K]^2$.

Lemma 9.3.33. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_t,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $c_0,\dots,c_{e-1}$ be a sequence of positive integers and let $I_0,\dots,I_{e-1}$ be a sequence of pairwise disjoint unions of J_i's for $i \in [e'-1]$. Let $K \subseteq [d-1]$ and let $c' \in \mathbb{N}^{>0}$.*

Then the following equality holds:

$$\begin{aligned}
&\delta(q,[K;\emptyset]^{c'} \quad \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} \\
&\qquad\qquad \prod_{j=0}^{e'-1}\left[\emptyset;J_j\right] \quad) \\
=&\delta(q,\begin{bmatrix}K\setminus\bigcup_{i=0}^{e}I_i;\emptyset\end{bmatrix}^{c'} \prod_{i=0}^{e-1}([I_i\setminus K;\emptyset]^{c_i}\,[I_i\cap K;\emptyset]^{c_i+c'}) \\
&\qquad\begin{bmatrix}\emptyset;K\setminus\bigcup_{i=0}^{e'-1}J_i\end{bmatrix} \prod_{i=0}^{e'-1}([\emptyset;J_i\setminus K]\;\;[\emptyset;J_i\cap K]) \quad).
\end{aligned} \tag{9.41}$$

Proof. The proof is by induction on c'. Let us first consider the case $c'=1$.

$$\begin{aligned}
&\delta(q,[K;\emptyset] \quad \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} \\
&\qquad\qquad \prod_{j=0}^{e'-1}\left[\emptyset;J_j\right] \quad) \\
=&\delta(q,[K;\emptyset][\emptyset;K] \quad \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} \\
&\qquad\qquad \prod_{j=0}^{e'-1}\left[\emptyset;J_j\right] \quad) \qquad \text{(using Equality (9.8))} \\
=&\delta(q,[K;\emptyset] \quad \prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i} \\
&\qquad\begin{bmatrix}\emptyset;K\setminus\bigcup_{i=0}^{e'-1}J_i\end{bmatrix} \prod_{i=0}^{e'-1}([\emptyset;J_i\setminus K]\;\;[\emptyset;J_i\cap K]) \quad) \qquad \text{(using Corollary 9.3.23)} \\
=&\delta(q,\begin{bmatrix}K\setminus\bigcup_{i=0}^{e}I_i;\emptyset\end{bmatrix} \prod_{i=0}^{e-1}([I_i\setminus K;\emptyset]^{c_i}\,[I_i\cap K;\emptyset]^{c_i+1}) \\
&\qquad\begin{bmatrix}\emptyset;K\setminus\bigcup_{i=0}^{e'-1}J_i\end{bmatrix} \prod_{i=0}^{e'-1}([\emptyset;J_i\setminus K]\;\;[\emptyset;J_i\cap K]) \quad) \qquad \text{(using Lemma 9.3.30).}
\end{aligned}$$

Let us assume that $c'>1$ and that Equality (9.41) holds for $c'-1$.

In order to prove the inductive case, two equalities must first be proven. Let us first prove that:

$$K\setminus\left\{\left(K\setminus\bigcup_{i=0}^{e-1}I_i\right)\cup\bigcup_{i=0}^{e-1}[(I_i\setminus K)\cup(I_i\cap K)]\right\}=\emptyset. \tag{9.42}$$

For the sake of contradiction, let us assume that there exists

$$j\in K\setminus\left\{\left(K\setminus\bigcup_{i=0}^{e-1}I_i\right)\cup\bigcup_{i=0}^{e-1}[(I_i\setminus K)\cup(I_i\cap K)]\right\}.$$

Hence, $j\in K$, $j\notin K\setminus\bigcup_{i=0}^{e-1}I_i$ and $j\notin(I_i\setminus K)\cup(I_i\cap K)$ for all $i\in[e-1]$. Having $j\in K$ and $j\notin K\setminus\bigcup_{i=0}^{e-1}I_i$ imply $j\in\bigcup_{i=0}^{e-1}I_i$, that is, there exists $i\in[e-1]$ such that $j\in I_i$. Since $j\in I_i$, $j\in(I_i\setminus K)\cup(I_n\cap K)$. Note that j belongs and does not belong to $(I_i\setminus K)\cup(I_i\cap K)$, it is a contradiction.

Let us now prove that:

$$K\setminus\left\{\left(K\setminus\bigcup_{i=0}^{e-1}J_i\right)\cup\bigcup_{i=0}^{e-1}\{(J_i\setminus K)\cup(J_i\cap K)\}\right\}=\emptyset \tag{9.43}$$

For the sake of contradiction, let us assume that there exists

$$j\in K\setminus\left\{\left(K\setminus\bigcup_{i=0}^{e-1}J_i\right)\cup\bigcup_{i=0}^{e-1}\{(J_i\setminus K)\cup(J_i\cap K)\}\right\},$$

hence $j \in K$, $j \notin \left(K \setminus \bigcup_{i=0}^{e-1} J_i\right)$ and $j \notin \bigcup_{i=0}^{e-1}\{(J_i \setminus K) \cup (J_i \cap K)\}$. Since $j \in K$ and $j \notin \left(K \setminus \bigcup_{i=0}^{e-1} J_i\right)$, $j \in \bigcup_{i=0}^{e-1} J_i$, that is, there exists $i \in [e-1]$ such that $j \in J_i$. Then $j \in (J_i \setminus K) \cup (J_i \cap K)$, hence $j \in \bigcup_{i=0}^{e-1}(J_i \setminus K) \cup (J_i \cap K)$. It has been proved that j belongs and do not belongs to $\bigcup_{i=0}^{e-1}(J_i \setminus K) \cup (J_i \cap K)$, which is a contradiction.

Let us now prove that Equality (9.41) holds.

$$
\begin{array}{lllll}
\delta(q,[K;\emptyset]^{c'} & \Pi_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right] &) & \\
=\delta(q,[K;\emptyset][K;\emptyset]^{c'-1} & \Pi_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \Pi_{j=0}^{e'-1}\left[\emptyset;J_j\right] &) & \\
=\delta(q,[K;\emptyset] & & \left[K \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right]^{c'-1} & & \\
 & \Pi_{i=0}^{e-1}([I_i \setminus K;\emptyset]^{c_i} & [I_i \cap K;\emptyset]^{c_i+c'-1}) & & \\
\left[\emptyset;K \setminus \bigcup_{i=0}^{e-1} J_i\right] & \Pi_{i=0}^{e-1}([\emptyset;J_i \setminus K] & [\emptyset;J_i \cap K]) &) & \text{(using induction)} \\
=\delta(q,\left[K \setminus \left\{\left(K \setminus \bigcup_{i=0}^{e-1} I_i\right) \cup \bigcup_{i=0}^{e-1}[(I_i \setminus K \cup I_i \cap K)]\right\};\emptyset\right] & & & & \\
\left[\left(K \setminus \bigcup_{i=0}^{e-1} I_i\right) \setminus K;\emptyset\right]^{c'-1} & & \left[\left(K \setminus \bigcup_{i=0}^{e-1} I_i\right) \cap K;\emptyset\right]^{c'} & & \\
 & \Pi_{i=0}^{e-1}([(I_i \setminus K) \setminus K;\emptyset]^{c_i} & [(I_i \setminus K) \cap K;\emptyset]^{c_i+1} & & \\
 & [(I_i \cap K) \setminus K;\emptyset]^{c_i+c'-1} & [(I_i \cap K) \cap K;\emptyset]^{c_i+c'}) & & \\
\left[\emptyset;K \setminus \left\{\left(K \setminus \bigcup_{i=0}^{e-1} J_i\right) \cup \bigcup_{i=0}^{e-1}\{(J_i \setminus K) \cup (J_i \cap K)\}\right\}\right] & & & & \\
 & \left[\emptyset;\left(K \setminus \bigcup_{i=0}^{e-1} J_i\right) \setminus K\right] & \left[\emptyset;\left(K \setminus \bigcup_{i=0}^{e-1} J_i\right) \cap K\right] & & \\
 & \Pi_{i=0}^{e-1}([\emptyset;(J_i \setminus K) \setminus K] & [\emptyset;(J_i \setminus K) \cap K] & & \\
 & [\emptyset;(J_i \cap K) \setminus K] & [\emptyset;(J_i \cap K) \cap K]) &) & \text{(using Lemma 9.3.30)} \\
=\delta(q,[\emptyset;\emptyset] & [\emptyset;\emptyset]^{c'-1} & \left[K \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right]^{c'} & & \text{(using Equality (9.42))} \\
 & \Pi_{i=0}^{e-1}([I_i \setminus K;\emptyset]^{c_i} & [\emptyset;\emptyset]^{c_i+1} & & \\
 & [\emptyset;\emptyset]^{c_i+c'-1} & [I_i \cap K;\emptyset]^{c_i+c'}) & & \\
[\emptyset;\emptyset] & [\emptyset;\emptyset] & \left[\emptyset;K \setminus \bigcup_{i=0}^{e-1} J_i\right] & & \text{(using Equality (9.43))} \\
 & \Pi_{i=0}^{e-1}([\emptyset;J_i \setminus K][\emptyset;\emptyset] & [\emptyset;\emptyset][\emptyset;J_i \cap K]) &) & \text{(set equality)} \\
=\delta(q, & & \left[K \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right]^{c'} & & \\
 & \Pi_{i=0}^{e-1}([I_i \setminus K;\emptyset]^{c_i} & [I_i \cap K;\emptyset]^{c_i+c'}) & & \\
 & \left[\emptyset;K \setminus \bigcup_{i=0}^{e-1} J_i\right] & & & \\
 & \Pi_{i=0}^{e-1}([\emptyset;J_i \setminus K] & [\emptyset;J_i \cap K]) &). & \text{(using Equality (9.1))}
\end{array}
$$

□

The following lemma is similar to Lemma 9.3.33, with different values of K.

Lemma 9.3.34. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_t,6}$, let q be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_q = \emptyset$, let $J_0,\ldots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $c_0,\ldots,c_{e-1}$ be a sequence of positive integers and let $I_0,\ldots,I_{e-1}$ be a sequence of pairwise disjoint unions of J_i's for $i \in [e'-1]$. Let $K_0,\ldots,K_{k-1}$ be a sequence of disjoint subsets of $[d-1]$ and let $c'_0,\ldots,c'_{e-1}$ be a sequence of positive integers. The following equality holds:*

$$
\begin{array}{lll}
\delta(q,\Pi_{i=0}^{k-1}[K_i;\emptyset]^{c'_i} & \Pi_{i=0}^{e-1}[I_i;\emptyset]^{c_i} & \Pi_{i=0}^{e'-1}[\emptyset;J_i] \quad) \\
=\delta(q,\Pi_{i=0}^{k-1}\left[K_j \setminus \bigcup_{j=0}^{e-1} I_j;\emptyset\right]^{c'_i} & \Pi_{i=0}^{e-1}(\left[I_i \setminus \bigcup_{j=0}^{k-1} K_j;\emptyset\right]^{c_i} & \Pi_{j=0}^{k-1}\left[I_i \cap K_j;\emptyset\right]^{c_i+c'_j}) \\
\Pi_{j=0}^{k-1}\left[\emptyset;K_j \setminus \bigcup_{i=0}^{e-1} J_i\right] & \Pi_{i=0}^{e'-1}(\left[\emptyset;J_i \setminus \bigcup_{j=0}^{k-1} K_j\right] & \Pi_{j=0}^{k-1}\left[\emptyset;J_i \cap K_j\right]) \quad).
\end{array}
\tag{9.44}
$$

Proof. The proof is by induction on k. Let us assume that $k = 0$, both sides of Equality (9.44) are syntactically equal. Let us assume that $k > 0$ and that the lemma holds for $k-1$.

As in the preceding lemma, two equalities must first be proven.

$$\begin{array}{l} K_0 \setminus \left\{\bigcup_{j=1}^{k-1}\left(K_j \setminus \bigcup_{i=0}^{e-1} I_i\right) \cup \bigcup_{i=0}^{e-1}\left\{\left(I_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \left(\bigcup_{j=1}^{k}\left(I_i \cap K_j\right)\right)\right\}\right\} \\ = K_0 \setminus \left\{\bigcup_{i=0}^{e-1} I_i\right\}. \end{array} \tag{9.45}$$

Let

$$k \in K_0 \setminus \left\{\bigcup_{j=1}^{k-1}\left(K_j \setminus \bigcup_{i=0}^{e-1} I_i\right) \cup \bigcup_{i=0}^{e-1}\left\{\left(I_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \left(\bigcup_{j=1}^{k}\left(I_i \cap K_j\right)\right)\right\}\right\}$$

and let us prove that $k \in K_0 \setminus \left\{\bigcup_{i=0}^{e-1} I_i\right\}$.

By hypothesis, $k \notin I_i \setminus \bigcup_{j=1}^{k-1} K_j$, and $k \notin I_i \cap \bigcup_{j=1}^{k-1} K_j$ for all $i \in [e-1]$, hence, $k \notin I_i$, and then, $k \notin \bigcup_{i=0}^{e-1} I_i$. Since $k \in K_0$ and $k \notin \bigcup_{i=0}^{e-1} I_i$, $k \in K_0 \setminus \bigcup_{i=0}^{e-1} I_i$.

Let us now suppose that $k \in K_0 \setminus \left\{\bigcup_{i=0}^{e-1} I_i\right\}$ and let us prove that

$$k \in K_0 \setminus \left\{\bigcup_{j=1}^{k-1}\left[K_j \setminus \bigcup_{i=0}^{e-1} I_i\right] \cup \bigcup_{i=0}^{e-1}\left\{\left(I_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \left(\bigcup_{j=1}^{k}\left(I_i \cap K_j\right)\right)\right\}\right\}.$$

Since $k \in K_0$, and since K_0 is disjoint from the K_j's, $k \notin \left\{\bigcup_{j=1}^{k-1}\left(K_j \setminus \bigcup_{i=0}^{e-1} I_i\right)\right\}$. Since $k \notin \bigcup_{i=0}^{e-1} I_i$, $k \notin \bigcup_{i=0}^{e-1}\left\{\left(I_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \left(\bigcup_{j=1}^{k}\left(I_i \cap K_j\right)\right)\right\}$. Since $k \in K_0$, $k \notin \left\{\bigcup_{j=1}^{k-1}\left(K_j \setminus \bigcup_{i=0}^{e-1} I_i\right)\right\}$ and $k \notin \bigcup_{i=0}^{e-1}\left\{\left(I_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \left(\bigcup_{j=1}^{k}\left(I_i \cap K_j\right)\right)\right\}$ then

$$k \in K_0 \setminus \left\{\left[\bigcup_{j=1}^{k-1}\left(K_j \setminus \bigcup_{i=0}^{e-1} I_i\right)\right] \cup \bigcup_{i=0}^{e-1}\left[\left(I_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \left(\bigcup_{j=1}^{k}\left(I_i \cap K_j\right)\right)\right]\right\}.$$

The proof of the following equality is similar:

$$\begin{array}{l} K_0 \setminus \left\{\bigcup_{j=1}^{k-1}\left(K_j \setminus \bigcup_{i=0}^{e-1} J_i\right) \cup \left\{\bigcup_{i=0}^{e-1}\left(\left(J_i \setminus \bigcup_{j=1}^{k-1} K_j\right) \cup \bigcup_{j=1}^{k-1}\left(J_i \cap K_j\right)\right)\right\}\right\} \\ = K_0 \setminus \left\{\bigcup_{i=0}^{e-1} J_i\right\}. \end{array} \tag{9.46}$$

Then:

$$
\begin{aligned}
&\delta(q, && \textstyle\prod_{j=0}^{k-1} \left[K_j;\emptyset\right]^{c'_j} && \textstyle\prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i}\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \\
&=\delta(q,[K_0;\emptyset]^{c'_0} && \textstyle\prod_{j=1}^{k-1} \left[K_j;\emptyset\right]^{c'_i} && \textstyle\prod_{i=0}^{e-1}[I_i;\emptyset]^{c_i}\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \\
&=\delta(q,[K_0;\emptyset]^{c'_0} && \textstyle\prod_{j=1}^{k-1} \left[K_j \setminus \bigcup_{i=0}^{e-1} I_i;\emptyset\right]^{c'_j} && && \\
& && \textstyle\prod_{i=0}^{e-1}(\left[I_i \setminus \bigcup_{j=1}^{k-1} K_j;\emptyset\right]^{c_i} && \textstyle\prod_{j=1}^{k-1}\left[I_i\cap K_j;\emptyset\right]^{c_i+c'_j}) && \\
& && \textstyle\prod_{j=1}^{k-1} \left[\emptyset;K_j \setminus \bigcup_{i=0}^{e-1} J_i\right] && && \\
& && \textstyle\prod_{i=0}^{e'-1}(\left[\emptyset;J_i \setminus \bigcup_{j=1}^{k-1} K_j\right] && \textstyle\prod_{j=1}^{k-1}\left[\emptyset;J_i\cap K_j\right]) &&) \quad \text{(using induction)} \\
&=\delta(q,[K_0\setminus && \{\textstyle\bigcup_{j=1}^{k-1}(K_j \setminus \bigcup_{i=0}^{e-1} I_i)\cup && && \\
& && \textstyle\bigcup_{i=0}^{e-1} (I_i \setminus \bigcup_{j=1}^{k-1} K_j)\cup && \textstyle\bigcup_{j=1}^{k-1} I_i\cap K_j))\};\emptyset]^{c'_0} && \\
& && \textstyle\prod_{j=1}^{k-1}(\left[(K_j \setminus \bigcup_{i=0}^{e-1} I_i)\setminus K_0;\emptyset\right]^{c'_i} && \left[(K_j \setminus \bigcup_{i=0}^{e-1} I_i)\cap K_0;\emptyset\right]^{c'_i+c'_0}) && \\
& && \textstyle\prod_{i=0}^{e-1}(\left[(I_i \setminus \bigcup_{j=1}^{k-1} K_j)\setminus K_0;\emptyset\right]^{c_i} && \left[(I_i \setminus \bigcup_{j=1}^{k-1} K_j)\cap K_0;\emptyset\right]^{c_i+c'_0} && \\
& && && \textstyle\prod_{j=1}^{k-1}(\left[(I_i\cap K_j)\setminus K_0;\emptyset\right]^{c_i+c'_j} \left[(I_i\cap K_j)\cap K_0;\emptyset\right]^{c_i+c'_j+c'_0})) && \\
& [\emptyset;K_0\setminus\{ && (\textstyle\bigcup_{j=1}^{k-1}(K_j \setminus \bigcup_{i=0}^{e-1} J_i))\cup && && \\
& && (\textstyle\bigcup_{i=0}^{e-1} J_i \setminus \bigcup_{j=1}^{k-1} K_j && \cup\textstyle\bigcup_{j=1}^{k-1}(J_i\cap K_j))\}] && \\
& && \textstyle\prod_{j=1}^{k-1}(\left[\emptyset;(K_j \setminus \bigcup_{i=0}^{e-1} J_i)\setminus K_0\right] && \left[\emptyset;(K_j \setminus \bigcup_{i=0}^{e-1} J_i)\cap K_0\right]) && \\
& && \textstyle\prod_{i=0}^{e'-1}(\left[\emptyset;(J_i \setminus \bigcup_{j=1}^{k-1} K_j)\setminus K_0\right] && \left[\emptyset;(J_i \setminus \bigcup_{j=1}^{k-1} K_j)\cap K_0\right] && \\
& && && \textstyle\prod_{j=1}^{k-1}(\left[\emptyset;(J_i\cap K_j)\setminus K_0\right] \left[\emptyset;(J_i\cap K_j)\cap K_0\right])) &&) \quad \text{(using Lemma 9.3.33)} \\
&=\delta(q,[K_0\setminus\{ && \textstyle\bigcup_{i=0}^{e-1} I_i\};\emptyset]^{c'_0} && && && \text{(Using Equality (9.45))} \\
& && \textstyle\prod_{j=1}^{k-1}(\left[(K_j \setminus \bigcup_{i=0}^{e-1} I_i);\emptyset\right]^{c'_i} && [\emptyset;\emptyset]^{c'_j+c'_0}) && \\
& && \textstyle\prod_{i=0}^{e-1}(\left[I_i \setminus \bigcup_{j=0}^{k-1} K_j;\emptyset\right]^{c_i} && [I_i\cap K_0;\emptyset]^{c_i+c'_0} && \\
& && && \textstyle\prod_{j=1}^{k-1}(\left[I_i\cap K_j;\emptyset\right]^{c_i+c'_j} && [\emptyset;\emptyset]^{c_i+c'_j+c'_0})) && \\
& [\emptyset;K_0\setminus\{ && \textstyle\bigcup_{i=0}^{e-1} J_i\}] && && && \text{(Using Equality (9.46))} \\
& && \textstyle\prod_{j=1}^{k-1}(\left[\emptyset;K_j \setminus \bigcup_{i=0}^{e-1} J_i\right] && [\emptyset;\emptyset]) && \\
& && \textstyle\prod_{i=0}^{e'-1}(\left[\emptyset;J_i \setminus \bigcup_{j=0}^{k-1} K_j\right] && [\emptyset;J_i\cap K_0] && \\
& && && \textstyle\prod_{j=1}^{k-1}(\left[\emptyset;J_i\cap K_j\right] && [\emptyset;\emptyset])) &&) \quad \left(K_0\cap K_j=\emptyset\right) \\
&=\delta(q,[K_0\setminus\{ && \textstyle\bigcup_{i=0}^{e-1} I_i\};\emptyset]^{c'_0} && && && \\
& && \textstyle\prod_{i=1}^{k-1} \left[(K_j \setminus \bigcup_{i=0}^{e-1} I_i);\emptyset\right]^{c'_i} && && && \\
& && \textstyle\prod_{i=0}^{e-1}(\left[I_i \setminus \bigcup_{j=0}^{k-1} K_j;\emptyset\right]^{c_i} && [I_i\cap K_0;\emptyset]^{c_i+c'_0} && \\
& && && \textstyle\prod_{j=1}^{k-1}\left[I_i\cap K_j;\emptyset\right]^{c_i+c'_j}) && && \\
& [\emptyset;K_0\setminus\{ && \textstyle\bigcup_{i=0}^{e-1} J_i\}] && && && \\
& && \textstyle\prod_{j=1}^{k-1} \left[\emptyset;K_j \setminus \bigcup_{i=0}^{e-1} J_i\right] && && && \\
& && \textstyle\prod_{i=0}^{e'-1}(\left[\emptyset;J_i \setminus \bigcup_{j=0}^{k-1} K_j\right] && [\emptyset;J_i\cap K_0] && \\
& && && \textstyle\prod_{j=1}^{k-1}\left[\emptyset;J_i\cap K_j\right]) && &&) \quad \text{(using Equality (9.1))} \\
&=\delta(q, && \textstyle\prod_{j=0}^{k-1} \left[(K_j \setminus \bigcup_{i=0}^{e-1} I_i);\emptyset\right]^{c'_i} && && && \\
& && \textstyle\prod_{i=0}^{e-1}(\left[I_i \setminus \bigcup_{j=0}^{k-1} K_j;\emptyset\right]^{c_i} && \textstyle\prod_{j=0}^{k-1}\left[I_i\cap K_j;\emptyset\right]^{c_i+c'_j}) && \\
& && \textstyle\prod_{j=0}^{k-1} \left[\emptyset;K_j \setminus \bigcup_{i=0}^{e-1} J_i\right] && && && \\
& && \textstyle\prod_{i=0}^{e'-1}(\left[\emptyset;J_i \setminus \bigcup_{j=0}^{k-1} K_j\right] && \textstyle\prod_{j=0}^{k-1}\left[\emptyset;J_i\cap K_j\right]) &&). \quad \text{(Syntactical equality)}
\end{aligned}
$$

□

9.3.2.4 $\left(A_b^d\right)^*$ to $\mathcal{L}^*$

In this section, a lemma similar to Proposition 9.3.10 is proved.

The main technical lemma of this part is now introduced.

Lemma 9.3.35. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}_t',6}$, let q be a cyclic state of $\mathcal{A}$, let $\boldsymbol{w} \in \left(A_b^d\right)^+$ which ends with $\mathbf{0}$. Then:*

$$\delta(q,\boldsymbol{w}) = \delta(q, \left[\mathbb{O}_{q\setminus \boldsymbol{w}};\emptyset\right]\Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^f \Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]\mathbf{0}^{|\boldsymbol{w}|}). \tag{9.47}$$

Proof. The proof is by induction on $|w|$.

Base case Let us suppose that $|\boldsymbol{w}| = 1$. Then $\boldsymbol{w} = \mathbf{0} = \langle\emptyset;\emptyset\rangle$. Since $\boldsymbol{w} = \mathbf{0}$, $\mathbb{O}_{q\setminus\boldsymbol{w}} = \emptyset$. Since $\boldsymbol{w} = \mathbf{0}$ and $\mathbb{O}_{q\setminus\boldsymbol{w}} = \emptyset$, $(i)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}} = \mathbf{0}$.

$$\begin{aligned}
&\delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{w}};\emptyset\right]\Pi_{f=1}^{b^{|\mathbf{0}|}-1}\left[(f)_{\mathbf{0}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^f \Pi_{f=1}^{b^{|\mathbf{0}|}-1}\left[\emptyset;(f)_{\mathbf{0}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]\mathbf{0}^{|\mathbf{0}|})\\
=&\delta(q, [\emptyset;\emptyset]\ \Pi_{f=1}^{b-1}\ [(f)_{\mathbf{0}-\emptyset};\emptyset]^f\ \Pi_{f=1}^{b-1}\ [\emptyset;(f)_{\mathbf{0}-\emptyset}]\ \mathbf{0}\ ) && \text{(using the definition of } \boldsymbol{w} = \mathbf{0})\\
=&\delta(q, [\emptyset;\emptyset]\ \Pi_{f=1}^{b-1}\ [\emptyset;\emptyset]^f\ \Pi_{f=1}^{b-1}\ [\emptyset;\emptyset]\ \mathbf{0}\ ) && (\mathbf{0}-\emptyset = \mathbf{0})\\
=&\delta(q, \mathbf{0}\ ). && \text{(using Equality (9.1))}
\end{aligned}$$

Inductive case Now, let us suppose that $|\boldsymbol{w}| > 1$, that is, that $\boldsymbol{w} = \boldsymbol{a}\boldsymbol{w}'$ with $\boldsymbol{a} \in A_b^d$ and $\boldsymbol{w}' \in \left(A_b^d\right)^+$. The last letter of $\boldsymbol{w}'$ is $\mathbf{0} = \langle\emptyset;\emptyset\rangle$. Let $q' = \delta(q,\boldsymbol{a})$.

By the induction hypothesis:

$$\delta(q',\boldsymbol{w}') = \delta(q', \left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right]\Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}};\emptyset\right]^f \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\right]\mathbf{0}^{|\boldsymbol{w}'|}).$$

In order to use simultaneously Proposition 9.3.10 and the inductive hypothesis, we need to transform q' in $q\cdot\boldsymbol{a}$ in the preceding term. Let us claim that:

$$\begin{aligned}
&\delta(q',\ \left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right]\ \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}};\emptyset\right]^f\ \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\right]\ \mathbf{0}^{|\boldsymbol{w}'|})\\
=&\delta(q,a\left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'};\emptyset\right]\Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^f\Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right]\mathbf{0}^{|\boldsymbol{w}'|}).
\end{aligned} \tag{9.48}$$

The sets $\mathbb{O}_{q\setminus\boldsymbol{a}}$ and $\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$ are now used in order to begin the inductive part of the proof of Equality (9.47).

$$\begin{aligned}
\delta(q,\boldsymbol{w}) =& \delta(q,\boldsymbol{a}\,\boldsymbol{w}' && && &&) && (\boldsymbol{w} = \boldsymbol{a}\boldsymbol{w}')\\
=&\delta(q,\boldsymbol{a}\left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right] && \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}};\emptyset\right]^f && &&) && \\
& && \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-q'\setminus\mathbb{O}_{q'\cdot\boldsymbol{w}'}}\right] && \mathbf{0}^{|\boldsymbol{w}'|} &&) && \text{(using induction)}\\
=&\delta(q,\boldsymbol{a}\left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'};\emptyset\right] && \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^f && &&) && \\
& && \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] && \mathbf{0}^{|\boldsymbol{w}'|} &&) && \text{(using Equality (9.48))}\\
=&\delta(q,\ \left[\mathbb{O}_{q\setminus\boldsymbol{a}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]\Pi_{g=1}^{b-2} && \left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}};\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]^g && \left\langle\emptyset;\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right\rangle && && \\
& \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'};\emptyset\right] && \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^f && && && \\
& && \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] && \mathbf{0}^{|\boldsymbol{w}'|} &&). && \text{(using Proposition 9.3.10)}
\end{aligned} \tag{9.49}$$

Merging $< \emptyset, \mathbb{B}_{\delta(q,\boldsymbol{a})} >$ and $< \emptyset, \emptyset >$ The following step of the proof consists in using Equality (9.3) in order to rewrite the last term of Equation (9.49) and, intuitively, move the symbol $\left\langle \emptyset; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \right\rangle$ to the right.

$$
\begin{aligned}
&\delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] && \prod_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]^{g} \left\langle \emptyset; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \right\rangle \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right] && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{f} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}'|} \quad) \\
&= \delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] && \prod_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]^{g} \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right] \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{b-1} \mathbf{0} && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{f} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}'|} \quad) \qquad \text{(using Equality (9.3))} \\
&= \delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] && \prod_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]^{g} \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right] \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{b-1} && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{bf} \mathbf{0} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}'|} \quad) \qquad \text{(using Equality (9.3))} \\
&= \delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] && \prod_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]^{g} \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right] \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{b-1} && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{bf} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}|} \quad). \qquad \text{(using Equality (9.11))} \\
&&&&& (9.50)
\end{aligned}
$$

In the last equality, the fact that $|\boldsymbol{w}'| + 1 = |\boldsymbol{w}|$ is used.

Merging $\mathbb{O}_{q\setminus\boldsymbol{a}}$ and $\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$ The next step of the proof consists in rewriting the last term of Equation (9.50), using equalities of Definition 9.3.14, in order to merge $\left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]$ and $\left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right]$ on the left.

$$
\begin{aligned}
&\delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] && \prod_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]^{g} \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right] \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{b-1} && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{bf} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}|} \quad) \\
&= \delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{a}}; \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}; \emptyset\right] && \prod_{g=1}^{b-2} \left(\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right] \right. \\
&&& \left. \left[\emptyset; \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]\right)^{g} \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{b-1} && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{bf} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}|} \quad) \qquad \text{(using Equality (9.6))} \\
&= \delta(q, \left[\mathbb{O}_{q\setminus\boldsymbol{w}}; \emptyset\right] \\
&\quad \left[\emptyset; \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] && \prod_{g=1}^{b-2} \left(\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{g} \right. \\
&&& \left. \left[\emptyset; \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right]\right)^{g} \\
&\quad \left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}; \emptyset\right]^{b-1} && \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}; \emptyset\right]^{bf} \\
&&& \prod_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \quad \mathbf{0}^{|\boldsymbol{w}|} \quad). \qquad \text{(using Equality (9.4))} \\
&&&&& (9.51)
\end{aligned}
$$

Using equalities 9.49, 9.50, 9.51, the following equation holds:

$$\begin{aligned}
&\delta(q,\boldsymbol{w}) \\
=&\delta(q,\left[\mathbb{O}_{q\backslash \boldsymbol{w}};\emptyset\right] \\
&\left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]\ \Pi_{g=1}^{b-2}\left(\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{g}\ \left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]\right) \\
&\left[\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{b-1}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}};\emptyset\right]^{bf}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}}\right]\boldsymbol{0}^{|\boldsymbol{w}|}).
\end{aligned} \tag{9.52}$$

In the last equality, the fact that $\mathbb{O}_{q\backslash\boldsymbol{w}} = \mathbb{O}_{q\backslash\boldsymbol{a}} \cup \mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}$ is used.

Let $q'' = \delta(q,\left[\mathbb{O}_{q\backslash\boldsymbol{w}};\emptyset\right])$, since $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,3}$ then $\mathbb{B}_{q''} = \emptyset$. Using Equation (9.52), in order to prove Equation (9.47), it suffices to prove:

$$\begin{aligned}
&\delta(q'',\left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]\ \Pi_{g=1}^{b-2}\left(\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{g}\ \left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]\right) \\
&\quad\left[\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{b-1}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}};\emptyset\right]^{bf}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}}\right]) \\
=&\delta(q'',\ \Pi_{f=1}^{b^{|\boldsymbol{w}|-1}}\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\backslash\boldsymbol{w}}};\emptyset\right]^{f}\ \Pi_{f=1}^{b^{|\boldsymbol{w}|-1}}\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\backslash\boldsymbol{w}}}\right]).
\end{aligned} \tag{9.53}$$

Removing the $[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}]$ The next step of the proof consists in removing all of the symbols $\left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]$ from the first term of Equality (9.53).

$$\begin{aligned}
&\delta(q'',\ \left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right] \\
&\quad\Pi_{g=1}^{b-2}\left(\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{g}\ \left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right]\right) \\
&\quad\left[\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{b-1} \\
&\quad\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}};\emptyset\right]^{bf}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}}\right]) \\
=&\delta(q'',\ \Pi_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{g}\ \left[\emptyset;\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}\right] \\
&\quad\left[\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{b-1} \\
&\quad\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}};\emptyset\right]^{bf}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}}\right])\quad\text{(using Equality (9.9))} \\
=&\delta(q'',\ \Pi_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{g}\ \left[\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}\cup\mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]^{b-1} \\
&\quad\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}};\emptyset\right]^{bf}\Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}}\right]).\quad\text{(using Equality (9.7))}
\end{aligned} \tag{9.54}$$

The next step of the proof consists in transforming all of the symbols $\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}};\emptyset\right]$ and all of the symbols $\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}};\emptyset\right]$ into symbols $\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\backslash\boldsymbol{w}}};\emptyset\right]$.

Let $J_i = (i+1)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\backslash\boldsymbol{w}'}}$ and $I_i = J_i$ for $i \in [b^{|\boldsymbol{w}'|-1} - 2]$. Let $K_i = (i+1)_{\boldsymbol{a}-\mathbb{O}_{q\backslash\boldsymbol{a}}}$ for $i \in [b-3]$, and

$K_{b-2} = \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}$. Using Lemma 9.3.34, the last term of Equation (9.54) is equal to:

$$\begin{aligned}
\delta(q'', \quad & \Pi_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \setminus \bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^{g} \\
& \left[\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \setminus \bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^{b-1} \\
& \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\{\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \setminus \left\{\bigcup_{g=1}^{b-2}(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cup \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right)\right\};\emptyset\right]^{bf} \\
& \quad \Pi_{g=1}^{b-2}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}};\emptyset\right]^{bf+g} \\
& \quad \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right);\emptyset\right]^{bf+b-1}\} \\
& \Pi_{g=1}^{b-2}\left[\emptyset;(f)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \setminus \bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \\
& \left[\emptyset;\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \setminus \bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \\
& \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\{\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \setminus \left\{\bigcup_{g=1}^{b-1}(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cup \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right)\right\}\right] \\
& \quad \Pi_{g=1}^{b-2}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] \\
& \quad \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right)\right]\} \qquad)
\end{aligned} \tag{9.55}$$

Since $\bigcup_{g=1}^{b-2}(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} = \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}$ and $\bigcup_{f=1}^{b^{|w|-1}-1}(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} = \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}$, (9.55) is equal to:

$$\begin{aligned}
\delta(q'', \quad & \Pi_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \setminus \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^{g} \\
& \left[\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \setminus \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^{b-1} \\
& \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\{\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \setminus \left\{\overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cup \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right\};\emptyset\right]^{bf} \\
& \quad \Pi_{g=1}^{b-2}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}};\emptyset\right]^{bf+g} \\
& \quad \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right);\emptyset\right]^{bf+b-1}\} \\
& \Pi_{g=1}^{b-2}\left[\emptyset;(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \setminus \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \\
& \left[\emptyset;\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \setminus \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \\
& \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\{\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \setminus \left\{\overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cup \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right\}\right] \\
& \quad \Pi_{g=1}^{b-2}\left[\emptyset;(g)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (f)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] \\
& \quad \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right)\right]\} \qquad)
\end{aligned} \tag{9.56}$$

Note that:

$$[d-1] \setminus \left(\overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) = \mathbb{O}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}. \tag{9.57}$$

Since $\boldsymbol{w}'$ ends with the letter $\mathbf{0}$, $\mathbb{B}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} = \emptyset$. Note also that:

$$\begin{aligned}
[d-1] \setminus \overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} &= [d-1] \setminus \left(\overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cup \emptyset\right) \\
&= [d-1] \setminus \left(\overline{\mathbb{O}}\,\overline{\mathbb{B}}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cup \mathbb{B}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right) \qquad \left(\mathbb{B}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} = \emptyset\right) \\
&= \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}.
\end{aligned} \tag{9.58}$$

Equalities 9.57 and 9.58 imply that (9.56) equals:

$$\begin{array}{l}\delta(q'', \quad \Pi_{g=1}^{b-2}\left[(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^{g} \\ \quad \left[\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^{b-1} \\ \quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\ \{\left[\left\{(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \mathbb{O}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right\} \setminus \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'};\emptyset\right]^{bf} \\ \quad\quad \Pi_{g=1}^{b-2}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}};\emptyset\right]^{bf+g} \\ \quad\quad \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right);\emptyset\right]^{bf+b-1}\} \\ \quad \Pi_{g=1}^{b-2}\left[\emptyset;(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \\ \left[\emptyset;\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] \\ \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\{\left[\emptyset;\left\{(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \mathbb{O}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right\} \setminus \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}\right] \\ \quad \Pi_{g=1}^{b-2}\left[\emptyset;(g)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (f)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right] \\ \quad \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right)\right]\} \qquad)\end{array} \tag{9.59}$$

Note that, for $g \in \{1,\ldots,b-2\}$, $f \in \left\{1,\ldots,b^{|\boldsymbol{w}'|}-1\right\}$, considering the definition of base b expansion of integers and of $\boldsymbol{w} - \mathbb{O}_{q\setminus\boldsymbol{w}}$:

$$\begin{array}{rcl}(g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} & = & (g)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}} \\ \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} & = & (b-1)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}} \\ \left\{(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \mathbb{O}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right\} \setminus \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} & = & (bf)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}} \\ (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap (g)_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}} & = & (bf+g)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}} \\ (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap \left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \cup \mathbb{B}_{\boldsymbol{a}-\mathbb{O}_{q\setminus\boldsymbol{a}}}\right) & = & (bf+b-1)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\end{array} \tag{9.60}$$

Term (9.61) is obtained by replacing each term of (9.59) which appears on the left-side of an equality of (9.60) by the term on the right side of the same equality. Hence (9.59) and (9.61) are equal.

$$\begin{array}{l}\delta(q'',\Pi_{g=1}^{b-2}\left[(g)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{g}\left[(b-1)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{b-1} \\ \quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left\{\left[(bf)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{bf}\Pi_{g=1}^{b-2}\left[(bf+g)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{bf+g}\left[(bf+b-1)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{bf+b-1}\right\} \\ \quad \Pi_{g=1}^{b-2}\left[\emptyset;(g)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]\left[\emptyset;(b-1)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right] \\ \quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left\{\left[\emptyset;(bf)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]\Pi_{g=1}^{b-2}\left[\emptyset;(bf+g)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]\left[\emptyset;(bf+b-1)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]\right\} \qquad)\end{array} \tag{9.61}$$

Simplifying the expressions which occur in (9.61) leads to (9.62).

$$\delta(q'',\Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{f}\Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]). \tag{9.62}$$

And finally by Equations (9.54), (9.55), (9.56), (9.59), (9.61) and (9.62), Equality (9.53) holds.

Proving Equality (9.48) It remains to prove Equality (9.48). In order to prove this equality, let us prove some equalities which show how $\mathbb{O}_{q'\setminus\boldsymbol{w}'}$ and $\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$ relate, and how $(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$ and $(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$ relate.

For technical reasons, two sets are now considered.

$$\begin{array}{rcl}S & = & \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'} \setminus \mathbb{O}_{q'}, \\ T & = & \left\{\mathbb{O}_{\boldsymbol{w}'} \cup \left((1)_{\boldsymbol{w}'} \cap \mathbb{O}_{q'}\right) \cup S\right\}.\end{array}$$

Intuitively, S and T are both sets of zeros of some states or words. On the one hand, the positions of S are the positions of the zeros of $q\cdot\boldsymbol{a}$ which does not remain zero, neither by application of $\Downarrow_{\phi}$, nor by concatenation of $\boldsymbol{w}'$. On the other hand, T contains the zeros of w', of $q\cdot\boldsymbol{a}$, and of $\boldsymbol{w}' - \mathbb{O}_{q'\setminus\boldsymbol{w}'}$.

In order to prove Equality (9.48), some equality of sets are required. Let $f > 0$, let us claim that:

$$\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right) \cap \mathbb{O}_{q'} = \mathbb{O}_{q'\setminus \boldsymbol{w}'}, \tag{9.63}$$

$$(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}} \cap S = (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \cap T, \tag{9.64}$$

$$(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}} \setminus S = (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \setminus T, \tag{9.65}$$

$$S \setminus \{ \bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1} (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}} \} = (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \cap T, \tag{9.66}$$

$$\{[d-1]\setminus T\} \setminus \left\{ \bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1} (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \right\} = \emptyset \tag{9.67}$$

In order to prove Equality (9.48), let us prove that both terms of this equality are equal to:

$$\begin{array}{r} \delta(q', \left[\mathbb{O}_{q'\setminus \boldsymbol{w}'}; \emptyset\right] \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1} (\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \cap S; \emptyset\right]^f \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \setminus S; \emptyset\right]) \\ \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1} (\left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \cap S\right] \left[\emptyset; (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}} \setminus S\right])) \end{array}$$

It follows from:

$$
\begin{array}{lll}
\delta(q',\left[\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'};\emptyset\right] & & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^f & \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] &) \\
=\delta(q',\left[\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}\right)\cap\mathbb{O}_{q'};\emptyset\right] & [S;\emptyset] & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}};\emptyset\right]^f & \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\right] &) \quad \text{(using Equality (9.69))} \\
=\delta(q',\left[\left(\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}\right)\cap\mathbb{O}_{q'};\emptyset\right] & \left[S\setminus\{\cup_{f=1}^{b^{|\boldsymbol{w}'|-1}}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\};\emptyset\right] & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\setminus S;\emptyset\right]^f & \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\cap S;\emptyset\right]^{f+1}) & \\
\quad \left[S\setminus\{\cup_{f=1}^{b^{|\boldsymbol{w}'|-1}}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\};\emptyset\right] & & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\setminus S\right] & \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}\cap S\right]) &) \quad \text{(using Lemma 9.3.30)} \\
=\delta(q',\left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right] & \left[(1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T;\emptyset\right] & \text{(using Equalities (9.63), (9.66))} \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T;\emptyset\right]^f & \left[(f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T;\emptyset\right]^{f+1}) & \text{(using Equalities (9.64), (9.65))} \\
\quad \left[\emptyset;(1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T\right] & & \text{(using Equality (9.66))} \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T\right] & \left[\emptyset;(f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T\right]) &) \quad \text{(using Equalities (9.64), (9.65))} \\
=\delta(q',\left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right] & & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T;\emptyset\right]^f & \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T;\emptyset\right]^f) & \\
\quad \left[\left(b^{|\boldsymbol{w}'|-1}\right)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T);\emptyset\right]^{b^{|\boldsymbol{w}'|}} & & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T\right] & \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T\right]) & \\
\quad \left[\emptyset;\left(b^{|\boldsymbol{w}'|}\right)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T\right] & &) \quad \text{(Syntactical equality)} \\
=\delta(q',\left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right] & & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T;\emptyset\right]^f & \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T;\emptyset\right]^f)[\emptyset;\emptyset]^{b^{|\boldsymbol{w}'|-1}} & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T\right] & \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T\right])[\emptyset;\emptyset] &) \quad \left(\left(b^{|\boldsymbol{w}'|-1}\right)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}=\emptyset\right) \\
=\delta(q',\left[\mathbb{O}_{q'\setminus\boldsymbol{w}'};\emptyset\right] & & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T;\emptyset\right]^f & \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T;\emptyset\right]) & \\
\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|-1}}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\cap T\right] & \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}\setminus T\right]) &). \quad \text{(using Equality (9.1))}
\end{array}
$$

Note that $[d-1]\setminus T$ is disjoint from $\mathbb{O}_{w'}$, hence is an union of $(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\mathbb{O}_{q'\cdot\boldsymbol{w}'}}}$ for $f\in\left\{1,\ldots,b^{|\boldsymbol{w}'|}\right\}$. This fact allows to use Corollary 9.3.24 in the first of the following equalities:

$$
\begin{aligned}
&\delta(q',\left[\mathbb{O}_{q'\setminus \boldsymbol{w}'};\emptyset\right]\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\ \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}};\emptyset\right]^f \qquad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right])\\
=&\delta(q',\left[\mathbb{O}_{q'\setminus \boldsymbol{w}'};\emptyset\right] \qquad\qquad [\emptyset;[d-1]\setminus T]\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\ \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}};\emptyset\right]^f \qquad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right]) \qquad \text{(using Corollary 9.3.24)}\\
=&\delta(q',\left[\mathbb{O}_{q'\setminus \boldsymbol{w}'};\emptyset\right]\left[\emptyset;\{[d-1]\setminus T\}\setminus\left\{\bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right\}\right]\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\setminus([d-1]\setminus T);\emptyset\right]^f\\
&\qquad\qquad \left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap([d-1]\setminus T);\emptyset\right]^f)\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\setminus([d-1]\setminus T)\right]\\
&\qquad\qquad \left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap([d-1]\setminus T)\right]) \qquad) \qquad \text{(using Corollary 9.3.32)}\\
=&\delta(q',\left[\mathbb{O}_{q'\setminus \boldsymbol{w}'};\emptyset\right] \qquad\qquad [\emptyset;\emptyset] \qquad\qquad \text{(Equality (9.67))}\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T;\emptyset\right]^f\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\setminus T;\emptyset\right]^f)\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T\right]\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\setminus T\right]) \qquad) \qquad \text{(Set equality)}\\
=&\delta(q',\left[\mathbb{O}_{q'\setminus \boldsymbol{w}'};\emptyset\right]\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}(\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T;\emptyset\right]^f\left[(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\setminus T;\emptyset\right]^f)\\
&\quad \Pi_{f=1}^{b^{|\boldsymbol{w}'|}-1}(\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T\right]\left[\emptyset;(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\setminus T\right]) \qquad) \qquad \text{(using Equality (9.1))}
\end{aligned}
$$

Proving set equalities It now remains to prove the set equalities claimed above.

Proving (9.63) Let us prove Equality (9.63) Let $i \in [d-1]$:

$$
\begin{aligned}
i \in \left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right)\cap \mathbb{O}_{q'} &\iff i\in \mathbb{O}_{q\cdot \boldsymbol{a}} \wedge w'_i \notin 0^* \quad \wedge i\in \mathbb{O}_{q'}\\
&\iff i\in \mathbb{O}_{q\cdot \boldsymbol{a}} \wedge w'_i \notin 0^* \quad \wedge i\in \mathbb{O}_{q'} \qquad \text{(using the definition of } \cdot)\\
&\iff \qquad\quad w'_i \notin 0^* \quad \wedge i\in \mathbb{O}_{q'} \qquad (q' \sqsubseteq q\cdot \boldsymbol{a})\\
&\iff \qquad\quad i\in \mathbb{O}_{q'\setminus \boldsymbol{w}'}.
\end{aligned}
$$

Proving (9.64) Let us prove Equality (9.64) Let us first prove that $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}\cap S$ implies $i\in (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T$.

Let $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}\cap S$, then $i\in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}$ and $i\in S$. Since $i\in S$, by definition of S, $i\in \mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}$ and $i\notin \mathbb{O}_{q'}$. Since $i\in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}$ and since $i\in \mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}$, $i\in (f+1)_{\boldsymbol{w}'}$. Since $i\notin \mathbb{O}_{q'}$ and since $i\in (f+1)_{\boldsymbol{w}'}$, $i\in (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}$. Since $i\in S$, by definition of T, $i\in T$. Since $i\in (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}$ and $i\in T$ then $i\in (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T$.

Let us now prove that $i\in (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\cap T$ implies $i\in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}\cap S$.

Since $i\in (f+1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}$, either ($i\in (f+1)_{\boldsymbol{w}'}$ and $i\notin \mathbb{O}_{q'\setminus \boldsymbol{w}'}$) or ($i\in (f+2)_{\boldsymbol{w}'}$ and $i\in \mathbb{O}_{q'\setminus \boldsymbol{w}'}$). Both cases are considered separately.

- Let us suppose that $i\in (f+1)_{\boldsymbol{w}'}$ and $i\notin \mathbb{O}_{q'\setminus \boldsymbol{w}'}$. Since $i\in (f+1)_{\boldsymbol{w}'}$ and $f>0$, $w'_i\notin 0^*$. Since $i\notin \mathbb{O}_{q'\setminus \boldsymbol{w}'}$ and since $w'_i\notin 0^*$ $i\notin \mathbb{O}_{q'}$. Since $i\in T$, $i\notin \mathbb{O}_{q'}$ and $w'_i\notin 0^*$, by definition of T, $i\in S$. Since $i\in S$, by definition of S, $i\in \mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}$. Since $i\in (f+1)_{\boldsymbol{w}'}$ and since $i\notin \mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}$ $i\in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}$. Since $i\in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}$ and since $i\in S$, $i\in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}\cap S$.
- Let us suppose that $i\in (f+2)_{\boldsymbol{w}'}$ and $i\in \mathbb{O}_{q'\setminus \boldsymbol{w}'}$. Since $i\in \mathbb{O}_{q'\setminus \boldsymbol{w}'}$, $i\in \mathbb{O}_{q'}$, hence, by definition of S, $i\notin S$. Since $i\in (f+2)_{\boldsymbol{w}'}$ and since $f>0$, $\overline{w'_i}^{\mathbb{N}}>1$. Since $i\notin S$ and $\overline{w'_i}^{\mathbb{N}}>1$, by definition of T, $i\notin T$, which contradicts the hypothesis.

Proving (9.65) Let us prove Equality (9.65). Let us first prove that $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \setminus S$ implies $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \setminus T$.

Since $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$, either ($i \in (f)_{\boldsymbol{w}'}$ and $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$) or ($i \in (f+1)_{\boldsymbol{w}'}$ and $i \in \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$), both cases are considered separately.

- Let us suppose $i \in (f)_{\boldsymbol{w}'}$ and $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$. Since $i \in (f)_{\boldsymbol{w}'}$ and since $f > 0$ $w'_i \notin 0^*$. Since $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$ and since $w'_i \notin 0^*$, $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}}$. Since $q' \sqsubseteq q\cdot\boldsymbol{a}$ and since $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}}$, $i \notin \mathbb{O}_{q'}$, hence $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$. Since $i \in (f)_{\boldsymbol{w}'}$ and since $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$, $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$. Since $i \notin S$, $w'_i \notin 0^*$ and $i \notin \mathbb{O}_{q'}$, by definition of T, $i \notin T$. Since $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$ and since $i \notin T$, $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \setminus T$.

- Let us suppose $i \in (f+1)_{\boldsymbol{w}'}$ and $i \in \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$. Since $i \in (f+1)_{\boldsymbol{w}'}$ and $f > 0$, $\overline{w'_i}^{\mathbb{N}} > 1$. Since $\overline{w'_i}^{\mathbb{N}} > 1$ and $i \notin S$, $i \notin T$. Since $i \in \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$ and $i \notin S$, by definition of S, $i \in \mathbb{O}_{q'}$. Since $i \in \mathbb{O}_{q'}$ and since $\overline{w'_i}^{\mathbb{N}} > 1$, $i \in \mathbb{O}_{q'\setminus\boldsymbol{w}'}$. Since $i \in \mathbb{O}_{q'\setminus\boldsymbol{w}'}$ and since $i \in (f+1)_{\boldsymbol{w}'}$, $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$. Since $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$ and since $i \notin T$, $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \setminus T$.

Let us now prove that $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \setminus T$ implies $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \setminus S$.

Since $i \notin T$, by definition of S, $i \notin S$, hence it remains to prove that $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$. Since $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$ either ($i \in (f)_{\boldsymbol{w}'}$ and $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$) or ($i \in (f+1)_{\boldsymbol{w}'}$ and $i \in \mathbb{O}_{q'\setminus\boldsymbol{w}'}$). Both cases are considered separately.

- Let us suppose that $i \in (f)_{\boldsymbol{w}'}$ and $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$. Since $i \in (f)_{\boldsymbol{w}'}$, $w'_i \notin 0^*$. Since $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$ and $w'_i \notin 0^*$ then $i \notin \mathbb{O}_{q'}$. Since $w'_i \notin 0^*$, $i \notin \mathbb{O}_{q\cdot\boldsymbol{w}}$. Since $i \notin S$, $i \notin \mathbb{O}_{q'}$ and $i \notin \mathbb{O}_{q\cdot\boldsymbol{w}}$, by definition of S, $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}}$. Since $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}}$, $i \notin q\cdot\boldsymbol{a} \setminus \mathbb{O}_{q\cdot\boldsymbol{w}}$. Since $i \in (f)_{\boldsymbol{w}'}$ and since $i \notin q\cdot\boldsymbol{a} \setminus \mathbb{O}_{q\cdot\boldsymbol{w}}$, $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$.

- Let us suppose that $i \in (f+1)_{\boldsymbol{w}'}$ and $i \in \mathbb{O}_{q'\setminus\boldsymbol{w}'}$. Since $i \in \mathbb{O}_{q'\setminus\boldsymbol{w}'}$, $i \in \mathbb{O}_{q'}$ and $w'_i \notin 0^*$. Since $i \in \mathbb{O}_{q'}$ and since $q' \sqsubseteq q\cdot\boldsymbol{a}$, $i \in \mathbb{O}_{q\cdot\boldsymbol{a}}$. Since $w'_i \notin 0^*$ and since $i \in \mathbb{O}_{q\cdot\boldsymbol{a}}$, $i \in \mathbb{O}_{q\cdot\boldsymbol{a}} \setminus \mathbb{O}_{q\cdot\boldsymbol{w}}$. Since $i \in (f+1)_{\boldsymbol{w}'}$ and since $i \in \mathbb{O}_{q\cdot\boldsymbol{a}} \setminus \mathbb{O}_{q\cdot\boldsymbol{w}}$, $i \in (f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$.

Proving (9.66) Let us prove Equality (9.66). Note that $[d-1]\setminus\bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} = \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$, hence it suffices to prove:

$$S \cap \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} = (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \cap T.$$

Let us first prove that $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap S$ implies $i \in (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \cap T$. Since $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}}$, either ($\overline{w'_i}^{\mathbb{N}} = 0$ and $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$) or ($\overline{w'_i}^{\mathbb{N}} = 1$ and $i \in \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$), both cases are considered separately.

- Let us suppose that $\overline{w'_i}^{\mathbb{N}} = 0$ and $i \notin \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$. Since $i \in S$, $i \in \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$, which is a contradiction.

- Let us suppose that $\overline{w'_i}^{\mathbb{N}} = 1$ and $i \in \mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}$. Since $i \in S$, $i \notin \mathbb{O}_{q'}$, hence $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$. Since $\overline{w'_i}^{\mathbb{N}} = 1$ and since $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$, $i \in (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$. Since $i \in S$, by definition of T, $i \in T$. Since $i \in (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$ and since $i \in T$, $i \in (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \cap T$.

Let us now prove that $i \in (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}} \cap T$ implies $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot\boldsymbol{a}\setminus\boldsymbol{w}'}} \cap S$.

Since $i \in (1)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus\boldsymbol{w}'}}$, either ($\overline{w'_i}^{\mathbb{N}} = 1$ and $i \notin \mathbb{O}_{q'\setminus\boldsymbol{w}'}$) or ($\overline{w'_i}^{\mathbb{N}} = 2$ and $i \in \mathbb{O}_{q'\setminus\boldsymbol{w}'}$), both cases are considered separately.

- Let us suppose that $\overline{w'_i}^{\mathbb{N}} = 1$ and $i \notin \mathbb{O}_{q'\setminus \boldsymbol{w}'}$. Since $i \notin \mathbb{O}_{q'\setminus \boldsymbol{w}'}$ and since $w'_i \notin 0^*$, $i \notin \mathbb{O}_{q'}$. Since $w'_i \notin 0^*$, $i \notin \mathbb{O}_{q'}$ and $i \in T$, by definition of T, $i \in S$. Since $i \in S$, $i \in \mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}$. Since $\overline{w'_i}^{\mathbb{N}} = 1$ and since $i \in \mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}$, $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}$. Since $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}}$ and since $i \in S$, $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}} \cap S$.
- Let us suppose that $\overline{w'_i}^{\mathbb{N}} = 2$ and $i \in \mathbb{O}_{q'\setminus \boldsymbol{w}'}$, hence $i \in \mathbb{O}_{q'}$. Since $i \in \mathbb{O}_{q'}$, by definition of S, $i \notin S$. Since $\overline{w'_i}^{\mathbb{N}} = 2$ and $i \notin S$, by definition of T, $i \notin T$, which contradicts the hypothesis.

Proving (9.67) Let us prove Equality (9.67). For the sake of contradiction, let us assume that there exists $i \in \{[d-1]\setminus T\} \setminus \left\{\bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right\}$.

Since $i \in \{[d-1]\setminus T\} \setminus \left\{\bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right\}$ then $i \notin T$ and $i \notin \left\{\bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right\}$. Having $i \notin T$ implies $w_i \notin 0^*$, ($\overline{w'_i}^{\mathbb{N}} \neq 1$ or $i \notin \mathbb{O}_{q'}$) and $i \notin S$. Since $i \notin \left\{\bigcup_{f=1}^{b^{|\boldsymbol{w}'|}-1}(f)_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}\right\}$ and since $w'_i < b^{\boldsymbol{w}'-1}$, $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}$. Since $i \in \mathbb{O}_{\boldsymbol{w}'-\mathbb{O}_{q'\setminus \boldsymbol{w}'}}$ and since $w_i \notin 0^*$, $\overline{w'_i}^{\mathbb{N}} = 1$ and $i \in \mathbb{O}_{q'\setminus \boldsymbol{w}'}$, hence $i \in \mathbb{O}_{q'}$. Having $\overline{w'_i}^{\mathbb{N}} = 1$, $i \in \mathbb{O}_{q'}$ and ($\overline{w'_i}^{\mathbb{N}} \neq 1$ or $i \notin \mathbb{O}_{q'}$) is a contradiction.

Since $[d-1]\setminus \mathbb{O}_{q'}$ is an $\mathbb{L}_{q'}$-upper set, contains $\mathbb{B}_{q'}$ and is disjoint from $\mathbb{O}_{q'}$, since $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_t,3}$, by Condition 1 of Definition 9.2.13:

$$\delta(q', \left[\emptyset; [d-1]\setminus \mathbb{O}_{q'}\right]) = q'. \tag{9.68}$$

Let us prove that the preceding equality implies

$$\delta(q', \left[\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}; \emptyset\right]) = \delta(q', \left[\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right) \cap \mathbb{O}_{q'}; \emptyset\right][S; \emptyset]) \tag{9.69}$$

It follows from:

$$\begin{aligned}
&\delta(q', \left[\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}; \emptyset\right] &&) \\
=&\delta(q', \left[\emptyset; [d-1]\setminus \mathbb{O}_{q'}\right] \\
&\left[\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}; \emptyset\right] &&) && \text{(using Equality (9.68))} \\
=&\delta(q', \left[\emptyset; [d-1]\setminus \mathbb{O}_{q'}\right] \\
&\left[\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right)\setminus\left([d-1]\setminus \mathbb{O}_{q'}\right); \emptyset\right]\left[\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right)\cap\left([d-1]\setminus \mathbb{O}_{q'}\right); \emptyset\right] &&) && \text{(using Equality (9.5))} \\
=&\delta(q', \left[\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right)\setminus\left([d-1]\setminus \mathbb{O}_{q'}\right); \emptyset\right]\left[\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right)\cap\left([d-1]\setminus \mathbb{O}_{q'}\right); \emptyset\right] &&) && \text{(using Equality (9.68))} \\
=&\delta(q', \left[\left(\mathbb{O}_{q\cdot \boldsymbol{a}\setminus \boldsymbol{w}'}\right)\cap \mathbb{O}_{q'}; \emptyset\right] \quad [S; \emptyset] &&)
\end{aligned}$$

□

The previous lemma admits the following Corollary:

Corollary 9.3.36. *Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_t,6}$. Let m be the least common multiple of the LoopSize(q,I) for each strongly state q and each $\mathbb{E}\mathbb{S}_q$-class I. Let q be a cyclic state of $\mathcal{A}$, let $\boldsymbol{w} \in \left(A_b^d\right)^+$ which ends with $\mathbf{0}$. Then*

$$\begin{aligned}
&\delta(q, \boldsymbol{w}) \\
=&\delta(q, \left[\mathbb{O}_{q\setminus \boldsymbol{w}}; \emptyset\right] \Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus \boldsymbol{w}}}\right|-1}\left[\mathbb{E}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus \boldsymbol{w}}}(i); \emptyset\right]^{\mathrm{mod}^{>0}((i)_{\boldsymbol{w}-\mathbb{O}_{q\setminus \boldsymbol{w}}}, m)} \\
&\Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus \boldsymbol{w}}}\right|-1}\left[\emptyset; \mathbb{E}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus \boldsymbol{w}}}(i)\right]\mathbf{0}^{|\boldsymbol{w}|})
\end{aligned} \tag{9.70}$$

where $\mathrm{mod}^{>0}(a,m)$ *denote the integer* $i \in \{1,\ldots,m\}$ *such that* $i \equiv a \mod m$.

Proof. Let us first remark that: 9.2.22.

$$
\begin{array}{rll}
& \delta(q,\boldsymbol{w}) & \\
=\delta(q,\left[\mathbb{O}_{q\setminus\boldsymbol{w}};\emptyset\right]\ \Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{f} & & \\
\qquad\qquad\Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right] & \mathbf{0}^{|\boldsymbol{w}|}.) & \text{(using Lemma 9.3.35)} \\
=\delta(q,\left[\mathbb{O}_{q\setminus\boldsymbol{w}};\emptyset\right]\ \Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{\mathrm{mod}^{>0}(f,m)} & & \\
\qquad\qquad\Pi_{i=1}^{b^{|\boldsymbol{w}|}-1}\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right] & \mathbf{0}^{|\boldsymbol{w}|}) & \text{(using Lemma 9.2.22)}
\end{array}
\tag{9.71}
$$

Note that, for all $f \in \left\{1,\ldots,b^{|\boldsymbol{w}|}-1\right\}$, $(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}$ is either the empty set or a $\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}$-class. Using Equality (9.1) on all $\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]$'s and $\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right]$ such that $(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}$ is the empty set, the following equality holds:

$$
\begin{array}{rll}
\delta(q,\left[\mathbb{O}_{q\setminus\boldsymbol{w}};\emptyset\right]\ \Pi_{f=1}^{b^{|\boldsymbol{w}|}-1}\left[(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}};\emptyset\right]^{\mathrm{mod}^{>0}(f,m)} & & \\
\qquad\qquad\Pi_{i=1}^{b^{|\boldsymbol{w}|}-1}\left[\emptyset;(f)_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right] & \mathbf{0}^{|\boldsymbol{w}|}) & \\
=\delta(q,\left[\mathbb{O}_{q\setminus\boldsymbol{w}};\emptyset\right]\ \Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right|-1}\left[\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}(i);\emptyset\right]^{\mathrm{mod}^{>0}(\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}}(i),m)} & & \\
\qquad\qquad\Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right|-1}\left[\emptyset;\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}(i)\right] & \mathbf{0}^{|\boldsymbol{w}|}) & \text{(using Equality (9.1))}
\end{array}
\tag{9.72}
$$

By Equations (9.71) and (9.72), Equation (9.70) holds. □

9.3.2.5 Proving Proposition 9.3.17

Proposition 9.3.17 is finally proven in this section.

Proof of Proposition 9.3.17. Since $\mathrm{TOP}^{m}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}) = \mathrm{TOP}^{m}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}')$, $\mathbb{O}_{\boldsymbol{w}} = \mathbb{O}_{\boldsymbol{w}'}$, hence $\mathbb{O}_{q\setminus\boldsymbol{w}} = \mathbb{O}_{q\setminus\boldsymbol{w}'}$. By Corollary 9.3.36 then

$$
\begin{array}{rll}
& \delta(q,\boldsymbol{w}) & \\
=\delta(q,\left[\mathbb{O}_{q\setminus\boldsymbol{w}};\emptyset\right]\ \Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right|-1}\left[\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}(i);\emptyset\right]^{\mathrm{mod}^{>0}(\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}}(i),m)} & & \\
\qquad\qquad\Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}\right|-1}\left[\emptyset;\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}-\mathbb{O}_{q\setminus\boldsymbol{w}}}(i)\right] & \mathbf{0}^{|\boldsymbol{w}|}) & \text{(using Lemma 9.3.35)} \\
=\delta(q,\left[\mathbb{O}_{q\setminus\boldsymbol{w}'};\emptyset\right]\ \Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}'-\mathbb{O}_q\setminus\mathbb{O}_{q\cdot\boldsymbol{w}'}}\right|-1}\left[\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}'-\mathbb{O}_q\setminus\mathbb{O}_{q\cdot\boldsymbol{w}'}}(i);\emptyset\right]^{\mathrm{mod}^{>0}(\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}'}(i),m)} & & \\
\qquad\qquad\Pi_{i=0}^{\left|\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}'-\mathbb{O}_q\setminus\mathbb{O}_{q\cdot\boldsymbol{w}'}}\right|-1}\left[\emptyset;\mathbb{E}^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}_{\boldsymbol{w}'-\mathbb{O}_q\setminus\mathbb{O}_{q\cdot\boldsymbol{w}'}}(i)\right] & \mathbf{0}^{|\boldsymbol{w}'|}) & \\
=\delta(q,\boldsymbol{w}' &) & \text{(using Lemma 9.3.35).}
\end{array}
$$

The second equality is a syntactical equality when the vocabulary is $\mathcal{V}_1^{\mathbb{N}}$. For the vocabulary $\mathcal{V}_2^{\mathbb{N}}$, the second equality follows from Lemma 9.3.25.

□

9.4 The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$

The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ is given in this section. Recall that this algorithm takes as input an automaton $\mathcal{A}$ and the algorithm accepts if $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0[\mathcal{V}]/\nu$-definable.

Two lemmas concerning $\mathbb{A}_{\mathcal{V}'_\iota,6}$ and $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ are now given. It should be noted that here, the formula ϕ is only restricted by ν, but neither by the sets ζ, β nor by a restricted vocabulary. That is, this lemma concerns all logics studied in Section 7.2.

The set $\mathbb{A}_{\mathcal{V}'_\iota,6}$ of automata is the last set of the sequence announced in the introduction of Chapter 9. Another name is given to it.

***Definition 9.4.1** ($\mathbb{A}_{\mathcal{V}'_\iota}$)**.** Let $\mathbb{A}_{\mathcal{V}'_\iota}$ denote $\mathbb{A}_{\mathcal{V}'_\iota,6}$.

Lemma 9.4.2. *The set $\mathbb{A}_{\mathcal{V}'_\iota}$ is closed under taking the quotient of automaton.*

Proof. Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota}$ and $\mathcal{A}'$ be a quotient of $\mathcal{A}$ by a morphism μ. Let q' be a cyclic state of $\mathcal{A}'$, then, there exists a cyclic state q of $\mathcal{A}$ such that $\mu(q) = q'$. By Definition 9.1.9, $\mathcal{A}_q$ is minimal, hence $\mathcal{A}_q = \mathcal{A}_{q'}$. Since Definitions 9.1.9, 9.2.4, 9.2.13, 9.3.4, 9.2.17 and 9.3.14, only depends of the state q and of states accessible by q, then the automaton $\mathcal{A}'$ belongs to $\mathbb{A}_{\mathcal{V}'_\iota}$. □

The following lemma states that any set $R \subseteq \mathbb{N}^d$ which is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable is accepted by an automaton of $\mathbb{A}_{\mathcal{V}'_\iota}$.

Lemma 9.4.3. *For each $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, the automaton $\mathcal{A}_{\phi,\mathbb{N}}$ given in Definition 7.2.33, belongs to $\mathbb{A}_{\mathcal{V}'_\iota}$.*

Proof. The proof is by induction on the number of states of $\mathcal{A}_{\phi,\mathbb{N}}$. Two cases must be considered, depending on whether $\phi \in \Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$ or not. Let us first suppose that $\phi \in \Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$, then it is proven in Lemma 9.4.3 that $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota}$.

Let us now suppose that $\phi \notin \Sigma_0[\mathcal{V}'_\iota]/\cdot,\cdot,\nu$, then by Definition 7.2.33, the initial state of $\mathcal{A}_{\phi,\mathbb{N}}$ is not cyclic, hence the induction hypothesis can be used on $\mathcal{A}_{\boldsymbol{a}^{-1}\phi}$ for all letter $\boldsymbol{a} \in A_b^d$. Hence, for each q distinct from the initial state, $\mathcal{A}_q \in \mathbb{A}_{\mathcal{V}'_\iota}$.

Since the definition 9.3.14 only considers the cyclic states and that the initial state of $\mathcal{A}_{\phi,\mathbb{N}}$ is not cyclic, $\mathcal{A}_{\phi,\mathbb{N}} \in \mathbb{A}_{\mathcal{V}'_\iota}$. □

This lemma admits this corollary:

Corollary 9.4.4. *Let $\mathcal{A}$ be a minimal automaton which accepts a $\Sigma_0[\mathcal{V}]/\nu$-definable set. The set of cyclic states of $\mathcal{A}$ is closed under taking transition.*

Proof. Since $\mathcal{A}$ accepts a $\Sigma_0[\mathcal{V}]/\nu$-definable set, there exists a $\Sigma_0[\mathcal{V}]/\nu$-formula ϕ such that $\mathcal{A} = \mathcal{A}_{\phi,\mathbb{N}}$. By Lemma 9.4.3, $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota}$, hence $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,1}$. By Definition 9.1.9, the corollary holds. □

The second lemma states that each automaton of $\mathbb{A}_{\mathcal{V}'_\iota}$ accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set.

Lemma 9.4.5. *For each $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota}$, the set $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.*

Proof. By Proposition 7.2.10, it suffices to prove that for each cyclic state q, the automaton $\mathcal{A}_q$ accepts a $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set.

Let m be the least common multiple of the $\mathrm{LoopSize}(C, I)$ for each strongly connected component C and each $\mathbb{E}\mathbb{S}_C$-class I. By Lemma 7.3.32, it is enough to prove that for all words $\boldsymbol{w}, \boldsymbol{w}' \in \left(A_b^d\right)^+$ ending by $\mathbf{0}$, $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}) = \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}')$ implies $\boldsymbol{w} \in \underline{\mathcal{A}_q} \Longleftrightarrow \boldsymbol{w}' \in \underline{\mathcal{A}_q}$.

Let $\boldsymbol{w}, \boldsymbol{w}' \in \left(A_b^d\right)^+$ ending by $\mathbf{0}$, such that $\mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}) = \mathrm{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}'_\iota}(\boldsymbol{w}')$. Let us assume that $|\boldsymbol{w}'| \leq |\boldsymbol{w}|$, then let $\boldsymbol{w}'' = \boldsymbol{w}'\mathbf{0}^{|\boldsymbol{w}|-|\boldsymbol{w}|}$. Then $|\boldsymbol{w}| = |\boldsymbol{w}''|$. Since $\mathcal{A}_q$ is an automaton over $\mathbb{N}$, $\boldsymbol{w}' \in \underline{\mathcal{A}_q}$ if and only if $\boldsymbol{w}'' \in \mathcal{A}_q$. It then suffices to prove that $\boldsymbol{w} \in \underline{\mathcal{A}_q} \Longleftrightarrow \boldsymbol{w}'' \in \underline{\mathcal{A}_q}$.

Proposition 9.3.17 states that $\delta(q, \boldsymbol{w})$ and $\delta(q, \boldsymbol{w}'')$ are both equal to the same state. Then, by transitivity, $\delta(q, \boldsymbol{w}) = \delta(q, \boldsymbol{w}')$, which implies that $\boldsymbol{w} \in \underline{\mathcal{A}_q} \Longleftrightarrow \boldsymbol{w}'' \in \underline{\mathcal{A}_q}$. □

9.4.1 The algorithm

The algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$, announced in the proof of Theorem 7.1.14 is now given. This algorithm accepts if and only if there Exists a Quantifier-Free formula which defines the set accepted by the automaton.

***Algorithm 9.4.6** ($EQF(\mathcal{V}_\iota^{\mathbb{N}})$)**.** Let $\mathcal{A}$ be an automaton over the alphabet A_b^d. The algorithm computes the minimal automaton $\mathcal{A}'$ of $\mathcal{A}$. The algorithm of Lemma 9.3.16 is then applied to $\mathcal{A}'$.

Lemma 9.4.7. *The algorithm* $\mathrm{EQF}(\mathcal{V}_\iota^{\mathbb{N}})$ *runs in time* $O\left(nb^d(\log(n) + 3^d d)\right)$ *over an automaton* $\mathcal{A}$ *with* n *states, and it time* $O\left(nb^d 3^d d\right)$ *if* $\mathcal{A}$ *is minimal.*

Proof. Since:

- minimization runs in times $O\left(n\log(n)b^d\right)$, and
- the algorithm of Lemma 9.3.16 runs in time $O\left(nb^d 3^d d\right)$,

the whole algorithm runs in time $O\left(nb^d(\log(n) + 3^d d)\right)$, and if $\mathcal{A}$ is minimal, in time

$$O\left(nb^d 3^d d\right).$$

□

Finally, it is proven that $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ accepts exactly the automaton which accepts a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable set.

Theorem 9.4.8. *Let* $\nu \subseteq [d-1]$. *Let* $\mathcal{A}$ *be an automaton over the alphabet* A_b^d *with* n *states. The algorithm* $\mathrm{EQF}(\mathcal{V}_\iota^{\mathbb{N}})$ *accepts if and only if* $\overline{\mathcal{A}}^{\mathbb{N}}$ *is* $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$*-definable.*

Proof. Let $\mathcal{A}$ be an automaton over the alphabet A_b^d. Let us first prove that if $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ accepts $\mathcal{A}$ then $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

Let $\mathcal{A}'$ be the minimal automaton of $\mathcal{A}$, by construction $\overline{\mathcal{A}}^{\mathbb{N}} = \overline{\mathcal{A}'}^{\mathbb{N}}$, hence it remains to prove that $\overline{\mathcal{A}'}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable. If $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ accepts, then the algorithm of Lemma 9.3.16 accepts $\overline{\mathcal{A}'}^{\mathbb{N}}$, hence $\overline{\mathcal{A}'}^{\mathbb{N}}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota'}$. Then, by Lemma 9.4.5, the automaton $\overline{\mathcal{A}'}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable.

Let us now prove that if $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-definable, then $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ accepts $\mathcal{A}$. By hypothesis, there exists $\phi \in \Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$ such that $\overline{\mathcal{A}}^{\mathbb{N}} = \overline{\phi}^{\mathbb{N}}$. By Lemma 9.3.6, $\mathcal{A}_{\phi,\mathbb{N}} \in \mathbb{A}_{\mathcal{V}_\iota'}$. Since $\mathcal{A}_{\phi,\mathbb{N}}$ is minimal and since accepts the same language than $\mathcal{A}$, $\mathcal{A}_{\phi,\mathbb{N}}$ is the minimal automaton of $\mathcal{A}$. Then the automaton $\mathcal{A}'$ of the Algorithm $EQF(\mathcal{V}_\iota^{\mathbb{N}})$ is $\mathcal{A}_{\phi,\mathbb{N}}$, and $\mathcal{A}'$ is accepted by the algorithm of Lemma 9.3.16. □

Chapter 10

The algorithm *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$

Recall that the algorithm *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$ was announced in Section 7.2.1.2. It takes as input a minimal initially-cyclic automaton $\mathcal{A} = \left(Q, A_b^d, \delta, q_0, F\right)$ over A_b^d, with n states, which accepts a $\Sigma_0[\mathcal{V}]/\nu$-definable set, and outputs a $\Sigma_1[\mathcal{V}]/\nu$-formula $\psi_{\mathcal{A}}$ of polynomial size, which defines $\overline{\mathcal{A}}^{\mathbb{N}}$. The case where $\mathcal{A}$ is not initially-cyclic is reduced to the case where $\mathcal{A}$ is initially-cyclic in Theorem 7.2.14 using Algorithm 7.2.13.

In this section, let $\mathcal{A}$ be a minimal initially-cyclic automaton which accepts a $\Sigma_0[\mathcal{V}]/\nu$-definable set. By Lemma 9.4.5, there exists a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\cdot,\cdot,\nu$-formula ϕ which defines $\overline{\mathcal{A}}^{\mathbb{N}}$. By Lemma 9.4.3, $\mathcal{A}$ belongs to $\mathbb{A}_{\mathcal{V}_\iota'}$. Since $\mathcal{A}$ and $\mathcal{A}_{\phi,\mathbb{N}}$ are minimal and accept the same language, $\mathcal{A}$ is isomorphic to $\mathcal{A}_{\phi,\mathbb{N}}$. Let us ignore the isomorphism and consider that $\mathcal{A} = \mathcal{A}_{\phi,\mathbb{N}}$.

Recall that, for each state P of $\mathcal{A}$, the notations $\mathbb{O}_P$, $\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{L}_P$ and $\mathbb{B}_P$, are introduced in Section 9.2. It is proven in Section 9.2 that considering P as a state of $\mathcal{A}_{\phi,\mathbb{N}}$ or as an element of $\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ leads to two equivalent definitions of $\mathbb{O}_P$, $\mathbb{E}\wr\mathbb{S}_P$, $\mathbb{L}_P$ and $\mathbb{B}_P$. It remains to compute $\mathbb{E}_P$, $\mathbb{S}_P$, $\textsc{modulo}_m[P]$ and $\textsc{length}_{m,b}[P]$.

An algorithm similar to *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$, which is simpler but has greater time complexity, is given in Section 10.1. The relations $\mathbb{E}$ and $\mathbb{S}$ are considered in Section 10.2. The modular part is considered in Section 10.3. The algorithm is finally given in Section 10.4.

10.1 A polynomial-time algorithm for a fixed dimension d.

Before giving the algorithm *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$, a similar but simpler algorithm is given in this section. When the dimension d is fixed, this algorithm also runs in polynomial time.

The algorithm is given in Section 10.1.1, and it is explained in Section 10.1.2 how to adapt this simple algorithm in order to obtain a polynomial-time algorithm *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$.

10.1.1 The algorithm

An algorithm which outputs a $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula which defines $\overline{\mathcal{A}}^{\mathbb{N}}$ is given in this section.

By Corollary 7.3.33, a $\Sigma_0\left[\mathcal{V}_\iota'\right]/\zeta,\beta,\nu$-definable set is union of sets $\overline{T}^{\mathcal{V}_\iota'(m),\zeta,\beta}$ for some $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops T. Furthermore, for each $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, the formula $\phi_T(\boldsymbol{x}) \in \Sigma_0\left[\mathcal{V}_\iota'(m)\right]/\zeta,\beta,\nu$ defines

$\overline{T}^{\mathcal{V}_\iota'(m),\zeta,\beta}$. This formula is introduced in Notation 7.3.30.

Intuitively, the formula $\psi_{\mathcal{A}}$ is the disjunction of the formulas $\phi_T(\boldsymbol{x})$ for $T \in \overline{\phi}^{\mathbb{Z}}$. The only trouble is that the number of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops is not polynomially-bounded in the size of the automaton. Let us now give a upper bound on this number.

For each $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$, an element of $\{\emptyset,\{\mathbb{E}\},\{\mathbb{S},\mathbb{L}\},\{\mathbb{P},\mathbb{G}\},\{\mathbb{L}\},\{\mathbb{G}\}\}$ is associated to each pair of positions. An element of $\{\emptyset,\{\mathbb{O}\},\{\mathbb{B}\}\}$ and an element of $[m-1]$ is associated to each position. Hence the cardinality of $\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ is:

$$O\Big(6^{(d^2)} \times 4^d \times m^d\Big) = O\Big(6^{(d^2)} \times (4m)^d\Big).$$

This number is not polynomial in the length of the input, because of the term d^2 in exponent and because of the term m^d. Note however that, when d is assumed to be constant, this idea leads to the following polynomial time algorithm.

Algorithm 10.1.1. The algorithm runs on each $(\nu,\mathcal{V}_\iota')^m$-top T. For each T, the algorithm computes a word $\boldsymbol{w}_T \in \left(A_b^d\right)^*$ such that $\mathrm{TOP}^m_{\nu,\mathcal{V}_\iota'}(\boldsymbol{w}_T) = T$, using the algorithm of Lemma 7.3.10. The algorithm then computes the state $P_T = \delta(q_0,\boldsymbol{w}_T)$. The algorithm outputs the disjunction of the formulas $\phi_T(\boldsymbol{x})$ for each T such that $P_t \in F$. Here, $\phi_T(\boldsymbol{x})$ is the formula described in the proof of Lemma 7.3.32.

It is easy to prove that this algorithm accepts the same language as the automaton $\mathcal{A}$. In order to prove that this algorithm runs in polynomial time, it suffices to prove that m is polynomial in the number of states of $\mathcal{A}$. It is not done here as a more efficient algorithm is given in the rest of this chapter.

Let us give two examples of classes of automata which show how the number of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops is not polynomial bounded by the number of states.

Example 10.1.2 (The modular case)**.** Consider $m \in \mathbb{C}_b$ such that $\omega_{b,m} = 1$. Consider the dimension $d = 2$ and the base $b = 2$. Let $R = \left\{(x_0,x_1) \in \mathbb{N}^2 \mid x_0 + x_1 \equiv 0 \mod m\right\}$. It is accepted by the automaton $([m-1],\{0,1\},+,0,\{0\})$.

Note that there are at least 2^m $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-tops while there are m states.

Example 10.1.3 (The order case)**.** The automaton $\left(\{q_0\},A_b^d,(q_0,\boldsymbol{a}) \mapsto q_0,q_0,\{q_0\}\right)$ accepts $\mathbb{N}^d$. This automaton has one state. For $m = 1$, as stated above, the number of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top is $O\Big(6^{(d^2)}4^d\Big)$. Hence the number of $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top is not polynomially-bounded in the length of the automaton.

10.1.2 Reducing the set of consider states

The algorithm $CEF'(\mathcal{V}_\iota^{\mathbb{N}})$ is similar to Algorithm 10.1.1. It outputs a $\Sigma_1[\mathcal{V}]/\nu$-formula $\psi_{\mathcal{A}}$ which is, mainly, a disjunction of the formulas $\chi_P(\boldsymbol{x})$ for the states P of $\mathcal{A}$. Intuitively, $\chi_P(\boldsymbol{x})$ must define the union of the $\overline{T}^{\mathcal{V}_\iota'(m),\zeta,\beta}$ for $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $\Downarrow_\phi T = P$.

More precisely, $CEF'(\mathcal{V}_\iota^{\mathbb{N}})$ outputs a disjunction of formulas $\chi_P(\boldsymbol{x})$, for only some states P. In this section, the reason for this restriction is given and the set of states P considered in this disjunction is characterized.

Note that, by Definition 2.3.6, the automaton $\mathcal{A}$ accepts a word $\boldsymbol{w}$ if and only if it accepts $\boldsymbol{w}\mathbf{0}$. Hence, the sets:

$$\left\{\overline{\boldsymbol{w}}^{\mathbb{N}} \mid \boldsymbol{w} \in \left(A_b^d\right)^*, \delta(q_0,\boldsymbol{w}) \in F\right\}$$

equals

$$\left\{\overline{\boldsymbol{w}}^{\mathbb{N}} \mid \boldsymbol{w} \in \left(A_b^d\right)^*, \delta(q_0,\boldsymbol{w}) \in F, |\boldsymbol{w}| \equiv 0 \mod \omega_{b,m}, \mathbb{B}_{\boldsymbol{w}} = \emptyset\right\}.$$

This equality implies that the above-mentioned disjunction of formula $\psi_{\mathcal{A}}$, computed by *CEF'*($\mathcal{V}_\iota^{\mathbb{N}}$) can be restricted to states P such that P is accessible from q_0 by a word $\boldsymbol{w} \in \left(A_b^d\right)^*$ such that $|\boldsymbol{w}| \equiv 0 \mod \omega_{b,m}$ and $\mathbb{B}_{\delta(q_0,\boldsymbol{w})} = \emptyset$. That is, a state P such that $\textsc{length}_{m,b}[P] = 0$ and $\mathbb{B}_P = 0$.

Let us a give a name to this set of states.

Definition 10.1.4 ($\mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $\mathbb{POP}^{m,0,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $\mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$)**.** Let $\mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be the set of $P \in \mathbb{POP}^{m}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $\textsc{length}_{m,b}[P] = 0$ and $\mathbb{B}_P = 0$. Let $\mathbb{POP}^{m,0,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} = \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \cap \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} = \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \cap \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

10.2 Considering $\mathbb{O}$, $\mathbb{E}$, $\mathbb{S}$ and $\mathbb{B}$

In this section, some results regarding the relations $\mathbb{E}$ and $\mathbb{S}$ are given. The values of $\mathbb{E}_P$ and $\mathbb{S}_P$ are defined in Section 10.2.1. The values of the relations $\mathbb{O}_P$, $\mathbb{E}_P$, $\mathbb{S}_P$ and $\mathbb{B}_P$ for different states P of a strongly connected component are considered in Section 10.2.2.

10.2.1 The $\mathbb{E}_P$ and $\mathbb{S}_P$

By Definition 7.3.17, having ζ, β and $\mathbb{E}\wr\mathbb{S}_P$ directly gives $\mathbb{E}_P$ and $\mathbb{S}_P$. Let us now define a pair of sets $\zeta_{\mathcal{A}}$ and $\beta_{\mathcal{A}}$ such that the set $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0[\mathcal{V}_\iota']/\zeta_{\mathcal{A}},\beta_{\mathcal{A}},\nu$-definable.

Lemma 10.2.1. *The set $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0[\mathcal{V}_\iota']/\left([d-1] \setminus \left(\mathbb{B}_{q_0}\right)\right),\mathbb{B}_{q_0},\nu$-definable.*

Proof. By Lemma 9.1.14 $q_0 \cdot \left[\emptyset;\mathbb{B}_{q_0}\right] = q_0$, hence $\delta(q_0,\left[\emptyset;\mathbb{B}_{q_0}\right]) = q_0$. Note that $\beta_{\left[\emptyset;\mathbb{B}_{q_0}\right]} = \mathbb{B}_{q_0}$ and $\zeta_{\left[\emptyset;\mathbb{B}_{q_0}\right]} = [d-1] \setminus \mathbb{B}_{q_0}$. By Proposition 7.2.31, $\overline{\mathcal{A}}^{\mathbb{N}}$ is $\Sigma_0[\mathcal{V}_\iota']/\left([d-1] \setminus \left(\mathbb{B}_{q_0}\right)\right),\mathbb{B}_{q_0},\nu$-definable. □

Let us now give a name to those precise values ζ and β.

***Definition 10.2.2** ($\zeta_{\mathcal{A}}$, $\beta_{\mathcal{A}}$)**.** Let $\zeta_{\mathcal{A}} = [d-1] \setminus \mathbb{B}_{q_0}$ and $\beta_{\mathcal{A}} = \mathbb{B}_{q_0}$.

The notations $\mathbb{E}_P$, $\mathbb{S}_P$ and $\mathbb{L}_P$ are now introduced.

***Definition 10.2.3** ($i\ \mathbb{E}_P\ j$, $i\ \mathbb{S}_P\ j$, $i\ \mathbb{L}_P\ j$)**.** Let $i,j \in [d-1]$ and P be a state of $\mathcal{A}$. Then let $i\ \mathbb{E}_P\ j$ denote that $i\ \mathbb{E}\wr\mathbb{S}_P\ j$ and $(i \in \zeta_{\mathcal{A}}) \Longleftrightarrow (j \in \zeta_{\mathcal{A}})$ and $(i \in \beta_{\mathcal{A}}) \Longleftrightarrow (j \in \beta_{\mathcal{A}})$. Let $i\ \mathbb{S}_P\ j$ denote that $i\ \mathbb{E}\wr\mathbb{S}_P\ j$ and $i \in \beta_{\mathcal{A}}$ and $j \in \zeta_{\mathcal{A}}$. Finally, let $i\ \mathbb{L}_P\ j$ denote that either $i\ \mathbb{L}\overline{\mathbb{S}}_P\ j$ or $i\ \mathbb{S}_P\ j$ hold.

10.2.2 Strongly connected component

The following lemma shows that the values of $\mathbb{O}_P$, $\mathbb{E}_P$, $\mathbb{S}_P$ and $\mathbb{B}_P$ are constant on each strongly connected component. This lemma only extends the local properties given in Section 9.2 in order to obtain a property on strongly connected components.

The set of strongly connected component is computed by Algorithm 7.2.11. It is now shown that a more efficient algorithm exists in the special case considered in this part.

***Lemma 10.2.4** (Strongly connected component)**.** The set of strongly connected component of $\mathcal{A}$ is computable in time $O\left(n2^d\right)$ where n is the number of state of the automaton.

Proof. By Lemma 9.3.35, if a state q is accessible from q' by an A_b^d-word, it is accessible by a $\{[K;\emptyset],[\emptyset;K] \mid K \subseteq [d-1]\} \cup \{\langle\emptyset;\emptyset\rangle\}$-word. Hence it suffice to restrict Algorithm 7.2.11 to the alphabet $\{[K;\emptyset],[\emptyset;K]\} \cup \{\langle\emptyset;\emptyset\rangle \mid K \subseteq [d-1]\}$, whose cardinality is $O\left(2^d\right)$. □

Lemma 10.2.5. *Let C be a strongly connected component of $\mathcal{A}$. Let P and O be states of C, then $P \overset{\mathbb{OESB}}{\cong} O$.*

Proof. Let $P, O \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be two states belonging to the same strongly connected component, and let $\boldsymbol{w} \in \left(A_b^d\right)^*$ be such that $P = O \circ_\phi \boldsymbol{w}$. By Corollary 9.3.13, $P \overset{\mathbb{OEB}}{\preccurlyeq} O$. By symmetry, $O \overset{\mathbb{OEB}}{\preccurlyeq} P$. Since $P \overset{\mathbb{OEB}}{\preccurlyeq} O$ and $O \overset{\mathbb{OEB}}{\preccurlyeq} P$, by Lemma 8.1.13, $P \overset{\mathbb{OEB}}{\cong} O$.

Since $P \overset{\mathbb{OB}}{\cong} O$ and $P = O \circ_\phi \boldsymbol{w}$, by Corollary 9.3.13, $P \overset{\mathbb{S}}{\preccurlyeq} O$. By symmetry $O \overset{\mathbb{S}}{\preccurlyeq} P$. Since $P \overset{\mathbb{OESB}}{\preccurlyeq} O$ and $O \overset{\mathbb{OESB}}{\preccurlyeq} P$, by Lemma 8.1.13, $P \overset{\mathbb{OESB}}{\cong} O$. □

By Lemma 10.2.5, the values of $\mathbb{O}_P$, $\mathbb{E}_P$, $\mathbb{S}_P$ and $\mathbb{B}_P$ are functions of the strongly connected component of P, hence the following notations are introduced.

***Definition 10.2.6** ($\mathbb{O}_C$, $\mathbb{E}_C$, $\mathbb{S}_C$, $\mathbb{B}_C$)**.** Let $\mathcal{A} \in \mathbb{A}_{\mathcal{V}'_\iota,3}$, let C be a strongly connected component of $\mathcal{A}$, and let $P \in C$. Then let $\mathbb{O}_C$ denote $\mathbb{O}_P$, let $\mathbb{E}_C$ denote $\mathbb{E}_P$, let $\mathbb{S}_C$ denote $\mathbb{S}_P$ and let $\mathbb{B}_C$ denote $\mathbb{B}_P$.

By Lemma 10.2.5, the values defined above do not depend on the choice of $P \in C$.

It has been proved that two elements of the same strongly connected component are $\overset{\mathbb{OESB}}{\cong}$-equivalents, the inverse is now proved, using the definition $(P - O)_m$ of a word whose right action maps O to P.

Definition 10.2.7 ($(P - O)_m$)**.** Let $O, P \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ such that $O \overset{\mathbb{OESB}}{\cong} P$, let $(P - O)_m$ denote:

$$\Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1}\left[\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)),m)}\Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1}\left[\emptyset;\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right].$$

Here, $\mathrm{mod}(n,m)$ denotes the only integer of $[m-1]$ congruent to n modulo m.

Since $\textsc{modulo}_m[P]_{\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)}$ and $\textsc{modulo}_m[P]_{\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)}$ both belong to $[m-1]$ or both belong to $\{1,\ldots,m\}$:

$$\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)),m)$$

is

$$\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) + c$$

where c is 0 if

$$\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) \geq \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)),$$

and is m otherwise.

Lemma 10.2.8. *Let $O, P \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be such that $O \overset{\mathbb{OESB}}{\cong} P$. Then $P \overset{\mathbb{L}}{\sqsubseteq} O \cdot (P - O)_m$.*

Proof. It easily follows from Lemma 9.1.14. □

Note that this result holds because ϕ belongs to $\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\cdot,\cdot,\nu$, hence, there is a one to one correspondence between $\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and states of $\mathcal{A}_{\phi,\mathbb{N}}$. This statement does not hold in general, and, for example, does not hold on the automaton pictured in Figure 7.5.

The notation $(P - O)_m$ is justified by the following corollary.

Corollary 10.2.9. *Let $O \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and $P \in \mathbb{POP}^{m,0,min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be such that $O \overset{\mathbb{OESB}}{\cong} P$, then $P = O \circ_\phi (P - O)_m$.*

Proof. This results is a direct consequence of Lemma 10.2.8 and of the definition of $\Downarrow_\phi$ and of $\mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$. □

This corollary admits another corollary.

Corollary 10.2.10. *Let $O, P \in \mathbb{POP}^{m,0,min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ such that $O \overset{\mathbb{OESB}}{\cong} P$, then O and P belong to the same strongly connected component.*

Proof. By symmetry, it suffices to prove that O is accessible from P, which follows from Lemma 10.2.8. □

10.2.3 Encoding of $\mathbb{L}$: $\leq$ or $<$

Note that, given a word $\boldsymbol{w}$, $\mathbb{E}\wr\mathbb{S}_{\delta(q_0,\boldsymbol{w})}$ is not necessarily equal to $\mathbb{E}\wr\mathbb{S}_{\boldsymbol{w}}$. There may exist $i, j \in [d-1]$ such that $i\ \mathbb{L}_{\delta(q_0,\boldsymbol{w})}\ j$ while $i\ \mathbb{E}_{\boldsymbol{w}}\ j$. As explained in Section 8.3.1 before the example of Figure 8.2c, when $(i \in \zeta_{\mathcal{A}}) \Longleftrightarrow (j \in \zeta_{\mathcal{A}})$ and $(i \in \beta_{\mathcal{A}}) \Longleftrightarrow (j \in \beta_{\mathcal{A}})$, sometimes, $\mathbb{L}ij$ represents "$x_i < x_j$", and sometimes "$x_i \leq x_j$". Similarly, for $i \in \zeta_{\mathcal{A}}$ and $j \in \beta_{\mathcal{A}}$, $\mathbb{L}ij$ represents "$x_i < x_j + 1$", and sometimes "$x_i \leq x_j + 1$".

In this section, it is tested, for each pair (I, J) of $\mathbb{E}\wr\mathbb{S}_P$-classes whether $I\ \mathbb{L}_P\ J$ should be encoded as $x_I < x_J$ or as $x_I \leq x_J$ in the formula χ_P generated by *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$ for the state P. Similarly, it is tested whether $i \notin \mathbb{O}_P$ means that $x_i \neq 0$ must appear in the formula generated by *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$ for the state P.

Definition 10.2.11 ($\mathfrak{E}$, $\mathfrak{O}$)**.** For a state $P \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ of $\mathcal{A}$ and for a pair (i, j) of $\mathbb{E}\wr\mathbb{S}_P$-classes, let $i\ \mathfrak{E}_P\ j$ (respectively, $i \in \mathfrak{O}_P$) denote that there exists $O \in \mathbb{TOP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ with $i\ \mathbb{E}\wr\mathbb{S}_O\ j$ (respectively $i \in \mathbb{O}_O$) and $\Downarrow_\phi O = P$.

Let us now give an algorithm which computes $\mathfrak{E}$.

***Algorithm 10.2.12** ($\mathfrak{E}$)**.** Let us first give a method *prop*(P,i,j), for P a state and i, j two $\mathbb{E}\wr\mathbb{S}_P$-classes. This method propagates the information $i\ \mathfrak{E}_O\ j$ to states O accessible from P by words w such that $i\ \mathbb{E}\wr\mathbb{S}_w\ j$ for all $w_i = w_j$.

If $i\ \mathfrak{E}_P\ j$ does not hold, then the algorithm sets $i\ \mathfrak{E}_P\ j$ and then runs on every set $K \subseteq [d-1]$ which contains $\{i, j\}$ or which is disjoint from it. For each K, the method calls *prop*$(\delta(P,[\emptyset;K]),i,j)$, *prop*$(\delta(P,[K;\emptyset]),i,j)$ and *prop*$(\delta(P,\langle\emptyset;\emptyset\rangle),i,j)$.

The main algorithm is now given. The algorithm runs on each $K \subseteq \zeta_{\mathcal{A}}$. For each K, the algorithm runs on all $i, j \in [d-1]$ such that $(i \in K \cup \beta_{\mathcal{A}}) \Longleftrightarrow (j \in K \cup \beta_{\mathcal{A}})$. For each i, j, the algorithm calls *prop*$(\delta(q_0,[K;\emptyset]),i,j)$.

Lemma 10.2.13. *Algorithm 10.2.12 computes $\mathfrak{E}$ in time $O\left(n2^d d^3\right)$ where n is the number of state of the automaton.*

Proof. Let us call S the set of 3-tuples (P,i,j) such that $i\ \mathfrak{E}_P\ j$ is set by the algorithm. Let us first prove that, at the end of the computation, $(P,i,j) \in S$ if and only if $i\ \mathfrak{E}_P\ j$.

Let us first assume that $(P,i,j) \in S$ and let us prove that $i\ \mathfrak{E}_P\ j$, that is, that there exists $O \in \mathbb{TOP}^{m}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ with $\Downarrow_\phi O = P$ and $i\ \mathbb{E}\wr\mathbb{S}_O\ j$. The proof is by induction on the number of times *prop* has been called when (P,i,j) has been added to S. The 3-tuple (P,i,j) could have been added in two cases:

- Either $P = \delta(q_0,[K;\emptyset])$ for some $K \subseteq \zeta_{\mathcal{A}}$, in this case it suffices to consider $O = q_0 \cdot [K;\emptyset]$.

- Or there exists a state P' such that P is $\delta(P,a)$, with a being either $[\emptyset;K]$, $[K;\emptyset]$ or $\langle\emptyset;\emptyset\rangle$. By induction, $i\ \mathfrak{E}_{P'}\ j$, that is, there exists $O' \in \mathbb{TOP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_t'}$ with $i\ \mathbb{E}\wr\mathbb{S}_O\ j$ and $\Downarrow_\phi O' = P'$. In this case it suffices to take $O = O' \cdot a$.

Let us now suppose that $i\ \mathfrak{E}_P\ j$ and let us prove that $(P,i,j) \in S$. Let $O \in \mathbb{TOP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_t'}$ such that $i\ \mathbb{E}_O\ j$ and $\Downarrow_\phi O = P$. By definition of $\mathfrak{E}$, such a O exists. By Lemma 9.3.35, O is accessible by a word $\boldsymbol{w} \in \left(A_b^d\right)^*$ whose first letter $\boldsymbol{a}$ is of the form $[K;\emptyset]$ with $K \subseteq \zeta_{\mathcal{A}}$, and all other letters are of the form $[K;\emptyset]$, $[\emptyset;K]$ and $\langle\emptyset;\emptyset\rangle$ with $(i \in K) \Longleftrightarrow (j \in K)$. Hence $add(\delta(q_0,\boldsymbol{w}'),i,j)$ is called for each prefix $\boldsymbol{w}'$ of $\boldsymbol{w}$.

Let us now consider the computation time. There are $O(n)$ states P and d^2 pairs i,j of $\mathbb{E}\wr\mathbb{S}_P$-classes. There are $O\left(2^d\right)$ sets K.

Each 3-tuple is added at most once to (P,i,j). Computing $O = \delta(P,\langle\emptyset;K\rangle)$ takes time $O(d)$. Hence the time inside the method *prop* is $O\left(n2^d d^3\right)$. Let us now consider the time spent outside of *prop*. The time spent in the main loop is $O\left(d^3\right)$. Finally the time spent in the second loop is $O\left(n2^d d^3\right)$. □

A similar algorithm is now given to compute $\mathfrak{O}$.

***Algorithm 10.2.14** ($\mathfrak{O}$)**.** Let us first give a method $prop(P,i)$, for P a state and $i,j \in [d-1]$. This method propagates the information $i \in \mathfrak{O}_O$ to states O accessible from P by a word w with $w_i \in 0^+$.

If $i \in \mathfrak{O}_P$ is not set, the method sets $i \in \mathfrak{O}_P$ and runs on each set K which does not contains i. For each K, the method calls $prop(\delta(P,[\emptyset;K]),i)$, $prop(\delta(P,[K;\emptyset]),i)$ and $prop(\delta(P,\langle\emptyset;\emptyset\rangle),i)$

The algorithm runs on each $i \in \zeta_{\mathcal{A}}$. For each i, the algorithm calls $add(q_0,i)$.

Lemma 10.2.15. *Algorithm 10.2.12 computes $\mathfrak{O}$ in time $O\left(n2^d d^2\right)$ where n is the number of states of the automaton.*

The algorithm to compute $\mathfrak{O}$ is similar to the algorithm for $\mathfrak{E}$, and so is its proof.

10.3 The modular part

The modular parts of states are considered in this section. Recall that $\mathrm{LoopSize}(P,E)$ is introduced in Definition 9.2.17. The values of $\mathrm{LoopSize}(P,E)$ and $\mathrm{LoopSize}(O,E)$ for two $(\zeta,\beta,\nu,\mathcal{V}_t')^m$-pops P and O belonging to the same strongly connected component are studied in Section 10.3.1. The relation between $\mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)$ and $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is studied in Section 10.3.2. The modular parts of each sets of $\mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_t'}$ are computed in Section 10.3.3. A formula defining the function which sends $\mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)$ to $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is given in Section 10.3.4.

When considering the modular part of a state P, denoted by $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P)$, it is easier to assume that:

- having $i\ \mathbb{S}_P\ j$ implies that $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P,i) = \mathbb{M}^C_{\beta_{\mathcal{A}}}(P,j)$. This is the reason for the introduction of the notation $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ in Definition 8.1.5,
- the modular part belongs to $[m-1]^d$. This property is satisfied by $\textsc{modulo}_m[P]$ but not by $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$.

Note that $\mathbb{M}_{\beta_{\mathcal{A}}}(P,i)$ belongs to $\{1,\dots,m\}$ or to $[m-1]$ depending on whether i is $\mathbb{E}\wr\mathbb{S}_P$-equivalent to a position $j \in \beta_{\mathcal{A}}$ or not. In order to avoid a disjunction in each following proof based on this property, a notation similar to $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is now introduced.

***Definition 10.3.1** ($\beta_{\mathcal{A},C}$)**.** Let C be a strongly connected component of $\mathcal{A}$, then let $\beta_{\mathcal{A},C}$ be the set of positions $i \in [d-1]$ such that there exists $j \in \beta_{\mathcal{A}}$ such that $i\ \mathbb{E}\wr\mathbb{S}_C\ j$.

Equivalently, $\beta_{\mathcal{A},C}$ is the union of $\beta_{\mathcal{A}}$ and of $\mathbb{E}\wr\mathbb{S}_C$-classes which are composed of two $\mathbb{E}_C$-classes.

The main interest of this notation is that, for each $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pop P, $\mathbb{M}_{\beta_{\mathcal{A}}}(P) - \langle \beta_{\mathcal{A},C}; \emptyset\rangle \subseteq [m-1]^d$. This leads us to the following notation:

***Definition 10.3.2** ($\mathbb{M}^C_{\beta_{\mathcal{A}}}(P)$)**.** Let C be a strongly connected component, let $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P)$ denote

$$\mathbb{M}_{\beta_{\mathcal{A}}}(P) - \langle \beta_{\mathcal{A},C}; \emptyset\rangle.$$

Let $P,P' \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ and C and C' be their strongly connected component. Note that, if $P \sqsubseteq P'$ then on the one hand, $\mathbb{M}_{\beta_{\mathcal{A}}}(P) \leq_{\text{lex}} \mathbb{M}_{\beta_{\mathcal{A}}}(P')$ holds, and on the other hand $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) \leq_{\text{lex}} \mathbb{M}^{C'}_{\beta_{\mathcal{A}}}(P')$, does not hold in general. This explains why Definition 10.3.2 was not directly introduced in Section 8.1.2.

Note however that when $P \overset{\text{OESB}}{\cong} O$ then $P \sqsubseteq O$ implies $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) \leq_{\text{lex}} \mathbb{M}^C_{\beta_{\mathcal{A}}}(O)$. Since all strongly connected components are considered separately in the rest of this chapter, there is no trouble in considering this notation.

10.3.1 $[I;\emptyset]$-cycles and LoopSize(C,E)

As in Section 10.2.2, it is shown in this section that LoopSize(P,E) is constant on each strongly connected component.

Lemma 10.3.3. *Let C be a strongly connected component of $\mathcal{A}$. Let E be a $\mathbb{E}\wr\mathbb{S}_C$-class. Let $P,O \in C$ be such that E is $\mathbb{L}_P$- and $\mathbb{L}_O$-maximal. Then LoopSize(P,E) = LoopSize(O,E).*

In order to prove this equality, the following lemma must first be proven.

Lemma 10.3.4. *Let P be a cyclic state of $\mathcal{A}$ such that $\mathbb{B}_P = \emptyset$, let $J_0,\dots,J_{e-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$, then:*

$$\delta(P,\Pi_{i=0}^{e-1}[\emptyset;J_i]) = \delta(P,\Pi_{i=0}^{e-1}\left[\emptyset;\bigcup_{j=i}^{e-1} J_j\right]). \tag{10.1}$$

Proof. The proof is by induction on e. For $e \leq 1$ both terms of Equality (10.1) are syntactically equal. Let us now assume that $e > 1$ and that the lemma holds for $e-1$. Then:

$$\begin{aligned}
&\delta(P, && \Pi_{i=0}^{e-1}[\emptyset;J_i] &&) && \\
=&\delta(P,\Pi_{i=0}^{e-2}[\emptyset;J_i] && [\emptyset;J_{e-1}] &&) && \\
=&\delta(P,\Pi_{i=0}^{e-2}\left[\emptyset;\textstyle\bigcup_j^{e-1} J_i\right] && [\emptyset;J_0] &&) && \text{(using induction)}\\
=&\delta(P,\Pi_{i=0}^{e-3}\left[\emptyset;\textstyle\bigcup_j^{e-1} J_i\right] && [\emptyset;J_{e-2}] && [\emptyset;J_{e-1}] &&) && \\
=&\delta(P,\Pi_{i=0}^{e-1}\left[\emptyset;\textstyle\bigcup_j^{e-1} J_i\right] && [\emptyset;J_{e-2}\cup J_{e-1}] && [\emptyset;J_{e-1}] &&) && \text{(using Equality (9.23))}\\
=&\delta(P, && \Pi_{i=0}^{e-1}\left[\emptyset;\textstyle\bigcup_{j=i}^{e-1} J_j\right]). &&
\end{aligned}$$

□

Lemma 10.3.3 is now proven.

Proof of Lemma 10.3.3. By symmetry, it suffices to prove that $\mathrm{LoopSize}(P,E) \leq \mathrm{LoopSize}(O,E)$. By definition of $\mathrm{LoopSize}(O,E)$, $O \circ_\phi [E;\emptyset]^{\mathrm{LoopSize}(O,E)} = O$, hence $O \cdot [E;\emptyset]^{\mathrm{LoopSize}(O,E)} \sim_\phi O$. Let us prove that $P \cdot [E;\emptyset]^{\mathrm{LoopSize}(O,E)} \sim_\phi P$, since $P \in \mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, it implies that $P \circ_\phi [E;\emptyset]^{\mathrm{LoopSize}(O,E)} = P$, hence that $\mathrm{LoopSize}(P,E) \leq \mathrm{LoopSize}(O,E)$.

As usual, let $\mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(0),\ldots,\mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(\left|\mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1)$ be a sequence of the sets $\mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}$ in $\mathbb{L}_P$-non decreasing order. Furthermore, this time, let us require that $\mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(\left|\mathbb{E}_T^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1) = E$.

Note that, since $\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1) = E$, the set $\bigcup_{j=i}^{e-1} J_j$ is a superset of E for all i. This fact justifies the uses of Equality (9.21) below.

$$
\begin{aligned}
& P\cdot[E;\emptyset]^{\mathrm{LoopSize}(O,E)} \\
\sim_\phi\ & O\cdot((P-O)_m) && [E;\emptyset]^{\mathrm{LoopSize}(O,E)} && \text{(using Corollary 10.2.9)}\\
=\ & O\cdot\Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)),m)} \\
& \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)\right][E;\emptyset]^{\mathrm{LoopSize}(O,E)} && && \text{(using Definition 10.2.7)}\\
=\ & O\cdot\Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)),m)} \\
& \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\emptyset;\bigcup_{j=i}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(j)\right][E;\emptyset]^{\mathrm{LoopSize}(O,E)} && && \text{(using Lemma 10.3.4)}\\
=\ & O\cdot\Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)),m)} \\
& [E;\emptyset]^{\mathrm{LoopSize}(O,E)} && \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\emptyset;\bigcup_{j=i}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(j)\right] && \text{(using Equality (9.21))}\\
=\ & O\cdot\Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)),m)} \\
& [E;\emptyset]^{\mathrm{LoopSize}(O,E)} && \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)\right] && \text{(using Lemma 10.3.4)}\\
=\ & O\cdot[E;\emptyset]^{\mathrm{LoopSize}(O,E)} \\
& \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)),m)} \\
& \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)\right] && && \text{(using Lemma 9.3.26)}\\
=\ & O\cdot\Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)),m)} \\
& \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)\right] && && \text{(using hypothesis about } O)\\
=\ & O\cdot(P-O)_m && && \text{(using Definition 10.2.7)}\\
\sim_\phi\ & P. && && \text{(using Lemma 10.2.8)}
\end{aligned}
$$

□

The preceding lemma let us introduce the following definition.

***Definition 10.3.5** ($\mathrm{LoopSize}(C,E)$)**.** Let $\mathrm{LoopSize}(C,E)$ denote $\mathrm{LoopSize}(P,E)$ for $P \in C$ such that E is a $\mathbb{ES}_C$-class.

Lemma 10.3.6. *The notation $\mathrm{LoopSize}(C,E)$ is correctly defined.*

Proof. It follows from Corollary 10.2.10 that each $\mathbb{E}\wr\mathbb{S}_C$-class is $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$-maximal for some state $P \in C$, and it follows from Lemma 10.3.3 that $\text{LoopSize}(P,E)$ does not depend on the choice of P in C. □

Instead of considering $[m-1]^d$, where m is a value that the algorithm does not know, a notation is now introduced for d-tuple of integers whose component E is less than the size of the $[E;\emptyset]$-cycle.

Definition 10.3.7 (Loop-max_C, $\equiv_{\mod c}$)**.** Let C be a strongly connected component. Let Loop-max_C be the set of $\boldsymbol{c} \in \mathbb{N}^d$ such that, for all $\mathbb{E}\wr\mathbb{S}_C$-class E, $c_i = c_j$ for $i,j \in E$ and $c_E < \text{LoopSize}(C,E)$.

Let $\boldsymbol{x},\boldsymbol{y} \in \mathbb{N}^d$ such that $x_i = x_j$ and $y_i = y_j$ for all $i,j \in [d-1]$ such that $i \ \mathbb{E}\wr\mathbb{S}_C \ j$. Let $\boldsymbol{x} \equiv_{\mod C} \boldsymbol{y}$ denote that, for all $\mathbb{E}\wr\mathbb{S}_C$-class I, $x_I \equiv_{\mod \text{LoopSize}(C,I)} y_I$.

Note that the definition of $(P-O)_m$ uses the integer m, whose value is not known by the algorithm. On the other hand, the values of $\text{LoopSize}(C,E)$ are easy to compute as they are the size of some cycles. Hence, a notation similar to $(P-O)_m$ is now introduced, using $\text{LoopSize}(C,E)$ instead of m.

Definition 10.3.8 ($(P-O)_C$)**.** Let $O,P \in \mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ belonging to the same strongly connected component C, let $(P-O)_C$ denote:

$$\prod_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}\right|-1}\left[\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}(i);\emptyset\right]^{\mod(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}(i))-\mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}(i)),\text{LoopSize}(C,\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}(i)))}\prod_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}\right|-1}\left[\emptyset;\mathbb{E}\wr\mathbb{S}_P^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}(i)\right].$$

Lemma 10.3.9. *Let $O,P \in \mathbb{POP}^{m,0,min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ belonging to the same strongly connected component C. Then $P = O \circ_\phi (P-O)_C$.*

In order to prove this lemma, another lemma must first be proved.

Lemma 10.3.10. *Let P be a state of $\mathcal{A}$ such that $\mathbb{B}_P = \emptyset$, let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint subsets of $[d-1]$. Let $I_0,\dots,I_{e-1}$ be a sequence of unions of J_i's for $i \in [e-1]$. Let $k \in [e'-1]$.*

$$\delta(P,[\emptyset;J_k]\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) = \delta(P,\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]).$$

Proof. The proof consists in applying Lemma 9.3.21 and Corollary 9.3.20.

$$\begin{aligned}\delta(P,[\emptyset;J_k]\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) &= \delta(P,\prod_{i=0}^{e-1}[I_i;\emptyset][\emptyset;J_k]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using Lemma 9.3.21)}\\ &= \delta(P,\prod_{i=0}^{e-1}[I_i;\emptyset]\quad\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]). && \text{(using Corollary 9.3.20)}\end{aligned}$$

□

This lemma admits the following corollary.

Corollary 10.3.11. *Let P be a state of $\mathcal{A}$ in a strongly connected component C such that $\mathbb{B}_C = \emptyset$. Let $J_0,\dots,J_{e'-1}$ be a sequence of pairwise disjoint $\mathbb{E}\wr\mathbb{S}_C$-classes. Let $I_0,\dots,I_{e-1}$ be a sequence of unions of J_i's for $i \in [e-1]$. Let $k \in [e'-1]$ and $n \in \mathbb{N}$.*

$$\delta(P,[J_k;\emptyset]^n\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) = \delta(P,[J_k;\emptyset]^{\mod(n,\mathit{LoopSize}(C,J_k))}\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]).$$

Proof. The use of Lemma 10.3.10 is required because $\mod(n,\text{LoopSize}(C,J_k))$ may be equal to 0. Indeed J_k is not necessary $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$-maximal, but it is $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_{\delta(P,[\emptyset;J_k])}$-maximal, which let us use the definition of $\text{LoopSize}(C,J_k)$, as in Definition 9.2.17.

$$\begin{aligned}&\delta(P,\quad [J_k;\emptyset]^n\quad\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right])\\ =&\delta(P,[\emptyset;J_k][J_k;\emptyset]^n\quad\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using Lemma 10.3.10)}\\ =&\delta(P,[\emptyset;J_k][J_k;\emptyset]^{\mod(n,\text{LoopSize}(C,J_k))}\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]) && \text{(using the definition of LoopSize}(C,J_k))\\ =&\delta(P,\quad [J_k;\emptyset]^{\mod(n,\text{LoopSize}(C,J_k))}\prod_{i=0}^{e-1}[I_i;\emptyset]\prod_{j=0}^{e'-1}\left[\emptyset;J_j\right]). && \text{(using Lemma 10.3.10)}\end{aligned}$$

□

Let us now prove Lemma 10.3.9

Proof. Since $P \circ_\phi [E;\emptyset]^m = P$, $\mathrm{LoopSize}(C,E) = \mathrm{LoopSize}(P,E)$ divides m. Hence:

$$\begin{aligned}\mathrm{mod}(\,\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(j)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(j)),m),\mathrm{LoopSize}(C,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(j))) =\\ \mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(j)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(j)),\mathrm{LoopSize}(C,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(j))).\end{aligned} \tag{10.2}$$

and then:

$$\begin{aligned}
&P\\
&= O \circ_\phi (P - O)_m && \text{(using Corollary 10.2.9)}\\
&= O \circ_\phi \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1} \left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)),m)}\\
&\qquad \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1} \left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right] && \text{(using Definition 10.2.7)}\\
&= O \circ_\phi \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1} \left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i);\emptyset\right]^{\mathrm{mod}(\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)),m),\mathrm{LoopSize}(C,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)))}\\
&\qquad \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1} \left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right] && \text{(using Corollary 10.3.11)}\\
&= O \circ_\phi \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1} \left[\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i);\emptyset\right]^{\mathrm{mod}(\mathbb{M}_{\beta_{\mathcal{A}}}(P,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)) - \mathbb{M}_{\beta_{\mathcal{A}}}(O,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)),\mathrm{LoopSize}(C,\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)))}\\
&\qquad \Pi_{i=0}^{\left|\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1} \left[\emptyset;\mathbb{ES}_P^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right] && \text{(using Equality (10.2))}\\
&= O \circ_\phi (P - O)_C. && \text{(using Definition 10.3.8)}
\end{aligned}$$

□

10.3.2 Set of modular parts

The relation between $\mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)$ and $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is studied in this section. The following lemma states that if a $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop belongs to $\mathbb{POP}^{m,0,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, it implies that some particular elements of $\mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ also belongs to $\mathbb{POP}^{m,0,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

Lemma 10.3.12. *Let $P \in \mathbb{POP}^{m,0,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota''}$, $O \in \mathbb{POP}^{m,0,min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that:*

1. *$P \overset{\mathbb{OESB}}{\cong} O$ and*
2. *$\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) \leq \mathbb{M}^C_{\beta_{\mathcal{A}}}(O)$, where $\leq$ is the component-wise order,*

then $\Downarrow_\phi P \overset{\mathbb{M}}{\cong} P$.

Proof. Note that by Lemma 10.2.8, $O \overset{\mathbb{L}}{\sqsubseteq} P \cdot (O-P)_m$, hence $O \overset{\mathbb{M}}{\cong} P \cdot (O-P)_m$.

For the sake of contradiction, let us assume that $\Downarrow_\phi P \overset{\mathbb{M}}{\ncong} P$. Since $\Downarrow_\phi P \overset{\mathbb{M}}{\ncong} P$ and $\Downarrow_\phi P \overset{\mathbb{M}}{\preccurlyeq} P$, by Lemma 8.1.11, $\Downarrow_\phi P \overset{\mathbb{M}}{\prec} P$, that is, there exists an $\mathbb{ES}_P$-class I such that $\mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P, I) < \mathbb{M}_{\beta_{\mathcal{A}}}(P,I)$ and for all $\mathbb{ES}_P$-class J lexicographically smaller than I, $\mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P, J) = \mathbb{M}_{\beta_{\mathcal{A}}}(P,J)$.

Let us claim that $\left(\Downarrow_\phi P\right) \cdot (O-P)_m \overset{\mathbb{M}}{\prec} P \cdot (O-P)_m$, since $P \cdot (O-P)_m \overset{\mathbb{M}}{\cong} O$, it implies that $\left(\Downarrow_\phi P\right) \cdot (O-P)_m \overset{\mathbb{M}}{\prec} O$. Having both $\left(\Downarrow_\phi P\right) \cdot (O-P)_m \sim_\phi O$ and $\Downarrow_\phi P \cdot (O-P)_m \overset{\mathbb{M}}{\prec} O$ contradict the fact that $O \in \mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$.

Let us prove that $\left(\Downarrow_\phi P\right) \cdot (O-P)_m \overset{\mathbb{M}}{\prec} P \cdot (O-P)_m$. It suffices to prove that:

$$\mathbb{M}^C_{\beta_{\mathcal{A}}}\left(\left(\Downarrow_\phi P\right) \cdot (O-P)_m, I\right) < \mathbb{M}^C_{\beta_{\mathcal{A}}}(P \cdot (O-P)_m, I) \tag{10.3}$$

and that, for each $\mathbb{E}\wr\mathbb{S}_P$-class J lexicographically smaller than I,

$$\mathbb{M}^C_{\beta_{\mathcal{A}}}\left(\left(\Downarrow_\phi P\right) \cdot (O-P)_m, J\right) = \mathbb{M}^C_{\beta_{\mathcal{A}}}(P \cdot (O-P)_m, J). \tag{10.4}$$

Let us prove Inequality 10.3, the proof of Equality 10.4 is similar. Having

$$\begin{aligned}\mathbb{M}^C_{\beta_{\mathcal{A}}}\left(\left(\Downarrow_\phi P\right) \cdot (O-P)_m, I\right) &\equiv \mathbb{M}^C_{\beta_{\mathcal{A}}}\left(\Downarrow_\phi P, I\right) + \mathbb{M}_{\beta_{\mathcal{A}}}(O)I - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I \\ &\equiv \mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)I + \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,I) - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I \mod m\end{aligned}$$

and

$$\begin{aligned}\mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)I + \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,i) - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I &< \mathbb{M}_{\beta_{\mathcal{A}}}(P)I + \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,i) - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I \qquad \text{(using Condition 2)} \\ &< \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,i) < m\end{aligned}$$

imply

$$\mathbb{M}^C_{\beta_{\mathcal{A}}}\left(\left(\Downarrow_\phi P\right) \cdot (O-P)_m, I\right) = \mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)I + \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,I) - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I. \tag{10.5}$$

If follows that:

$$\begin{aligned}\mathbb{M}^C_{\beta_{\mathcal{A}}}\left(\left(\Downarrow_\phi P\right) \cdot (O-P)_m, I\right) &= \mathbb{M}_{\beta_{\mathcal{A}}}(\Downarrow_\phi P)I + \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,I) - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I \qquad \text{(using Equation 10.5)} \\ &< \mathbb{M}_{\beta_{\mathcal{A}}}(P)I \quad + \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,I) - \mathbb{M}_{\beta_{\mathcal{A}}}(P)I \qquad \text{(using Condition 2)} \\ &= \qquad\qquad\quad \mathbb{M}^C_{\beta_{\mathcal{A}}}(O,I).\end{aligned}$$

□

The following lemma considers $\overset{\mathbb{MOESB}}{\cong}$-equivalent $(\zeta,\beta,\nu,\mathcal{V}'_\iota)^m$-pops.

Lemma 10.3.13. *Let $P,O \in \mathbb{POP}^{m,0,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ such that $P \overset{\mathbb{MOESB}}{\cong} O$, then $\Downarrow_\phi P \overset{\mathbb{M}}{\cong} \Downarrow_\phi O$.*

Proof. By symmetry, it suffices to prove that $\Downarrow_\phi P \overset{\mathbb{M}}{\preccurlyeq} \Downarrow_\phi O$.

Since $P \overset{\mathbb{MOESB}}{\cong} O$, by Lemma 9.1.14:

$$O \overset{\mathbb{L}}{\sqsubseteq} P \cdot \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O\right|-1}\left[\emptyset; \mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O(i)\right]. \tag{10.6}$$

Since $O \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, by Equation (10.6),

$$O \sim_\phi P \circ_\phi \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O\right|-1}\left[\emptyset; \mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O(i)\right]. \tag{10.7}$$

Since $P \sim_\phi \Downarrow_\phi P$ by Lemma 8.1.27,

$$P \circ_\phi \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O\right|-1}\left[\emptyset; \mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O(i)\right] \sim_\phi \left(\Downarrow_\phi P\right) \circ_\phi \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O\right|-1}\left[\emptyset; \mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O(i)\right]. \tag{10.8}$$

By transitivity, using Equations (10.7) and (10.8):

$$O \sim_\phi \left(\Downarrow_\phi P\right) \circ_\phi \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O\right|-1}\left[\emptyset; \mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_O(i)\right],$$

which implies that:

$$\Downarrow_\phi O = \left(\Downarrow_\phi P\right) \circ_\phi \Pi_{i=0}^{\left|\mathbb{EIS}_O^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1}\left[\emptyset; \mathbb{EIS}_O^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right]. \tag{10.9}$$

Let us prove by induction on $j \in [\left|\mathbb{EIS}_O^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|]$ that:

$$\left(\Downarrow_\phi P\right) \circ_\phi \Pi_{i=0}^{j-1}\left[\emptyset; \mathbb{EIS}_O^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right] \overset{\mathbb{M}}{\preccurlyeq} \Downarrow_\phi P. \tag{10.10}$$

The case $j = 0$ is trivial as both side of the inequality are syntactically equal. Let us assume that $j > 0$ and that Inequality 10.10 holds for $j-1$. By Lemma 9.1.14, the inequality holds for j.

Hence

$$\begin{array}{rcll} \Downarrow_\phi O & = & \left(\Downarrow_\phi P\right) \circ_\phi \Pi_{i=0}^{\left|\mathbb{EIS}_O^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|-1}\left[\emptyset; \mathbb{EIS}_O^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)\right] & \text{(using Equation 10.9)} \\ & \overset{\mathbb{M}}{\preccurlyeq} & \Downarrow_\phi P. & \text{(using Equation 10.10)} \end{array}$$

□

The results given in this section led us to the introduction of the two notations $\sim_{\phi,C}$ and $\Downarrow_{\phi,C}$, which are the equivalent of $\sim_\phi$ and of $\Downarrow_\phi$ the modular part of states belonging to a strongly connected component C.

Definition 10.3.14. Let C be a strongly connected component of $\mathcal{A}$ such that $\mathbb{B}_C = \emptyset$. Let $\boldsymbol{x}, \boldsymbol{y} \in$ Loop-max$_C$ such that $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{x}) \overset{\mathbb{OESB}}{\cong} C$ and $\textsc{top}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{y}) \overset{\mathbb{OESB}}{\cong} C$.

Let $P \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \cap C$ and $O \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'} \cap C$ be $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops such that $\mathbb{M}^C_{\beta_\mathcal{A}}(P) = \boldsymbol{x}$ and $\mathbb{M}^C_{\beta_\mathcal{A}}(O) = \boldsymbol{y}$. Then let $\Downarrow_{\phi,C} \boldsymbol{x} = \mathbb{M}_{\beta_\mathcal{A}}(\Downarrow_\phi P)$ and let $\boldsymbol{x} \sim_{\phi,C} \boldsymbol{y}$ denote that $\Downarrow_{\phi,C} \boldsymbol{x} = \Downarrow_{\phi,C} \boldsymbol{y}$.

By extension, for $\boldsymbol{x} \in \mathbb{N}^d$, let $\boldsymbol{x'} \in$ Loop-max$_C$, with $\boldsymbol{x} \equiv \boldsymbol{x'} \mod m$. Then $\Downarrow_{\phi,C} \boldsymbol{x} = \Downarrow_{\phi,C} \boldsymbol{x'}$.

By Lemma 10.3.13, in the definition, $\Downarrow_{\phi,C} \boldsymbol{x}$ is independent of the choice of P.

10.3.3 Computing the modular part

In order to compute the $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop associated to each state P, it remains to define $\textsc{modulo}_m[P]$. Equivalently, it suffices to define $\mathbb{M}_{\beta_\mathcal{A}}(P)$. The definition of the set of states of $\mathcal{A}_{\phi,\mathbb{N}}$ is in given in term of $\mathbb{M}_{\beta_\mathcal{A}}(P)$ and not of $\textsc{modulo}_m[P]$, this explain why the following algorithm deals with $\mathbb{M}_{\beta_\mathcal{A}}(P)$.

The two following lemmas show that the value of $\mathbb{M}_{\beta_\mathcal{A}}(P)$ can be deduced from the value of $\mathbb{M}_{\beta_\mathcal{A}}(O)$ for some other state O. Those lemmas lead to Algorithm 10.3.17, which defines $\mathbb{M}_{\beta_\mathcal{A}}(P)$ using the previously computed value of $\mathbb{M}_{\beta_\mathcal{A}}(O)$.

Lemma 10.3.15. *Let $P \in \mathbb{POP}^{m,0,min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ be a state and C its strongly connected component of $\mathcal{A}_{\phi,\mathbb{N}}$ such that $\mathbb{M}^C_{\beta_\mathcal{A}}(P) \neq \mathbf{0}$. There exists $O \in \mathbb{POP}^{m,min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ such that $P = O \circ_\phi \left[I; (\uparrow_{\mathbb{LEIS}_O} I) \setminus I\right]$ for some $\mathbb{EIS}_C$-class I, and $O \overset{\mathbb{M}}{\prec} P$.*

Proof. By hypothesis, there exists an $\mathbb{EIS}_C$-class I such that $\mathbb{M}^C_{\beta_\mathcal{A}}(P, I) > 0$. Let $O' = P \cdot \left[I; (\uparrow_{\mathbb{LEIS}_O} I) \setminus I\right]^m$ and $O = \Downarrow_\phi O'$.

It suffices to see that, by Lemma 9.1.14, $P \overset{\mathbb{L}}{\sqsubseteq} O' \cdot \left[I; (\uparrow_{\mathbb{LEIS}_P} I) \setminus I\right]$. Since $P \in \mathbb{POP}^{m,\min,\,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, $P = O \circ_\phi \left[I; (\uparrow_{\mathbb{LEIS}_P} I) \setminus I\right]$. □

Note that this lemma holds because $i \ \mathbb{S}_P \ j$ implies that $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P,i) = \mathbb{M}^C_{\beta_{\mathcal{A}}}(P,j)$. If $\textsc{modulo}_m[P]_i$ where used in the definition of $\overset{\mathbb{M}}{\prec}$ instead of $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P,i)$, the lemma would not hold.

By this lemma, it is seen that it suffices to assign the modular part of states P such that $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) = \mathbf{0}$. This case is now considered.

Lemma 10.3.16. *Let $P \in \mathbb{POP}^{m,0,min,\ \phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ be a state of $\mathcal{A}_{\phi,\mathbb{N}}$ such that $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) = \mathbf{0}$ where C is its strongly connected component. Let $T^P_{\zeta,\beta,\nu} = T_{\zeta,\beta,\nu} \circ_\phi [S;\emptyset]$ where S is the set of successor positions of P. There exists a sequence $J_0,\dots,J_{e-1}$ of $\mathbb{E}\wr\mathbb{S}_P$-classes such that $P = T^P_{\zeta,\beta,\nu} \circ_\phi \Pi_{i=0}^{e-1}[\emptyset;J_i]$ and $P \overset{\mathbb{M}}{\cong} T^P_{\zeta,\beta,\nu}$.*

Proof. It suffices to see that $P \overset{\mathbb{L}}{\sqsubseteq} T^P_{\zeta,\beta,\nu} \cdot \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_P\right|-1}\left[\emptyset;\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_P(i)\right]$. Since furthermore $P \in \mathbb{POP}^{m,\min,\ \phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $P = T^P_{\zeta,\beta,\nu} \circ_\phi \Pi_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_P\right|-1}\left[\emptyset;\mathbb{E}\wr\mathbb{S}^{\overline{\mathbb{O}}\ \overline{\mathbb{B}}}_P(i)\right]$. □

By this statement, it is seen that it suffices to assign the modular part of the states P such that $O = T^P_{\zeta,\beta,\nu}$.

The algorithm which assign the modular part to each state $P \in \mathbb{POP}^{m,0,\min,\ \phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ is now given. The algorithm which computes the modular is such that, given a state P, every states O with $\mathbb{B}_O$ such that $\mathbb{M}_{\beta_{\mathcal{A}}}(O) <_{\text{lex}} \mathbb{M}_{\beta_{\mathcal{A}}}(P)$ are assigned before P.

***Algorithm 10.3.17** (Modular part of states)**.** The algorithm assign a d-tuple of values $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ to each state P of $\mathcal{A}$. Each $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is first assigned to $+\infty$. Let L be a priority queue (implemented as a binary heap) containing each state, for the lexicographical order over $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$.

Let us first give a method $add(P,\boldsymbol{c})$ which takes as input a state P and a d-tuple of integers $\boldsymbol{c}$. Intuitively, this method is called when it is known that $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is at most $\boldsymbol{c}$. Two cases are considered, depending on whether $P \in L$ or not:

- if $P \notin L$ then $add(P,\boldsymbol{c})$ does nothing
- otherwise $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ is set to $\min_{\text{lex}}((0,\boldsymbol{c}),\mathbb{M}_{\beta_{\mathcal{A}}}(P))$ where $\min_{\text{lex}}$ is the function which returns the lexicographically minimal value.

The main algorithm is now introduced, it is composed of two successive loops:

1. For each set $I \subseteq \zeta_{\mathcal{A}}$, the algorithm calls $add(\delta(P,[I;\emptyset]),\langle I \cup \beta_{\mathcal{A}};\emptyset\rangle)$.
2. While L is not empty:
   - let P be a $\overset{\mathbb{M}}{\prec}$-minimal state belonging to L,
   - if $\mathbb{M}_{\beta_{\mathcal{A}}}(P) = \infty$, the algorithm halts,
   - the algorithm removes P from L and
   - the algorithm runs on each set $I \subseteq [d-1]$. For each I:
     - Let $O = \delta(P,[\emptyset;I])$. The algorithm calls $add\Big(O,\mathbb{M}_{\beta_{\mathcal{A}}}(P)\Big)$.
     - Let $O = \delta(P,[I;\emptyset])$. The algorithm calls $add\Big(O,\mathbb{M}_{\beta_{\mathcal{A}}}(P) + \langle I;\emptyset\rangle\Big)$.

Lemma 10.3.18. *Algorithm 10.3.17 on $\mathcal{A}_{\phi,\mathbb{N}}$ associates to each state P its value $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$. And this algorithm runs in time:*

$$O\Big(n\log(n)2^d d\Big),$$

where n is the number of state of the automaton.

Proof. Let $M(P)$ denotes the value $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ computed by the algorithm. It must be proven that, at the end of the computation, for all $P \in \mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$, $M(P) = \mathbb{M}_{\beta_{\mathcal{A}}}(P)$. Let us prove by induction on $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$ that:

1. when P is removed from L, for all $O \in \mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ with $O \overset{\mathbb{M}}{\prec} P$, O is removed from L,

2. for all $O \in \mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}$ removed from L, $\mathbb{M}_{\beta_{\mathcal{A}}}(O) = M(O)$.

Let us prove that $M(P) = \mathbb{M}_{\beta_{\mathcal{A}}}(P)$, it implies that P is eventually removed from L. Let us first prove that $M(P) \leq_{\text{lex}} \mathbb{M}_{\beta_{\mathcal{A}}}(P)$. It suffices to prove that each call to $add(P,\boldsymbol{c})$ is such that $\mathbb{M}_{\beta_{\mathcal{A}}}(P) \leq_{\text{lex}} \boldsymbol{c}$. A call to $add(P,\boldsymbol{c})$ occurs in two cases, either in Loop 1, in which case this inequality holds by definition of $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$, or in Loop 2, in which case this inequality holds by induction hypothesis.

Let us now prove that $\mathbb{M}_{\beta_{\mathcal{A}}}(P) \leq_{\text{lex}} M(P)$. It suffices to prove that there is a call to $add(P,\mathbb{M}_{\beta_{\mathcal{A}}}(P))$. Two cases must be considered, depending on whether $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) = \mathbf{0}$ or not.

- Let us suppose that $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P) = \mathbf{0}$. Let S be the set of successor positions of P and let $T^P_{\zeta,\beta,\nu} = T_{\zeta,\beta,\nu} \circ_\phi [S;\emptyset]$. Two cases must be considered, depending on whether $P = T^P_{\zeta,\beta,\nu}$ or not.

  - Let us suppose that $P = T^P_{\zeta,\beta,\nu}$, in this case $add(P,\mathbb{M}_{\beta_{\mathcal{A}}}(P))$ is called in in Loop 1.

  - Let us assume that $P \neq T^P_{\zeta,\beta,\nu}$. By Lemma 10.3.16, there exists a sequence $J_0,\dots,J_{e-1}$ of $\mathbb{E}\wr\mathbb{S}_P$-classes such that $P = T^P_{\zeta,\beta,\nu} \circ_\phi \Pi_{k=0}^{e-1}[\emptyset;J_k]$ and $P \overset{\mathbb{M}}{\cong} T^P_{\zeta,\beta,\nu}$. Let $O_j = T^P_{\zeta,\beta,\nu} \circ_\phi \Pi_{k=0}^{j-1}[\emptyset;J_k]$ for $j \in E$; In particular, there a sequence such that $add(O_j,\mathbb{M}_{\beta_{\mathcal{A}}}(T^P_{\zeta,\beta,\nu}))$ is called. Note that $\mathbb{M}_{\beta_{\mathcal{A}}}(T^P_{\zeta,\beta,\nu}) = \mathbb{M}_{\beta_{\mathcal{A}}}(P)$, hence $add(P,\mathbb{M}_{\beta_{\mathcal{A}}}(P))$ is called when $j = e$.

- Otherwise by Lemma 10.3.15, there exists a state O such that $P = O \circ_\phi \Big[I;(\uparrow_{\mathbb{L}\wr\mathbb{S}_O} I)\setminus I\Big]$ and $O \overset{\mathbb{M}}{\prec} P$. By the induction hypothesis 1, $O \overset{\mathbb{M}}{\prec} P$ implies that O is removed from L before P. Since O is already removed from L, by induction hypothesis 2, $M(O) = \mathbb{M}_{\beta_{\mathcal{A}}}(O)$. Hence $add(P,\mathbb{M}_{\beta_{\mathcal{A}}}(P))$ is called before O is removed from L.

Let us now consider the computation time. A call $add(P,\boldsymbol{c})$ runs in time $O(\log(n)d)$, since it must decrease elements in a binary heap of cardinality $O(n)$, and since comparing elements takes time $O(d)$.

There are $O\Big(2^d\Big)$ sets $I \subseteq \zeta_{\mathcal{A}}$. Hence, the first loop of the algorithm runs in time $O\Big(\log(n)2^d d\Big)$.

There are $O(n)$ states P removed from L. Removing the state takes time $O(\log(n))$. There are $O\Big(2^d\Big)$ sets I. The method *add* is then called twice. Hence, the computation time of the main loop is $O\Big(n\log(n)2^d d\Big)$.

Hence the whole algorithm runs in time $O\Big(n\log(n)2^d d\Big)$. □

10.3.4 Defining $\Downarrow_{\phi,C}$

In this section, a $\Sigma_1\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$-formula $\xi_C(\boldsymbol{x};\boldsymbol{z})$ is introduced, which defines the function $\Downarrow_{\phi,C}$. In order to do this, another notation is now introduced, in order to consider the modular values of syntactically equivalent $(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pops.

***Definition 10.3.19** ($l(C,E)$, $t(C,E)$)**.** Let C be a strongly connected component and let E be a $\mathbb{E}\wr\mathbb{S}_C$-class.

Let $l(C,E)$ be the least integer such that $\mathbb{M}^C_{\beta,\mathcal{A}}(P,E) \leq l(C,E)$ for all $P \in C$.

Let $P \in C$ such that $\mathbb{M}^C_{\beta,\mathcal{A}}(P) = (0,l(C,E)\langle E;\emptyset\rangle)$, then, let $t(C,E)$ be $\mathbb{M}^C_{\beta,\mathcal{A}}(P\cdot[E;\emptyset])$.

Recall that $\langle E;\emptyset\rangle \in A_b^d \subseteq \mathbb{N}^d$, hence $l(C,E)\langle E;\emptyset\rangle$ denotes the component-wise multiplication. The d-tuple $\boldsymbol{c} = l(C,E)\langle E;\emptyset\rangle$ is such that $c_i = l(C,E)$ if $i \in E$ and 0 otherwise.

By definition of lexicographical minimality, the $<$-least element i such that $\mathbb{M}^C_{\beta,\mathcal{A}}(t(C,E))_i > 0$ is greatest than the $<$-least element $j \in E$. It easily follows from Lemma 10.3.13 that the definition of $t(C,E)$ does not depend on the choice of P.

Let us now explain how to compute those values.

***Lemma 10.3.20** ($l(C,E)$, $t(C,E)$)**.** The values $l(C,E)$ and $t(C,E)$ are computable in time $O\left(nd^2\right)$.

Proof. The algorithm runs on each strongly connected component C. The algorithm first computes $l(C,E)$. For each C the algorithm runs on each $\mathbb{E}\wr\mathbb{S}_C$-class E. For each E, the algorithm initializes $l(C,E)$ to -1. The algorithm then runs on each state $P \in C$. For each P, the algorithm sets $l(C,E)$ to $\max\left(l(C,E),\mathbb{M}^C_{\beta,\mathcal{A}}(P,E)\right)$.

For each C and E, the algorithm runs on each state P until it finds some state such that $\mathbb{M}^C_{\beta,\mathcal{A}}(P) = l(C,E)\langle E;\emptyset\rangle$. By Lemma 10.3.12, such a P exists. The algorithm then sets $t(C,E)$ to $\mathbb{M}^C_{\beta,\mathcal{A}}(\delta(P,\langle E;\emptyset\rangle))$.

Let us now study the computation time. There are $O(n)$ states $P \in C$, there are $O(d)$ $\mathbb{E}\wr\mathbb{S}_C$-classes, each state is considered at most twice when computing the cycles. Computing each step is done in time $O(d)$. Hence the whole computations runs in time $O\left(nd^2\right)$. □

The following lemma shows how the values $l(C,E)$ and $t(C,E)$ let us define the function $\Downarrow_{\phi,C}$.

Lemma 10.3.21. *Let C be a strongly connected component. Let $\boldsymbol{x} \in \text{Loop-max}_C$ such that $\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{x}) \overset{\mathbb{OESB}}{\cong} C$. Let E be the $\leq_{lex}$-minimal $\mathbb{E}\wr\mathbb{S}_{\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{x})}$-class such that $\mathbb{M}^C_{\beta,\mathcal{A}}\left(\text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{x}),E\right) > l(C,E)$, then*

$$\boldsymbol{x} \sim_{\phi,C} \boldsymbol{x} + t(C,E) - l(C,E)\langle E;\emptyset\rangle.$$

Note that $\boldsymbol{x} + t(C,E) - l(C,E)\langle E;\emptyset\rangle \leq_{\text{lex}} \boldsymbol{x}$, hence this lemma can be used in a proof by induction in order to obtain a d-tuple $\boldsymbol{y}$ such that $\boldsymbol{x} \sim_\phi \boldsymbol{y}$ and $\boldsymbol{y} \in \text{Loop-max}_C$.

Proof. Let $\boldsymbol{w}$ be an expansion of $\boldsymbol{x}$, ending by $\boldsymbol{0}$, whose length is a multiple of $\omega_{b,m}$. Let $P = \text{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}(\boldsymbol{w})$ and let $P' \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ be such that $P' \overset{\mathbb{OESBL}}{\cong} P$ and $\mathbb{M}^C_{\beta,\mathcal{A}}(P') = \mathbb{M}^C_{\beta,\mathcal{A}}(P) + (0,t(C,E) - l(C,E)\langle E;\emptyset\rangle)$. It is straightforward that $P' \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. It remains to prove that $P \sim_\phi P'$.

Let us claim that there exists $O, O' \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ with $O \sim_\phi O'$ such that $P \overset{\mathbb{L}}{\sqsubseteq} O\cdot w$ and $P' \overset{\mathbb{L}}{\sqsubseteq} O'\cdot w$ for some word w. By Lemma 8.1.27, it implies $P \sim_\phi P'$.

Let $O, O' \in \mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$ be such that $O' \overset{\mathbb{OESBL}}{\cong} O \overset{\mathbb{OESBL}}{\cong} P$, $\mathbb{M}^C_{\beta,\mathcal{A}}(O) = (0,l(C,E)\langle E;\emptyset\rangle)$ and $\mathbb{M}^C_{\beta,\mathcal{A}}(O) = t(C,E)$. It is straightforward that O and O' belong to $\mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$. By definition of $t(C,E)$,

$\Downarrow_\phi O = O'$, hence $O \sim_\phi O'$. By Lemma 10.2.8, $P \overset{\mathbb{L}}{\sqsubseteq} O \cdot (P - O)_C$, hence it remains to prove that $P' \overset{\mathbb{L}}{\sqsubseteq} O' \cdot (P - O)_C$, which is a straightforward consequence of Lemma 9.1.14. □

This lemma implies the following corollary.

Corollary 10.3.22. *Let C, E and $\boldsymbol{x}$ be as in Lemma 10.3.21. Then*

$$\boldsymbol{x} \sim_{\phi,C} \boldsymbol{x} + \frac{\boldsymbol{x}}{l(C,E)}(t(C,E) - (0, l(C,E)\langle E;\emptyset\rangle))). \tag{10.11}$$

A formula $\xi_C(\boldsymbol{x};\boldsymbol{z})$ is now given, which states that $\Downarrow_{\phi,C} \boldsymbol{x} = \boldsymbol{z}$.

***Definition 10.3.23** ($\xi_C(\boldsymbol{x},\boldsymbol{z})$)**.** Let $I_0,\dots,I_{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}$ denote the sequence of $\mathbb{E}\wr\mathbb{S}_P$-classes in $\leq_{\text{lex}}$-increasing order. For I an $\mathbb{E}\wr\mathbb{S}_C$-class, let y_I denote:

- y_j for $j \in (I \setminus \beta_{\mathcal{A}})$ if such a j exists
- or $y_j - 1$ for $j \in (I \cap \beta_{\mathcal{A}})$.

Recall that the notation $\exists^\nu$ is introduced in Definition 7.1.3. Let $\xi_C(\boldsymbol{x}^0,\boldsymbol{x}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|})$ be:

$$\begin{aligned}
&\exists^\nu \boldsymbol{y}^0,\dots,\boldsymbol{y}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1},\boldsymbol{x}^1,\dots,\boldsymbol{x}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}.\\
&\quad\bigwedge_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1}\Big\{\Big[\boldsymbol{y}^i \equiv \boldsymbol{x}^i \mod C \wedge \boldsymbol{y} \in \text{Loop-max}_C\Big]\\
&\qquad\wedge \bigvee_{j=0}^{\text{LoopSize}(C,I_i)}\Big[y^i_{I_i} \doteq j \wedge \boldsymbol{x}^{i+1} \doteq \boldsymbol{y}^i + \Big\lfloor \tfrac{j}{l(C,I_i)}\Big\rfloor (t(C,I_i) - l(C,I_i)\langle I_i;\emptyset\rangle)\Big]\Big\}.
\end{aligned}$$

where $\boldsymbol{y} \in \text{Loop-max}_C$ denotes $\bigwedge_{i=0}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|-1} y_{\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i)} < \text{LoopSize}(C,\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(i))$.

Let us now prove that the formula $\xi_C(\boldsymbol{x},\boldsymbol{z})$ indeed defines $\Downarrow_{\phi,C}$.

Lemma 10.3.24. *The formula $\xi_C(\boldsymbol{x}^0,\boldsymbol{x}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|})$ is such that, for all $\boldsymbol{x} \in \mathbb{N}^d$ with $\delta(q_0,\underline{\boldsymbol{x}}_{\mathbb{N}}\mathbf{0}) \in C$, $\Downarrow_{\phi,C} \boldsymbol{x} = \boldsymbol{z}$. The length of $\xi_C(\boldsymbol{x}^0,\boldsymbol{x}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|})$ is $O\big(|C|\log(|C|)d^2\big)$.*

Proof. Let us prove by induction on i that:

1. for all $j \leq i$, there is exactly one possible value $\boldsymbol{x}^i$ such that the formula holds,
2. furthermore, $\boldsymbol{x}^i \sim_{\phi,C} \boldsymbol{x}^0$
3. and for all $k < i$, $x^j_{I_k} < l(C,I_k)$.

The lemma is implied by the inductive hypothesis when $i = d$. For $i = 0$ the induction hypothesis trivially holds. Let us assume that $i > 0$ and that the induction hypothesis holds for $i - 1$.

The second line of the formula states that $\boldsymbol{y}^i$ and $\boldsymbol{x}^i$ are congruent modulo C, hence $\boldsymbol{x}^i \sim_{\phi,C} \boldsymbol{y}^i$, and by induction hypothesis 2, $\boldsymbol{y}^i \sim_{\phi,C} \boldsymbol{x}^0$. By the second line, $\boldsymbol{y}^i \in \text{Loop-max}_C$. Since, $\boldsymbol{y}^i \in \text{Loop-max}_C$, $\boldsymbol{x}^i \sim_{\phi,C} \boldsymbol{y}^i$ and by induction hypothesis 1, there is exactly one possible value $\boldsymbol{y}^i$ such that the formula holds. By induction hypothesis 3 for all $k < i$, $y^j_{I_k} < l(C,I_k)$.

When $\boldsymbol{y}^i$ is the left term of Equation (10.11) of Corollary 10.3.22, then $\boldsymbol{x}^{i+1}$ is the right term of this equation. It implies that $\boldsymbol{x}^{i+1} \sim_{\phi,C} \boldsymbol{y}^i \sim_{\phi,C} \boldsymbol{x}^0$. Furthermore, for all $k \leq i$, $x^{i+1}_{I_k} \leq y^i_{I_k} < l(C,I_k)$. Hence the induction holds for $i + 1$.

Let us now consider the size of the formula. There are $2d$ variables, $\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right| = O(d)$ and $\text{LoopSize}(C,\mathbb{E}\wr\mathbb{S}_{C'}^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(I)) = O(n)$. The length of $\boldsymbol{y}^{i+1} \doteq \boldsymbol{y}^i + \left\lfloor \frac{j}{l(C,E)} \right\rfloor (t(C,E) - l(C,E)\langle E;\emptyset\rangle)$ is

$$\begin{aligned} d\log(\left\lfloor \tfrac{j}{l(C,E)} \right\rfloor (t(C,E) - l(C,E)\langle E;\emptyset\rangle)) &= O(d\log(jt(C,E))) \\ &= O\left(d\log(n^2)\right) = O(d\log(n)), \end{aligned}$$

and the length of $y^i_{I_i} \equiv j \mod \text{LoopSize}(C,\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(I))$ is

$$\log(\text{LoopSize}(C,\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}(I))) = O(\log(n)).$$

Hence the length of the formula is $O\left(n\log(n)d^2\right)$. □

10.4 The algorithm

The algorithm *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$ is finally given in this section. As explained in the chapter's introduction, intuitively, this algorithm outputs a disjunction of formulas χ_P for each accepting state $P \in \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota} \cap F$. The only exception to this construction is the formula $\xi_C(\boldsymbol{x}^0, \boldsymbol{x}^{\left|\mathbb{E}\wr\mathbb{S}_C^{\overline{\mathbb{O}}\,\overline{\mathbb{E}}}\right|})$, which is factorized and appears once in each strongly connected component instead of appearing once for each state P.

The formula χ_P is given in Section 10.4.1. The exact formula $\psi_{\mathcal{A}}$ which defines $\mathcal{A}$ is then given in Section 10.4.2.

10.4.1 Associating a language to a state

In this section, a formula χ_P is created, for each state P, such that χ_C defines the set of tuples of integers which have an expansion $\boldsymbol{w}$ such that $\delta(q_0,\boldsymbol{w}) \in P$.

***Definition 10.4.1** (χ_P)**.** Let $\chi_P(\boldsymbol{x},z)$ be the conjunction of the following formulas, for $i,j \in [d-1]$ such that $(i \in \nu) \Longleftrightarrow (j \in \nu)$:

- $x_i \doteq 0$ if $i \in \mathbb{O}_P$,
- $x_i \not\doteq 0$ if $i \notin \mathbb{O}_P$, $i \notin \mathfrak{O}_P$ and $i \notin \zeta_{\mathcal{A}}$,
- $x_i \doteq x_j$ if $i\ \mathbb{E}_P\ j$,
- $x_i \not\doteq x_j$ if $(i \in \zeta_{\mathcal{A}}) \Longleftrightarrow (j \in \zeta_{\mathcal{A}})$, $(i \in \beta_{\mathcal{A}}) \Longleftrightarrow (j \in \beta_{\mathcal{A}})$, $(i \in \nu) \Longleftrightarrow (j \in \nu)$, hold but neither $i\ \mathbb{E}_P\ j$ nor $i\ \mathfrak{E}_P\ j$ hold,
- $x_i + 1 \doteq x_j$ if $i\ \mathbb{S}_P\ j$,
- $x_i + 1 \not\doteq x_j$ if $(i \in \nu) \Longleftrightarrow (j \in \nu)$, $i \in \beta_{\mathcal{A}}$ and $j \in \zeta_{\mathcal{A}}$ hold but neither $i\ \mathbb{S}_P\ j$ nor $i\ \mathfrak{E}_P\ j$ hold,
- $x_i < x_j$ if $i\ \mathbb{L}_P\ j$, $(i \in \zeta_{\mathcal{A}}) \Longleftrightarrow (j \in \zeta_{\mathcal{A}})$ and $(i \in \beta_{\mathcal{A}}) \Longleftrightarrow (j \in \beta_{\mathcal{A}})$ hold but not $i\ \mathfrak{E}_P\ j$,
- $x_i \leq x_j$ if $i\ \mathbb{L}_P\ j$, $(i \in \zeta_{\mathcal{A}}) \Longleftrightarrow (j \in \zeta_{\mathcal{A}})$, $(i \in \beta_{\mathcal{A}}) \Longleftrightarrow (j \in \beta_{\mathcal{A}})$ and $i\ \mathfrak{E}_P\ j$ hold,
- $x_i + 1 < x_j$ if $i\ \mathbb{L}_P\ j$, $i \in \beta_{\mathcal{A}}$ and $j \in \zeta_{\mathcal{A}}$ hold but not $i\ \mathfrak{E}_P\ j$,
- $x_i + 1 \leq x_j$ if $i\ \mathbb{L}_P\ j$, $i \in \beta_{\mathcal{A}}$ and $j \in \zeta_{\mathcal{A}}$ and $i\ \mathfrak{E}_P\ j$ hold,
- $x_i < x_j + 1$ if $i\ \mathbb{L}_P\ j$, $i \in \zeta_{\mathcal{A}}$ and $j \in \beta_{\mathcal{A}}$ hold but not $i\ \mathfrak{E}_P\ j$,

- $x_i \leq x_j + 1$ if $i \mathbb{L}_P j$, $i \in \zeta_{\mathcal{A}}$ and $j \in \beta_{\mathcal{A}}$ and $i \mathfrak{E}_P j$ hold and
- $z_i \doteq \mathbb{M}^C_{\beta_{\mathcal{A}}}(P,i)$.

Lemma 10.4.2. *For each* $\overset{\mathbb{OESBL}}{\cong}$*-class* C *with* $\mathbb{B}_C = \emptyset$*, for each* $P \in C$*,* $\chi_P(\boldsymbol{x},z)$ *defines* $\overline{\{\boldsymbol{w} \mid \delta(q_0,\boldsymbol{w}) \in P\}}^{\mathbb{N}}$ *when* $z = \Downarrow_{\phi,C} \boldsymbol{x}$*. The length of* $\chi_P(\boldsymbol{x},z)$ *is* $O\left(2^d\right)$*.*

Proof. The fact that $\chi_P(\boldsymbol{x},z)$ indeed defines the set $\overline{\{\boldsymbol{w} \mid \delta(q_0,\boldsymbol{w}) \in P\}}^{\mathbb{N}}$, is straightforward from the definitions.

The formula is a disjunction of $O\left(2^d\right)$ atomic formula of length $O(1)$. Hence its length is $O\left(2^d\right)$. □

10.4.2 The algorithm

The algorithm is now given, it consists mainly in outputting the disjunction of the formula created above.

***Algorithm 10.4.3** (*CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$)**.** The algorithm computes:

- $\mathfrak{F}^{\mathcal{A}}(P)$ using Lemma 9.2.2,
- $\mathbb{O}_P$ and $\mathbb{B}_P$ using Lemma 9.2.9,
- $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_P$ using Lemma 9.2.12,
- $\mathbb{E}\wr\mathbb{S}_P$ using Algorithm 10.2.12,
- $\zeta_{\mathcal{A}}$ and $\beta_{\mathcal{A}}$, using Definition 10.2.2,
- $\mathbb{M}_{\beta_{\mathcal{A}}}(P)$, using Algorithm 10.3.17,
- $\mathfrak{E}_P$, $\mathfrak{D}_P$, using Algorithm 10.2.12,
- the set of strongly connected component, using Lemma 10.2.4,
- $l(C,E)$, $t(C,E)$ using Lemma 10.3.20.

The algorithm then returns:

$$\bigvee_C \exists \boldsymbol{z}.\xi_C(\boldsymbol{x}^0,\boldsymbol{x}^{\left|\mathbb{E}\wr\mathbb{S}^{\bar{\mathbb{O}}\ \bar{\mathbb{E}}}_C\right|}) \wedge \bigvee_{P \in C \cap F \cap \mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}'_\iota}} \chi_P(\boldsymbol{x}).$$

Proposition 10.4.4. Let $\mathcal{A}$ be a minimal initially-cyclic automaton over natural numbers which accepts a $\Sigma_0[\mathcal{V}]/\nu$-definable set. The algorithm *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$ on $\mathcal{A}$ returns a $\Sigma_1\left[\mathcal{V}'_\iota(m)\right]/\nu$-formula which defines $\overline{\mathcal{A}}^{\mathbb{N}}$ in time $O\left(n\left(\log(n)d^2 + 2^d\right)\right)$.

Proof. Let $\psi_{\mathcal{A}}$ be the formula returned by *CEF'*$(\mathcal{V}_\iota^{\mathbb{N}})$. Let us prove that $\overline{\psi_{\mathcal{A}}}^{\mathbb{N}} = \overline{\mathcal{A}}^{\mathbb{N}}$.

Having $\boldsymbol{x} \in \overline{\psi_{\mathcal{A}}}^{\mathbb{N}}$ is equivalent to the existence of some state $P \in F$ such that $\chi_P(\boldsymbol{x})$ holds, and, as proven in Lemma 10.4.2, it is equivalent to the fact that there is an expansion $\boldsymbol{w}$ of $\boldsymbol{x}$ such that $\delta(q_0,\boldsymbol{w}) = P$. It is then equivalent to $\boldsymbol{x} \in \overline{\mathcal{A}}^{\mathbb{N}}$.

There are $O(n)$ strongly connected components C and $O(n)$ states P. The formula $\chi_P(\boldsymbol{x})$ is computed in time $O\left(2^d\right)$ and the formula $\xi_C(\boldsymbol{x}^0, \boldsymbol{x}^{\left|\mathbb{E} \wr \mathbb{S}_C^{\overline{\mathbb{O}}\ \overline{\mathbb{E}}}\right|})$ is computed in time $O\left(|C| \log(|C|) d^2\right)$, hence the length of the formula is

$$O\left(\left(\sum_C |C| \log(|C|) d^2\right) + n2^d\right) = O\left(n\left(\log(n) d^2 + 2^d\right)\right).$$

Finally, the computation time is the sum of the computation times of the algorithm cited above, that is:

$$\begin{aligned} O\left(n2^d d + n2^d d + nd^2 2^d + n\log(n)2^d d + n2^d d^2 + nd^2 + nd^2 + n2^d d^3 + n\left(\log(n) d^2 + 2^d\right)\right) \\ = O\left(n2^d d\left(\log(n) + d^2\right)\right). \end{aligned}$$

□

Chapter 11

Conclusion

Two algorithms are given in this part. The first algorithm decides whether an automaton accepts a set definable in one of the three logics $\mathsf{FO}[<,-,\mathrm{mod}]$, $\mathsf{FO}[<,\mathrm{mod}]$ or $\mathsf{FO}[+1,\mathrm{mod}]$. This algorithm runs in time:

$$O\Big(2^d n b^d (\log(n) + 3^d d)\Big),$$

and if the automaton is minimal and over non-negative integers, it runs in time

$$O\Big(n b^d 3^d d\Big).$$

The second algorithm takes as input an automaton which accepts a set definable in one of the three above-mentioned logic and returns an existential formula which defines this set. This algorithm runs in time

$$O\Big(2^d n^3 \log(b)\Big(\log(n) d^2 + 2^d\Big)\Big)$$

and, if the automaton is over non-negative integers, it runs in time

$$O\Big(n^3 \log(b)\Big(\log(n) d^2 + 2^d\Big)\Big).$$

11.0.3 Considering other vocabularies

It should be noted that our result would also stand for the two following logics $\Sigma_0[\doteq,<,+\mathbb{N},\mathrm{mod}]$ and $\Sigma_0[\doteq,+\mathbb{N},\mathrm{mod}]$ over non-negative integers. That is, quantifier-free logic with the addition of constant but without the equality with constant. The proof of Theorem 9.4.8 is not fundamentally more complex, but it would be longer.

The only remaining utility of $\mathbb{O}$ is to create successor relations, which implies that, as soon as there is no $\mathbb{B}$ in a $(\nu,\mathcal{V}_\iota')^m$-pop, there is no reason to keep any $\mathbb{O}$. Hence the following axiom should be added to Section 7.3.1.2. (22 - $\mathbb{O}$ and $\underline{\mathbb{B}}$)

Axiom 22 ($\mathbb{O}$ and $\underline{\mathbb{B}}$)**.** *If $\doteq\mathbb{Z}$ does not belong to $\mathcal{V}_\iota'$ and $i \in \mathbb{O}_T$, there exists $j \in [d-1]$ such that $(i \in \nu) \Longleftrightarrow (j \in \nu)$ and $j \in \mathbb{B}_T$.*

Proof. This is a consequence of the new rule. □

Then, the definition of $\textsc{position}_{\mathcal{V}_\iota'(m)}[\boldsymbol{w}]$ should be adapted with the rule $i \in \mathbb{O}_w$ if and only if $\{w_i \in 0^*$ and [either $\doteq\mathbb{Z}$ belongs to $\mathcal{V}_\iota'$, or $(+1$ belongs to $\mathcal{V}_\iota'$ and there exists $j \in [d-1]$ such that

$(i \in \nu) \Longleftrightarrow (j \in \nu)$ and $w_j \in (b-1)^*)]\}$. Similarly, $i \in \mathbb{O}_{P \cdot O}$ holds if and $[i \in \mathbb{O}_P$, $i \in \mathbb{O}_O$ and ($\doteq\mathbb{Z}$ belongs to $\mathcal{V}_\iota'$ or there exists $j \in [d-1]$ such that $(i \in \nu) \Longleftrightarrow (j \in \nu)$, $j \in \mathbb{B}_P$ and $j \in \mathbb{B}_O$.)]

In Chapter 8 some $(\nu, \mathcal{V}_\iota')^m$-pops are explicitly constructed. Their construction should be changed in order to satisfy Axiom . That is, for each $(\nu, \mathcal{V}_\iota')^m$-pop O, to the condition of $i \in \mathbb{O}_O$, it should be added "either $\doteq\mathbb{Z}$ belongs to $\mathcal{V}_\iota'$ or there exists $j \in [d-1]$ such that $(i \in \nu) \Longleftrightarrow (j \in \nu)$ and that $j \in \mathbb{B}_O$."

Finally, a condition similar to Condition 4 of Definition 9.2.13 should be added, which states that, if $\mathbb{B}_q = \emptyset$ then $\mathbb{O}_q = \emptyset$.

Similarly, our result stand for the logics $\mathsf{FO}[\doteq\mathbb{N}, \mathrm{mod}]$ and $\mathsf{FO}[\mathrm{mod}]$. In this case, it suffices to assume that $\textsc{relation}_{\nu, \mathcal{V}_\iota'(m)}[\boldsymbol{w}](i,j) = \emptyset$ for all $i, j \in [d-1]$ and $\boldsymbol{w} \in \left(A_b^d\right)^*$ and, more generally, to ignore the symbols $\mathbb{E}$, $\mathbb{S}$, and $\mathbb{B}$ (and $\mathbb{O}$ in the case of the logic $\mathsf{FO}[\mathrm{mod}]$). The algorithm then assert that, for all cyclic states q, $\mathbb{E} \wr \mathbb{S}_q = \mathbb{B}_q = \emptyset$, (and $\mathbb{O}_q = \emptyset$ in the case of the logic $\mathsf{FO}[\mathrm{mod}]$).

11.0.4 The algorithm

As stated in the introduction, we now give the list of Definitions, Lemmas used in the algorithm $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$ and $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$, and the list of sub-algorithms.

- Definition 7.1.1: $\overline{f}_\nu$
- Definition 7.1.2: Polarity
- Definition 7.1.3: $\exists^\nu$
- Lemma 7.1.6: From $\mathbb{N}$ to $\mathbb{Z}$
- Definition 7.1.8: $\underline{f}$ and $\underline{f}_\nu$
- Lemma 7.1.11: Automaton over $\mathbb{Z}$ to automata over $\mathbb{N}$
- Algorithm 7.1.13: $EQF(\mathcal{V}_\iota^{\mathbb{Z}})$
- Algorithm 7.1.15: $CEF(\mathcal{V}_\iota^{\mathbb{Z}})$
- Definition 7.2.1: Left quotient of formulas
- Algorithm 7.2.11: Tarjan's algorithm, [Tar72]
- Lemma 7.2.12: ϕ^n
- Algorithm 7.2.13: $CEF(\mathcal{V}_\iota^{\mathbb{N}})$
- Definition 7.2.20: $\mathbb{C}_b$, $\mathcal{V}_\iota'$, $\mathcal{V}_\iota'(m)$
- Definition 7.3.1: $I^1_{\mathcal{V}_\iota'}$, $I^2_{\mathcal{V}_\iota'}$
- Definition 7.3.2: $\textsc{top}^m_{\nu, \mathcal{V}_\iota'}$
- Definition 7.3.3: $\mathbb{QUAD}^m_{\nu, \mathcal{V}_\iota'}$
- Definition 7.3.4: $\mathbb{TOP}_{\nu, \mathcal{V}_\iota'}$, $\mathbb{TOP}^m_{\nu, \mathcal{V}_\iota'}$
- Lemma 7.3.10: From $(\zeta, \beta, \nu, \mathcal{V}_\iota')^m$-top to words
- Definition 7.3.11: $\mathbb{QUAD}^m_{\nu, \mathcal{V}_\iota'}$'s product
- Definition 8.1.5: $\mathbb{M}_\beta(P)$
- Definition 8.1.6: $P \overset{x}{\cong} Q$, $P \overset{x}{\preccurlyeq} Q$, $P \overset{x}{\prec} Q$
- Definition 8.1.7: $P \overset{X}{\cong} Q$, $P \overset{X}{\preccurlyeq} Q$, $P \overset{X}{\prec} Q$
- Definition 8.1.9: $\sqsubseteq$, $\sqsubset$
- Definition 9.1.2: $\langle I; J \rangle$
- Definition 9.1.5: $\langle \emptyset; J \rangle^{-1}$
- Definition 9.1.6: Upper set, Lower set
- Lemma 9.1.8: Computing $< \emptyset; J >$
- Definition 9.1.9: $\mathbb{A}_{\mathcal{V}_\iota', 1}$
- Lemma 9.1.11: Deciding $\mathbb{A}_{\mathcal{V}_\iota', 1}$
- Definition 9.1.13: $[I; J]$
- Definition 9.2.1: $\mathfrak{F}^{\mathcal{A}}(q)$
- Lemma 9.2.2: Computing $\mathfrak{F}^{\mathcal{A}}(q)$
- Definition 9.2.4: $\mathbb{A}_{\mathcal{V}_\iota', 2}$
- Lemma 9.2.6: Deciding $\mathbb{A}_{\mathcal{V}_\iota', 2}$
- Definition 9.2.8: $\mathbb{B}_q$, $\mathbb{O}_q$
- Lemma 9.2.9: Computing $\mathbb{O}_q$ and $\mathbb{B}_q$

- Definition 9.2.10: $i\ \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q\ j$, $i\ \mathbb{E}\wr\mathbb{S}_q\ j$, $i\ \mathbb{L}\overline{\mathbb{S}}_q\ j$
- Lemma 9.2.12: Computing $\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q$
- Definition 9.2.13: $\mathbb{A}_{\mathcal{V}'_\iota,3}$
- Definition 9.2.14: $\text{TOP}_{\mathcal{V},\mathcal{V}'_\iota}q$
- Lemma 9.2.16: Deciding $\mathbb{A}_{\mathcal{V}'_\iota,3}$
- Definition 9.2.17: $\mathbb{A}_{\mathcal{V}'_\iota,4}$
- Lemma 9.2.20: Computing LoopSize(q,I)
- Lemma 9.2.21: Deciding $\mathbb{A}_{\mathcal{V}'_\iota,4}$
- Definition 9.3.1: $\boldsymbol{w}-S$
- Definition 9.3.3: $\mathfrak{S}_{\mathcal{A}}(q,\boldsymbol{a})$
- Definition 9.3.4: $\mathbb{A}_{\mathcal{V}'_\iota,5}$
- Lemma 9.3.7: Deciding $\mathbb{A}_{\mathcal{V}'_\iota,5}$
- Definition 9.3.14: $\mathbb{A}_{\mathcal{V}'_\iota,6}$
- Lemma 9.3.16: Deciding $\mathbb{A}_{\mathcal{V}'_\iota,6}$
- Definition 9.4.1: $\mathbb{A}_{\mathcal{V}'_\iota}$
- Algorithm 9.4.6: $EQF(\mathcal{V}_\iota^{\mathbb{N}})$
- Definition 10.2.2: $\zeta_{\mathcal{A}}$, $\beta_{\mathcal{A}}$
- Definition 10.2.3: $i\ \mathbb{E}_P\ j$, $i\ \mathbb{S}_P\ j$, $i\ \mathbb{L}_P\ j$
- Lemma 10.2.4: Strongly connected component
- Definition 10.2.6: $\mathbb{O}_C$, $\mathbb{E}_C$, $\mathbb{S}_C$, $\mathbb{B}_C$
- Algorithm 10.2.12: $\mathfrak{E}$
- Algorithm 10.2.14: $\mathfrak{O}$
- Definition 10.3.1: $\beta_{\mathcal{A},C}$
- Definition 10.3.2: $\mathbb{M}^C_{\beta_{\mathcal{A}}}(P)$
- Definition 10.3.5: LoopSize(C,E)
- Algorithm 10.3.17: Modular part of states
- Definition 10.3.19: $l(C,E)$, $t(C,E)$
- Lemma 10.3.20: $l(C,E)$, $t(C,E)$
- Definition 10.3.23: $\xi_C(\boldsymbol{x},\boldsymbol{z})$
- Definition 10.4.1: χ_P
- Algorithm 10.4.3: $CEF'(\mathcal{V}_\iota^{\mathbb{N}})$

11.1 Open questions

Some natural questions remain.

11.1.1 Deciding other classes of set

One can ask whether there exists a polynomial time algorithm which decides whether an automaton accepts a set definable in a fragment of FO[<, mod] such as FO[+1] or $\Sigma_0[<]$.

A technique would be to rewrite the automaton as a base 1 automaton, and testing whether it is aperiodic. It can not work as the transformation from base b to base 1 may be exponential. Indeed $\mathcal{A}_i^1$ and $\mathcal{A}_i^b$ be the minimal automaton, in base 1 and b respectively, which accept the set $R_i = \left\{x \in \mathbb{N} \mid x \equiv 0 \mod b^i\right\}$, then $\mathcal{A}_i^1$ has b^i states, while $\mathcal{A}_i^b$ has $i+1$ states.

For c coprime with b, our sections "from logic to automaton" proves that the minimal base-c automaton C_i which accepts R_i also contains at least b^i states; so there can not exist a polynomial time translation from a base to another one.

11.1.2 Writing a polynomial-size $\Sigma_0[\mathbb{N}, <, +\mathbb{N}, \mathrm{mod}\,\mathbb{N}]/\nu$-formula

It is now intended to give an argument to show that there may not exists polynomial size $\Sigma_0[<, = \mathbb{N}, +\mathbb{N}, \mathrm{mod}]/\nu$-formula, for $d = 1, b = 2$. Let

$$R_i = \left\{ n \in \mathbb{N} \mid n < 4^i, \forall 0 \leq j \leq i. \left\lfloor \frac{n}{2^{2j}} \right\rfloor \equiv 0 \mod b \right\},$$

that is the set of the 2^i integers which are described by the regular expression $\mathbf{(0(0+1))^i}$ in base 2.

The set R_i can clearly be written in $\Sigma_0[<, = \mathbb{N}, +\mathbb{N}, \mathrm{mod}\,\mathbb{N}]/\nu$ as a disjunction of 2^i equalities, taking size $O(i2^i)$. On the one hand, it seems to be hard to create a quantifier-free shorter formula. On the other hand, to our knowledge, there is no method to compute the size of the shortest formula that exists for a given set.

11.1.3 Sequential automaton

Our automaton alphabet is A_b^d, but in [Ler06], the alphabet is $[b-1]$, hence the size of his alphabet is b and not b^d, and b^d is not considered to be polynomial in the size of the input anymore. Let us call his automaton a sequential one, and our automaton a synchronous one.

Then let $\mathcal{A} = (Q, A, \delta, q_0, F)$ be an synchronous automaton. One can transform a synchronous automaton with n states into a sequential one with nb^{d-1} states.

$$A' = (Q \times \{w \in [b-1]^* \mid |w| < d\}, [d-1], \delta', q_0, F \times (0, \varepsilon))$$

with $\delta'((q,w),a)$ being, if $|w| < d-1$, (q, wa) otherwise $(\delta(q,wa), 0, \varepsilon)$. And reciprocally a sequential automaton can be seen as a synchronous one, reading d letters in one step.

It is still unknown whether there is a polynomial time algorithm for sequential automaton. In particular, it is still unknown whether our algorithm can be modified to satisfy this formalism.

11.1.4 Automaton over reals

In this part, only automata over integers were considered. Similarly, Büchi automata over the alphabet A_b^d accepts relations over non-negative real numbers. Results similar to [BHMV94] are given in [BBB10]. It is actually possible to adapt methods developed in this part in order to prove similar results over relation over real numbers.

Index of Part II

$\downarrow_{\preccurlyeq} x$, 200
$\Downarrow_{\phi}$, 193
$\Downarrow_{\phi,C} \boldsymbol{x}$, 260
$(f)_{\boldsymbol{w}}$, 217
$\uparrow_{\preccurlyeq} x$, 200
$\boldsymbol{w} - S$, 212
$P^{-1}\phi$ for $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 163
$T^{-1}\phi$, 152
$\boldsymbol{w}^{-1}\phi$, 120
$P \overset{X}{\sqsubseteq} Q$, 159
$P \overset{X}{\prec} Q$, 159
$\sqsubseteq$, 159
$P \overset{X}{\sqsubset} Q$, 159
$P \overset{X}{\preccurlyeq} Q$, 159
$P \overset{X}{\cong} Q$, 159
$P \sim_{\phi} T$, 162
$\mathbb{A}_{\mathcal{V}_\iota'}$, 246

$\mathcal{A}'_{\phi,\nu}$ for $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\nu$, 134
$\mathcal{A}'_{\phi,\zeta,\beta,\nu}$ for $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$, 153
$\mathbb{A}_{\mathcal{V}_\iota',2}$, 205
$\mathbb{A}_{\mathcal{V}_\iota',6}$, 220
$\mathbb{A}_{\mathcal{V}_\iota',1}$, 202
$\mathbb{A}_{\mathcal{V}_\iota'}$, 246
$\mathbb{A}_{\mathcal{V}_\iota',4}$, 210
$\mathbb{A}_{\mathcal{V}_\iota',3}$, 208
$\mathbb{A}_{\mathcal{V}_\iota',5}$, 213

$\mathbb{B}$, 136
$\beta_{\mathcal{A}}$, 251
$\mathbb{B}_T$, 137
$\mathbb{B}_C$, 252
$\beta_{\mathcal{A},C}$, 255
$\mathbb{B}_q$, 206
$\beta_{\boldsymbol{w}}$, 131

$\mathbb{C}_b$, 129
$C_b(m)$, 129
$c_b(m)$, 129
$CEF(\mathcal{V}_\iota^{\mathbb{N}})$, 126
$CEF(\mathcal{V}_\iota^{\mathbb{Z}})$, 118

$\mathfrak{E}$, 253

$\mathbb{E}_q^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)$, 138
$i \mathbb{E}_P j$, 251

$\mathbb{E}$, 136
$\left|\mathbb{E}_q\right|$, 138
$\mathbb{E}_T^{\mathbb{B}}$-classes, 138
$\mathbb{E}_T^{\mathbb{O}}$-classes, 138
$\left|\mathbb{E}_q^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|$, 138
$EQF(\mathcal{V}_\iota^{\mathbb{N}})$, 247
$EQF(\mathcal{V}_\iota^{\mathbb{Z}})$, 117
$\mathbb{E}\wr\mathbb{S}_C$, 207
$\mathbb{E}\wr\mathbb{S}_q^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}(i)$, 138
$i \mathbb{E}\wr\mathbb{S}_q j$, 207
$\left|\mathbb{E}\wr\mathbb{S}_q^{\overline{\mathbb{O}}\,\overline{\mathbb{B}}}\right|$, 138
$\mathbb{E}\wr\mathbb{S}_T^{\mathbb{B}}$-classes, 138
$\mathbb{E}\wr\mathbb{S}_T^{\mathbb{O}}$-classes, 138

$\overline{f}_{\nu}$, 110
$\underline{f}_{\nu}$, 114
$\overline{f}$, 114
$\overline{\mathfrak{F}}^{\mathcal{A}}(q)$, 205

$\mathbb{G}$, 136
LoopSize(C,E), 256

$I^2_{\mathcal{V}_\iota'}$, 135
$[I;J]$ for $I,J \subseteq [d-1]$ disjoint., 203
$\langle\emptyset;J\rangle^{-1}$ for $J \subseteq [d-1]$., 199
$\langle I;J\rangle, \langle\emptyset;J\rangle$ for $I,J \subseteq [d-1]$ disjoint., 198

$i \mathbb{L}_P j$, 251
$\mathbb{L}$, 136
$\mathbb{L}\wr\mathbb{E}\wr\mathbb{S}$, 138
$I \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_T J$, 138
$i \mathbb{L}\wr\mathbb{E}\wr\mathbb{S}_q j$, 207
left-quotient by a $(\nu,\mathcal{V}_\iota')^m$-top, 152
$\textsc{length}_{m,b}$, 136
LoopSize(q,I), 210
Loop-max$_C$, 257
Lower set, 200
$\mathbb{L}\overline{\mathbb{S}}$, 138
$I \mathbb{L}\overline{\mathbb{S}}_T J$, 138
$i \mathbb{L}\overline{\mathbb{S}}_q j$, 207

$\mathbb{M}_{\beta}(P)$, 158
$\mathbb{M}^C_{\beta,\mathcal{A}}(P)$, 255
mod(n,m), 252
mod$^{>0}$, 244
$\equiv \boldsymbol{y} \mod C$, 257

MODULO$_m$, 136

negative variable, 110

$\mathbb{O}$, 136
$\circ_\phi$, 193
$\underline{\mathbb{O}}_T$, 137
$\overline{\mathbb{O}}\,\overline{\mathbb{B}}_T$, 137
$\mathbb{O}_C$, 252
$\mathbb{O}_q$, 206
$\mathbb{O}_{q\setminus w}$, 217

$\mathbb{P}$, 136
$\underline{P}_{\mathcal{V}_\iota'(m)}$ for $P \in \mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 162
$\mathbb{PAIR}_{\nu,\mathcal{V}_\iota'}$, 136
$\mathbb{PAIR}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 146
$(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-pop, partially ordered partition, 157
$\mathbb{P}^d$, 198
$\overline{\phi}^{\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}}$, 193
$\overline{\phi}^{\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}}$, 151
$\overline{\phi}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$, 151
$\phi(P)$ for $P \in \mathbb{POP}^{m,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$ and $\phi \in \Sigma_0[\mathcal{V}_\iota']/\zeta,\beta,\nu$, 163
$\phi(T)$ for $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$ and $\phi \in \Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$, 151
ϕ^n, 125
$\phi_T(\boldsymbol{x})$, 150
$\phi^{\mathcal{A}}_{0,\mathbb{Z}}$, 116
polarity, 110
$\mathbb{POP}^m_{\nu,\mathcal{V}_\iota'}$, 157
$\mathbb{POP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 157
$\mathbb{POP}^{m,0,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 251
$\mathbb{POP}^{m,0,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 251
$\mathbb{POP}^{m,0}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 251
$\mathbb{POP}^{m,\min,\phi}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 193
POSITION$_{\mathcal{V}_\iota'(m)}$, 136
positive variable, 110
$\chi_P(\boldsymbol{x},\boldsymbol{z})$, 265

$\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$, 136
$\mathbb{QUAD}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 146

RELATION$_{\nu,\mathcal{V}_\iota'(m)}$, 136
Rigid, 141
R_ν for $R \subseteq \mathbb{Z}^d$, 110

$\mathbb{S}$, 136
$i\ \mathbb{S}_P\ j$, 251
$\Sigma_0\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, 110
$\Sigma_p\left[\mathcal{V}_\iota^{\mathbb{N}}\right]/\nu$, 110
$X(e,a,m)$, 127
$\Sigma_0[\mathcal{V}_\iota'(m)]/\zeta,\beta,\nu$, 130
$\mathfrak{S}_{\mathcal{A}}(q,\boldsymbol{a})$, 213

$\overline{T}^{\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}}$ for $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 149
$\underline{T}_{\mathcal{V}_\iota'(m),\zeta,\beta}\,\underline{T}_{\mathcal{V}_\iota'(m)}$ for $T \in \mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 149
$\underline{T}_{\mathcal{V}_\iota'(m)}$ for $T \in \mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$, 137
$i\mathbb{E}_T\,j$, 137
$i\mathbb{L}_T\,j$, 137
$\mathbb{TOP}^m_{\nu,\mathcal{V}_\iota'}$, 137
$\mathbb{TOP}_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 146
TOP$^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 148
$\mathbb{QUAD}^m_{\nu,\mathcal{V}_\iota'}$'s product, 143
TOP$^m_{\nu,\mathcal{V}_\iota'}$, 136
$(\zeta,\beta,\nu,\mathcal{V}_\iota')$-top, 147
$\mathbb{TOP}^m_{\zeta,\beta,\nu,\mathcal{V}_\iota'}$, 146
$(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top, 147
$(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top, 146
$(\zeta,\beta,\nu,\mathcal{V}_\iota')^m$-top, 137
Totally Ordered Partition, 144
$T_{\zeta,\beta,\nu}$, 148

Upper set, 200

$\mathcal{V}_\iota'$, 129
$\mathcal{V}_\iota'(m)$, 129

$\xi_C(\boldsymbol{x},\boldsymbol{z})$, 264

$\mathfrak{O}$, 253
$\zeta_{\mathcal{A}}$, 251
$\zeta_{\boldsymbol{w}}$, 131

Bibliography

[BBB10] Bernard Boigelot, Julien Brusten, and Véronique Bruyère. On the sets of real numbers recognized by finite automata in multiple bases. *Logical Methods in Computer Science*, 6(1), 2010.

[BC96] Alexandre Boudet and Hubert Comon. Diophantine equations, presburger arithmetic and finite automata. In *Proceedings of the 21st International Colloquium on Trees in Algebra and Programming*, CAAP '96, pages 30–43, London, UK, UK, 1996. Springer-Verlag.

[BHMV94] Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Logic and p-recognizable sets of integers. *Bull. Belg. Math. Soc*, 1:191–238, 1994.

[Bü60] J. Richard. Büchi. Weak second-order arithmetic and finite automata. *Zeitschrift für Mathematische Logik und Grudlagen der Mathematik*, 6:66–92, 1960.

[Cho08] Christian Choffrut. Deciding whether a relation defined in Presburger logic can be defined in weaker logics. *RAIRO ITA*, 42(1):121–135, 2008.

[Cob69] Alan Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Mathematical systems theory*, 3(2):186–192, 1969.

[Coo72] D. C. Cooper. Theorem proving in arithmetic without multiplication. *Machine Intelligence 7*, pages 91–99, 1972.

[CSRL01] Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson. *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd edition, 2001.

[DFL98] Arnaud Durand, Ronald Fagin, and Bernd Loescher. Spectra with only unary function symbols. In Mogens Nielsen and Wolfgang Thomas, editors, *Computer Science Logic*, volume 1414 of *Lecture Notes in Computer Science*, pages 189–202. Springer Berlin Heidelberg, 1998.

[Ehr59] Andrzej Ehrenfeucht. Decidability of the theory of the linear ordering relation. *Notices Amer. Math. Soc.*, 6(3):268:556–38, 1959.

[ER66] Calvin C. Elgot and Michael O. Rabin. Decidability and undecidability of extensions of second (first) order theory of (generalized) successor. *J. Symb. Log.*, 31(2):169–181, 1966.

[FL08] Alain Finkel and Jérôme Leroux. Presburger functions are piecewise linear. Research Report LSV-08-08, Laboratoire Spécification et Vérification, ENS Cachan, France, March 2008. 9 pages.

[Fra67] Roland Fraïssé. *Cours de Logique Mathématique*. Gauthier-Villars Nauwelaerts, 1967.

[GS03] Yuri Gurevich and Saharon Shelah. Spectra of monadic second-order formulas with one unary function. In *18th IEEE Symposium on Logic in Computer Science (LICS 2003), 22-25 June 2003, Ottawa, Canada, Proceedings*, pages 291–300, 2003.

[Hon86] Juha Honkala. A decision method for the recognizability of sets defined by number systems. *ITA*, 20(4):395–403, 1986.

[Knu76] Donald Ervin Knuth. *Mathematics and Computer Science: Coping with Finiteness*. STAN-CS-. Department of Computer Science, Stanford University, 1976.

[Lan04] Klaus-Jörn Lange. Some results on majority quantifiers over words. In *IEEE Conference on Computational Complexity*, pages 123–129. IEEE Computer Society, 2004.

[Lat05] Louis Latour. *Presburger Arithmetic: From Automata to Formulas*. PhD thesis, Université de liège, 2005.

[Lee90] Jan V. Leeuwen. *Handbook of Theoretical Computer Science: Algorithms and Complexity*. MIT Press, Cambridge, MA, USA, 1990.

[Ler06] Jérôme Leroux. Least significant digit first Presburger automata. *CoRR*, abs/cs/0612037, 2006.

[Min60] Marvin L. Minsky. *Recursive Unsolvability of Post's Problem of "tag": And Other Topics in Theory of Turing Machines*. Group report. Massachusetts Institute of Technology, Lincoln Laboratory, 1960.

[Moo56] Edward F. Moore. Gedanken-experiments on sequential machines. In Claude Shannon and John McCarthy, editors, *Automata Studies*, pages 129–153. Princeton University Press, Princeton, NJ, 1956.

[MS13] Victor Marsault and Jacques Sakarovitch. Ultimate periodicity of b-recognisable sets: A quasilinear procedure. In Marie-Pierre Béal and Olivier Carton, editors, *Developments in Language Theory*, volume 7907 of *Lecture Notes in Computer Science*, pages 362–373. Springer, 2013.

[Muc03] Andrei A. Muchnik. The definable criterion for definability in Presburger arithmetic and its applications. *Theor. Comput. Sci.*, 290(3):1433–1444, 2003.

[MV96] Christian Michaux and Roger Villemaire. Presburger arithmetic and recognizability of sets of natural numbers by automata: New proofs of cobham's and semenov's theorems. *Ann. Pure Appl. Logic*, 77(3):251–277, 1996.

[Pél92] Pierre Péladeau. Formulas, regular languages and boolean circuits. *Theor. Comput. Sci.*, 101(1):133–141, 1992.

[Pre27] Mojżesz Presburger. Über die vollständigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchen, die addition als einzige operation hervortritt. In *Comptes Rendus du Premier Congrès des Mathématicienes des Pays Slaves*, pages 92–101, 395, Warsaw, 1927.

[Sch65] M.P. Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8(2):190 – 194, 1965.

[Sem77] A. L. Semenov. The presburger nature of predicates that are regular in two number systems. *Siberian Math. J.*, 18:289,299, 1977.

[Sip96] Michael Sipser. *Introduction to the Theory of Computation*. International Thomson Publishing, 1st edition, 1996.

[Smo91] Craig A. Smoryński. *Logical number theory. 1. , an introduction*. Universitext. Springer-Verlag, Berlin, New York, 1991.

[Str91] Howard Straubing. Constant-depth periodic circuits. *International J. Algebra and Computation*, 1:49–88, 1991.

[Str94] Howard Straubing. *Finite Automata, Formal Logic, and Circuit Complexity*. Birkhäuser, 1994.

[Tar72] Robert Tarjan. Depth-first search and linear graph algorithms. *SIAM Journal on Computing*, 1(2):146–160, 1972.

[Tho75] Wolfgang Thomas. A note on undecidable extensions of monadic second order successor arithmetic. *Archiv für mathematische Logik und Grundlagenforschung*, 17:43–44, 1975.

[WB00] Pierre Wolper and Bernard Boigelot. On the construction of automata from linear arithmetic constraints. In Susanne Graf and Michael Schwartzbach, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 1785 of *Lecture Notes in Computer Science*, pages 1–19. Springer Berlin Heidelberg, 2000.

Manuscript's notation index

$+R$, 24
$\mathcal{N}$, 24
$\mathcal{Z}$, 24
$\lfloor \cdot \rfloor$ - Floor function, 24
$\Longleftrightarrow$, 26
$\Longrightarrow$, 26
$\langle \bigvee_{i \in F} \exists \boldsymbol{x}.\phi_i(\boldsymbol{x}) \mid \chi_i(\boldsymbol{x}) \mid \psi \rangle$, 27
$\wedge$, 24
$\vee$, 24
$\mathcal{S} \models \phi$, 25
$\neg$, 24
$\phi(\boldsymbol{x})^S$, 26
$\phi(\boldsymbol{x};\boldsymbol{y})$ - function notation, 26
$R-$, 24
$\doteq R$ - equality with a constant from a set R , 23
$\doteq$, 23
$\doteq c$ - equality with the constant c, 23

$\mathcal{A} = \left(Q, A_b^d, \delta, q_0, F\right)$, 36

$c >$ - the predicate of integers less than c, 24

$\mathrm{diag}(R; x_i = x_j + c)$, 32

$\exists$, 25

$\min_{\boldsymbol{x}}\{\phi(\boldsymbol{x})\}$, 26
$\min_{i \in F}\{\phi_i\}$, 26
$\min_{i \in F, \boldsymbol{x}}\{\phi_i(\boldsymbol{x})\}$, 26
$\mathrm{mod}\, R$ - the set of predicates $\mathrm{mod}\, m$ for $m \in R$, 24

$\mathbb{N}_\sigma^d$, 33

$\mathbb{S}_d$, 33
$\mathrm{mod}_m(R)$, 42

$\mathcal{S}$ a structure, 24
$\mathrm{sec}(R; x_i = c)$, 32
$\mathcal{S}_{|n}$, 24
$\mathrm{sub}(\chi(\boldsymbol{x}), \boldsymbol{t}, \boldsymbol{c})$, 32

$\mathrm{thres}_m(R)$ for R a set of integers, 41

$\times R$ - Multiplication by a constant of R, 24

Résumé

Ce manuscrit traite de la logique du premier ordre avec la relation d'ordre et les prédicats modulaires, notée $\mathsf{FO}[<,\mathrm{mod}]$. La classe des ensembles réguliers, c'est à dire des ensembles $\mathsf{FO}[<,\mathrm{mod}]$-définissables, est la classe des ensembles acceptés par un automate en base 1. C'est aussi la plus grande classe C d'ensembles telle que $\mathsf{FO}[C]$ ne définisse que des langages réguliers. Il est donc naturel de s'intéresser à cette logique et nous donnons dans ce manuscrit de nouvelles caractérisations des ensembles réguliers. Nous montrons que les ensembles réguliers ont une caractérisation en terme d'ensembles de dimension inférieure et en terme de périodicité. Nous montrons que si un ensemble R est définissable dans l'arithmétique de Presburger, alors il est régulier si et seulement si toutes les fonctions unaires $\mathsf{FO}[<,R]$-définissable sont réguliers. Cette caractérisation nous sert à montrer que le fragment maximal C de l'arithmétique de Presburger tel que la satisfiabilité de $\mathsf{FO}[<,C]$ soit décidable est la classe des ensembles réguliers. Similairement, la satisfiabilité de la logique du premier ordre sur les mots avec la fonction successeur et une fonction unaire f croissante est indécidable dès que $f(n)-n$ est non borné. Si f est non interprété, la logique du premier ordre avec la fonction successeur et f est indécidable sur les entiers. Enfin, on donne un algorithme en temps linéaire prenant en entrée un automate A en base b supérieur à 1 et acceptant si et seulement si A accepte un ensemble régulier. Un deuxième algorithme, en temps quasi-cubique, retourne alors une $\mathsf{FO}[<,\mathrm{mod}]$-formule qui définit l'ensemble d'entiers accepté par l'automate.

Abstract

This manuscript deals with first order logic with order relation and modular predicate, denoted by $\mathsf{FO}[<,\mathrm{mod}]$. The class of regular set, that is of of $\mathsf{FO}[<,\mathrm{mod}]$-definable sets, is the class of sets accepted by a base 1 automaton. It is also the greatest class C of set such that $\mathsf{FO}[C]$ only defines regular languages. It is therefore natural to consider this logic, and we give in this manuscript some new characterization of regular sets. We show that the class of regular sets admits a characterization in terms of set of smaller dimension and in term of periodicity. We show that a set, definable in Presburger arithmetic, is regular if and only if all unary function which are $\mathsf{FO}[<,R]$-definable are regulars. This characterization allows to prove that the maximal fragment C of Presburger arithmetic such that the satisfiability of $\mathsf{FO}[<,C]$ is decidable is the class of regular sets. Similarly, the satisfiability of first-order logic over words with the successor function and an unary increasing function f is undecidable as soon as $f(n)-n$ is unbounded. If f is uninterpreted, the first-order logic with the successor function and f is undecidable over integers. Finally, a linear time algorithm is given, which takes as input an automaton A in base b greater than 1 and accepts if and only if A accepts a regular set. A second algorithm, in quasi-cubic time, returns a $\mathsf{FO}[<,\mathrm{mod}]$-formula which defines the set of integers accepted by the automaton A.