Ehrenfeucht-Fraïssé goes elementarily automatic for structures of bounded degree

Antoine Durand-Gasselin and Peter Habermehl

Univ Paris Diderot, Sorbonne Paris Cité, LIAFA, UMR 7089 CNRS, F-75205 Paris, France
{adg,haberm}@liafa.jussieu.fr

Abstract

Many relational structures are automatically presentable, i.e. elements of the domain can be seen as words over a finite alphabet and equality and other atomic relations are represented with finite automata. The first-order theories over such structures are known to be primitive recursive, which is shown by the inductive construction of an automaton representing any relation definable in the first-order logic. We propose a general method based on Ehrenfeucht-Fraïssé games to give upper bounds on the size of these automata *and* on the time required to build them. We apply this method for two different automatic structures which have elementary decision procedures, Presburger Arithmetic and automatic structures of bounded degree. For the latter no upper bound on the size of the automata was known. We conclude that the very general and simple automata-based algorithm works well to decide the first-order theories over these structures.

1998 ACM Subject Classification F.4.1 Computational Logic; F.2.2 Computations on discrete structures

Keywords and phrases Automata-based decision procedures for logical theories, Automatic Structures, Ehrenfeucht-Fraïssé Games, Logics, Complexity

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

The idea of automatic structure first appeared in the work of Büchi and Elgot [1, 4] who showed how to use finite word automata to decide the weak second-order theory of integers with one successor and hence Presburger Arithmetic. Hodgson [7] exhibited that a general effective procedure to build an automaton whose language corresponds exactly to the solutions of a first-order formula over a relational structure can be given, if the basic relations can be described by automata. Khoussainov and Nerode [8] called these structures automatic structures and initiated a systematic study of which structures can be automatically presented.

The construction of an automaton accepting the solutions of a first order formula for an automatic structure is very simple. It can be done inductively on the structure of the formula by replacing the logical operators by corresponding operations on (deterministic) automata. For example, existential quantification can be done by projection and determinisation. The complexity in general is known to be primitive recursive, which is a tight bound since some automatic structures have a non-elementary first-order theory. Some work on the size of these automata has been done by Klaedtke [10] and Eisinger [3] for some (ω-)automatic structures, and for the well-studied Presburger Arithmetic an optimal time upper bound for the size [9] of the automaton and for its construction [2] has been obtained. In [3, 10] Ehrenfeucht-Fraïssé games are used as a proof tool. These games have been classically used to show bounds for the decision procedure of logical theories by using the fact that quantification over an infinite set can be replaced by quantification over some finite set (see e.g. [5]). First Klaedtke [10]

To appear in Proceedings of STACS 2012 (2 January 2012 preprint).

and then Eisinger [3] linked this approach with the automata approach by relating the states of a minimal automaton corresponding to a formula with equivalence classes (whose number can be bounded) determined by a suitable Ehrenfeucht-Fraïssé game. In [2] we obtain an upper bound for the complexity of the construction of the automata in a different way.

For automatic structures of bounded degree (i.e. elements of the domain are only in relation with a bounded number of other elements), several elementary complexity results were shown recently [11], notably a 2EXPSPACE algorithm for the uniform model-checking problem of injective automatic structures. These results are shown also via a kind of Ehrenfeucht-Fraïssé argument using Gaifman's locality principle [6] but the decision procedure is neither based on the inductive automata construction nor easily practically implementable. As far as we know, no upper bound on the size and the construction of the automaton corresponding to solutions of a formula has been shown. One result of this paper is a 3EXPTIME upper bound for this problem, using the simple inductive automaton construction.

To obtain this result we present an extension of Klaedtke's approach of the use of Ehrenfeucht-Fraïssé games to automatic structures. Roughly speaking, Klaedtke's approach consists in relating states of a minimal automaton of a formula to equivalence classes of suitably chosen refinements of relations defined by Ehrenfeucht-Fraïssé games (called Ehrenfeucht-Fraïssé relations). Showing an upper bound on the index of these relations then gives an upper bound on the size of the minimal automaton for a given formula. We use the same kind of relations and give in our main theorem general conditions allowing to obtain an upper bound even on the time needed to construct the automaton. Even though the automata constructed are in general not minimal, we show that they satisfy the crucial property that two words in the same equivalence class of the Ehrenfeucht-Fraïssé relation must lead to the same state of an automaton (even after determinisation of an automaton obtained by projection). This allows to obtain a bound on the size of all automata inductively constructed depending on the index of the Ehrenfeucht-Fraïssé relation.

We also apply our main theorem to Presburger Arithmetic (with *most*-significant digit first encoding), using very similar Ehrenfeucht-Fraïssé relations as [3] who shows a triple exponential upper bound on the size of the automaton, and we extend his results to show that even the construction can be done in 3EXPTIME. The same result for *least*-significant digit first encoding was shown in [2] using a complicated analysis of the automata obtained from quantifier-free formulas like in [9].

The paper is organised as follows. We first recall the notion of automatic structures and an explicit inductive construction of an automaton that accepts solutions of a formula. Then we present our main theorem which gives conditions on Ehrenfeucht-Fraïssé relations that imply upper bounds on the size (and the time required to inductively build it) of the automaton accepting solutions of a first-order formula. Finally, we show how to define Ehrenfeucht-Fraïssé relations allowing to apply our main theorem for automatic structures of bounded degree and for Presburger Arithmetic.

2 Preliminaries

We suppose that the reader is familiar with finite string (over finite alphabet) automata. We define the size of an automaton $A = (\Sigma, Q, q_0, F, \delta)$ as the space required to write it. We will only consider automata with alphabets such that letters are written in space logarithmic w.r.t. the size of the alphabet, and whose states are integers (ranging from 1 to the number of states). It is clear that the size of such an automaton is bounded by some polynomial in $|\Sigma|$ and $|Q|$. Many manipulations over deterministic automata (complementation, minimisation,

product of two automata, relabelling) can be performed within time polynomial w.r.t. the size of the input automata. In the following we use on-the-fly constructions, i.e. states in the constructed automata are created on demand; only reachable states are considered. Although the time (and space) complexity of automaton determinisation (using the well-known subset construction) can't be bounded by any polynomial of the size of the input, it is clear that it can be bounded by some fixed polynomial of the sizes of the input *and* the (trim) output automata. In the following we use mainly the same notation as [11].

2.1 Structures and first-order logic

A *signature* is a finite set $\mathcal{S}$ of *predicate* symbols. Each predicate symbol $P \in \mathcal{S}$ has a fixed arity denoted by ar_P. A *relational structure* of signature $\mathcal{S}$ is a couple $\mathcal{A} = (A, (P^{\mathcal{A}})_{P\in\mathcal{S}})$, with A a set called *domain* and $P^{\mathcal{A}} \subseteq A^{ar_P}$. We will identify a predicate P with its *interpretation* $P^{\mathcal{A}}$. We say that P holds for $(a_1, \dots, a_{ar_P}) \in A^{ar_P}$ (also formulated $P(a_1, \dots, a_{ar_P})$ holds) if $(a_1, \dots, a_{ar_P}) \in P^{\mathcal{A}}$. A *congruence* on the relational structure $\mathcal{A} = (A, (P^{\mathcal{A}})_{P\in\mathcal{S}})$ is an equivalence relation $\equiv$ on A such that for all $P \in \mathcal{S}$ and $a_1, \dots, a_{ar_P}, b_1, \dots, b_{ar_P} \in A$ such that $a_i \equiv b_i$ (for any $i \leq ar_P$), we have that if $P(a_1, \dots, a_{ar_P})$ holds, then $P(b_1, \dots, b_{ar_P})$ holds as well. We denote by $[a]_{\equiv}$ (or $[a]$) the equivalence class of $a \in A$ w.r.t. $\equiv$. $A/_{\equiv}$ denotes the set of all equivalence classes. For each predicate P we can define the quotient predicate $P/_{\equiv}$ by $P/_{\equiv}([a_1], \dots, [a_{ar_P}])$ holds iff $P(a_1, \dots, a_{ar_P})$ holds. Furthermore the quotient structure $\mathcal{A}/_{\equiv}$ is defined as the structure $(A/_{\equiv}, (P/_{\equiv})_{P\in\mathcal{S}})$.

We write $\bar{\alpha}_r$ as a shorthand for $(\alpha_1, \dots, \alpha_r)$, with the α_i possibly being elements of a set (typically A), or variables. We also write $[1, r]$ to denote the set of integers between 1 and r.

First-order formulas over the signature $\mathcal{S}$ are defined as usual as either:

- an atomic formula $\varphi(\bar{x}_r)$ over r variables ($\bar{x}_r$), i.e. of the form $P(x_{j_1}, \dots, x_{j_{ar_P}})$ for some predicate P with arity ar_P and $(j_k)_{1\leq k\leq ar_P}$ some ar_P-tuple of elements in $[1, r]$. Notice that some variables may not appear syntactically in the formula whereas others may appear more than once. The size of such a formula is defined as $\|\varphi\| = ar_P$.
- a conjunction, $\varphi(\bar{x}_r) = \varphi_1(\bar{x}_r) \wedge \varphi_2(\bar{x}_r)$ with φ_1 and φ_2 two first order formulas over the *same*[1] r variables. We define its size to be $\|\varphi\| = 1 + \|\varphi_1\| + \|\varphi_2\|$.
- a negation, $\varphi(\bar{x}_r) = \neg\varphi_1(\bar{x}_r)$ with φ_1 a formula over r variables; $\|\varphi\| = 1 + \|\varphi_1\|$.
- or an existential quantification, i.e. $\varphi(\bar{x}_r) = \exists y.\varphi_1(\bar{x}_r, y)$ where y is a fresh variable and φ_1 a formula over $r + 1$ variables; $\|\varphi\| = 1 + \|\varphi_1\|$.

Given a formula $\varphi(\bar{x}_r)$ over r variables, we denote by $\mathcal{A} \vDash \varphi(\bar{a}_r)$ (with $\bar{a}_r \in A^r$) that the formula φ is valid (in the usual sense) when we substitute the variables with the corresponding constants. We can associate to any formula its set of solutions (in the structure $\mathcal{A}$ which will always be clear from the context), that is the set of assignments of the free variables seen as r-tuples of elements of A that satisfy (in the usual sense) the formula. Thus first-order (r-variables) formulas define (r-ary) *first-order relations* over the domain.

2.2 Automatic presentations

Informally, an automatic structure is a relational structure whose domain can be represented by a regular language over an alphabet Σ such that ar-ary predicates can also be seen

[1] This will be useful for defining easily the automata corresponding to a formula. Notice that this is not a restriction, since if two formulas do not syntactically contain the same variables, we can consider that they have the same variables by adding them implicitly, e.g. in $P(x_1, x_2) \wedge P(x_2, x_3)$ both subformulas have free variables x_1, x_2, x_3.

as regular languages. We extend the representation of the domain as a regular language to a representation of any cartesian power of the domain as a regular language. As we can't represent a k-tuple of words of Σ^* with a word over the alphabet Σ^k —the k words do not necessarily have the same length— we pad the shorter words with an additional symbol $\diamond \notin \Sigma$. We repeatedly add $\diamond$ at the beginning of the shorter words (rather than at the end as done usually) giving the k words the same length leading to the definition of (right-aligning) *convolution* of words: Let $\bar{a}_k$ be a k-tuple of words in Σ^*. We write $\langle \bar{a}_k \rangle$ for its convolution which is a word over the alphabet $(\Sigma \cup \{\diamond\})^k \backslash \{\diamond\}^k$ (denoted by $\hat{\Sigma}_k$). Its length is $|\langle \bar{a}_k \rangle| = \max_i(|a_i|)$ where $|a_i|$ denotes the length of a_i and its j-th letter (starting from 1) is $(a_1[|a_1| - |\langle \bar{a}_k \rangle| + j], a_2[|a_2| - |\bar{a}_k| + j], \ldots, a_k[|a_k| - |\langle \bar{a}_k \rangle| + j])$ where $a_i[|a_i| - |\langle \bar{a}_k \rangle| + j]$ denotes $\diamond$, if $(|a_i| - |\langle \bar{a}_k \rangle| + j)$ is not strictly positive, and the $(|a_i| - |\langle \bar{a}_k \rangle| + j)$-th letter of a_i otherwise. For example, we have $\langle bab, \epsilon, bc \rangle = (b, \diamond, \diamond)(a, \diamond, b)(b, \diamond, c)$. Conversely, we define the operators $(.\downarrow_i)_{1 \leq i \leq k}$ and $(.\Downarrow_i)_{1 \leq i \leq k}$ for words in $\hat{\Sigma}_k^*$. $.\downarrow_i$ is a monoïd morphism from $\hat{\Sigma}_r^*$ to $(\Sigma \cup \{\diamond\})^*$ projecting each letter of the word to its i-th component. $w\Downarrow_i$ is defined as the greatest suffix of $w\downarrow_i$ not starting with $\diamond$. We write $\overline{w\Downarrow}_k$ as a shorthand for $(w\Downarrow_1, \ldots, w\Downarrow_k)$. The duality between convolution and $\Downarrow_.$ is exhibited by the identity: $\bar{a}_k = \overline{\langle \bar{a}_k \rangle \Downarrow}_k$.

▶ **Definition 1.** An *r-variable automaton* A over Σ is a finite automaton over the alphabet $\hat{\Sigma}_r$ such that $L(A) \subseteq \{\langle \overline{w}_r \rangle \mid \forall i \in [1, r], w_i \in \Sigma^*\}$. It represents the r-ary relation $R(A) = \{\overline{w\Downarrow}_k \mid w \in L(A)\}$.

Let us notice that provided letters of the alphabet Σ can be written within space logarithmic w.r.t. $|\Sigma|$, letters of $\hat{\Sigma}_r$ can be written within space logarithmic w.r.t. $|\hat{\Sigma}_r|$. Thus most operations over r-variable automata will also be achieved within polynomial time.

▶ **Definition 2.** An *automatic presentation* is a tuple $AP = (\Sigma, \mathcal{S}, A_D, A_=, (A_P)_{P \in \mathcal{S}})$ where Σ is a finite alphabet, $\mathcal{S}$ is a signature, A_D is an automaton over Σ, $(A_P)_{P \in \mathcal{S}}$ is a family of ar_P-variable automata over Σ and $A_=$ is a 2-variable automaton over Σ such that $R(A_=)$ is a congruence on the structure $(L(A_D), (R(A_P))_{P \in \mathcal{S}})$.

An automatic presentation AP is called deterministic, if all its automata are deterministic. Its size $\|AP\|$ is the space required to write all its automata. The structure *presented* by AP is the quotient $\mathcal{A}(AP) = (L(A_D), (R(A_P))_{P \in \mathcal{S}})/_{R(A_=)}$. AP is *injective* if $R(A_=)$ is the identity relation. A relational structure is called *automatically presentable* (or automatic) if there is an automatic presentation isomorphic to it. The element $[w]_{R(A_=)}$ with $w \in L(A_D)$ of the structure $\mathcal{A}(AP)$ is denoted by $[w]$. Given $u \in \hat{\Sigma}_r^*$ a convolution of r words in Σ^* we say that u represents $([u\Downarrow_1], \ldots, [u\Downarrow_r])$.

2.3 Automata-based model-checking

We are interested in the following problem.

▶ **Definition 3.** The model-checking problem for a relational structure $\mathcal{A} = (A, (P)_{P \in \mathcal{S}})$ over a signature $\mathcal{S}$ and a first-order sentence φ over the same $\mathcal{S}$ is to decide whether $\mathcal{A} \vDash \varphi$.

For automatic structures, this problem has been shown decidable using the following theorem [7, 8]. It provides also a way to get a representation of all solutions of a formula.

▶ **Theorem 4.** *Given an automatic presentation $AP = (\Sigma, \mathcal{S}, A_D, A_=, (A_P)_{P \in \mathcal{S}})$ and a first-order formula φ over $\mathcal{S}$ with r free variables one can build an r-variable automaton A_φ over Σ such that $R(A_\varphi) = \{(w_1, \ldots, w_r) \in L(A_D)^r \mid \mathcal{A}(AP) \vDash \varphi([w_1], \ldots, [w_r])\}$.*

In Section 3 we study the complexity of the automaton construction, i.e. the size of the automaton A_φ corresponding to a formula φ as well as the time needed to construct it. This in turn gives complexity bounds for the model-checking problem. We first give here a detailed description of the automaton construction. We consider *deterministic* automatic presentations. Given a formula φ (with r free variables) we have to build an automaton that distinguishes vectors of elements of the domain whose representatives satisfy the formula from those that don't. Intuitively, it is straightforward to build such automata inductively. We first give the construction of the r-variable minimal automaton A_{D^r} that accepts exactly all convolutions of words in $L(A_D)$. We will ensure we only build automata which reject any word not representing a convolution of words in $L(A_D)$ by product with A_{D^r}.

To construct A_{D^r} we build an automaton accepting $\diamond^* L(A_D)$ denoted by $A'_D = (\Sigma \cup \{\diamond\}, Q'_D, q_0, F, \delta)$ which has just one more state than A_D. Then we construct $A'_{D^r} = (\hat{\Sigma}_r, Q_{D^r}, q'_0, F', \delta_r)$ on-the-fly as follows: Q_{D^r} is the subset of $(Q'_D)^r$ reached by the on-the-fly construction, $q'_0 = (q_0, \dots, q_0)$, $F' = F^r$ and δ_r is defined as: let $q'_i = \delta(q_i, a_i)$ for all i, then $\delta_r((q_1, \dots, q_r), \bar{a}_r) = (q'_1, \dots, q'_r)$. Finally, A_{D^r} is obtained by minimising A'_{D^r}. It is clear that the time to build this minimal automaton is bounded by some polynomial of $\|AP\|^r$: indeed as $\|AP\|$ is greater than both $|\Sigma|$ and the number of states in A_D, $\|AP\|^r$ is greater than the number of states of A'_{D^r} and the size of its alphabet. Remark that the fact that A_{D^r} is minimal is needed later in Section 3.

We now detail an inductive (on the structure of the formula) construction of the r-variable automaton accepting representatives of solutions of some formula φ with r free variables.

Let's start by the **case of atomic formulas**, i.e. of the form $\varphi(\bar{x}_r) = P(x_{j_1}, \dots, x_{j_{ar}})$ with P a predicate of $\mathcal{S}$ with arity ar, and the $(j_k)_{1 \leq k \leq ar}$ a tuple of ar integers in $[1, r]$. The construction of the r-variable automaton $A_{P(x_{j_1}, \dots, x_{j_{ar}})}$ is performed in two steps: first we build $A'_{P(x_{j_1}, \dots, x_{j_{ar}})}$ which within words corresponding to a convolution of words in $L(A_D)$ accepts only those satisfying $P(x_{j_1}, \dots, x_{j_{ar}})$. As we introduce extra tracks for variables not appearing in $P(x_{j_1}, \dots, x_{j_{ar}})$, this automaton may accept words that are not convolutions of words in $L(A_D)$. Therefore we build $A_{P(x_{j_1}, \dots, x_{j_{ar}})}$ as the minimal automaton accepting the intersection of languages of $A'_{P(x_{j_1}, \dots, x_{j_{ar}})}$ and A_{D^r}. Let $A_P = (\hat{\Sigma}_{ar}, Q_P, q_0, F_P, \delta_P)$, then $A'_{P(x_{j_1}, \dots, x_{j_{ar}})} = (\hat{\Sigma}_r, Q_P, q_0, F_P, \delta')$ where δ' is given as follows: for all $q \in Q_P$ and $(l_1, \dots, l_r) \in \hat{\Sigma}_r$, $\delta'(q, (l_1, \dots, l_r)) = q_0$ if for all $k \leq r$, $l_{j_k} = \diamond$ and $\delta'(q, (l_1, \dots, l_r)) = q'$, if $\delta_P(q, (l_{j_1}, \dots, l_{j_{ar}})) = q'$. Then we obtain $A_{P(x_{j_1}, \dots, x_{j_{ar}})}$ by minimising the product of $A'_{P(x_{j_1}, \dots, x_{j_{ar}})}$ and A_{D^r}. It is clear that the time required to build $A_{P(x_{j_1}, \dots, x_{j_{ar}})}$ is also bounded by some polynomial of $\|AP\|^r$. Having a minimal automaton is needed in section 3.

The case of negation is closely related to automaton complementation which is simple for deterministic automata which we use. But a word in $\hat{\Sigma}_r^*$ is neither necessarily a convolution of words of $L(A_D)$, nor a convolution of words in Σ^*. Therefore the automaton for $\neg\psi$ is built from the complement of the automaton for ψ, followed by an on-the-fly product with A_{D^r}. Notice that we don't minimise this automaton; our results on complexity will still hold.

The case of conjunction is straightforward thanks to the fact that the free variables of the two formulas must be the same. The automaton is built as an on-the-fly product. We also do not need to minimise this inductively generated automaton.

The last case is $\varphi = \exists y.\psi(\bar{x}_r, y)$. By induction (as ψ is a subformula of φ) we build the $(r+1)$-variable automaton $A_\psi = (\hat{\Sigma}_{r+1}, Q_\psi, q_0, F_\psi, \delta_\psi)$. We assume that the track corresponding to variable y in A_ψ is the $(r+1)$-th (other cases are the same). We define from the $(r+1)$-variable automaton A_ψ by projection a *non-deterministic* r-variable automaton A'_φ that accepts representatives of solutions of φ. $A'_\varphi = (\hat{\Sigma}_r, Q_\varphi, Q_0, F_\varphi, \delta_\varphi)$ is built as follows: $Q_\varphi = Q_\psi$, the set of initial states Q_0 is the set of states reachable in A_ψ from q_0 by

transitions labelled in $\{\diamond\}^r \times \Sigma$, $F_\varphi = F_\psi$ and $\delta_\varphi(q,a) = \{q' \mid \exists b \in \Sigma \cup \{\diamond\}.\delta_\psi(q,(a,b)) = q'\}$.

We show the correctness of our construction. First we show that any word accepted by A'_φ is a convolution of words representing a solution of φ. Consider a word u that is accepted by A'_φ (see Fig. 1). Then there is an accepting run of u. Denote by q_1 the first state of the run (which is an initial state of A'_φ) and by q_2 the last state of the run ($q_2 \in F_\psi$). From this run we can get a word $w' \in \hat{\Sigma}^*_{r+1}$ (with $w'{\downarrow_i} = u{\downarrow_i}$ for any $i \leq r$) reaching q_2 from q_1 in A_ψ. By definition of the initial states of A'_φ, there is a word w'' in $(\{\diamond\}^r \times \Sigma)^*$ such that w'' reaches q_1 from q_0 in A_ψ. Thus $w''w'$ is accepted by A_ψ, which means it is a convolution of $r+1$ words in $L(A_D)$, so for any $i \leq r+1$, $(w''w'){\Downarrow_i} \in L(A_D)$. By definition of w' and w'', $(w''w'){\Downarrow_i} = u{\Downarrow_i}$ for any $i \leq r$ meaning u is a convolution of r words all in $L(A_D)$. We know that $([(w''w'){\Downarrow_i}])_{i\leq r+1}$ satisfies ψ, so $([w''w'{\Downarrow_i}])_{i\leq r} = ([u{\Downarrow_i}])_{i\leq r}$ satisfies $\exists y.\psi(\bar{x}_r, y)$. Thus u is a convolution of words in $L(A_D)$ that represent a solution of φ. We now show that A'_φ accepts any convolution of words in $L(A_D)$ that represent a solution of φ. Consider a solution of φ and take a representation u. There must exist a word w' such that the convolution of u and w' is accepted by A_ψ. Then u is also accepted by A'_φ. That concludes the proof of correctness of the construction of A'_φ an automaton accepting solutions of φ.

Finally we get A_φ by determinising A'_φ using the standard on-the-fly subset construction. Though in practice one can minimise this automaton, our complexity results still hold even if we don't.

3 Ehrenfeucht-Fraïssé relations for automata

Ehrenfeucht-Fraïssé equivalence relations are a general tool to establish upper and lower bounds on the complexity of the first-order theory over relational structures. They have been used for example extensively by Ferrante and Rackoff [5] to give some upper bounds for the decision procedure of several first-order logics. Let $\mathcal{A}$ be a relational structure with domain A. A set of Ehrenfeucht-Fraïssé equivalence relations for $\mathcal{A}$ is a ($\mathbb{N}^2$-indexed) family of relations $(E^r_m)_{m\in\mathbb{N},r\in\mathbb{N}}$ over A^r such that:

- $\bar{a}_r E^r_0 \bar{b}_r$ iff for any quantifier-free formula φ over r free variables: $\mathcal{A} \vDash \varphi(\bar{a}_r)$ iff $\mathcal{A} \vDash \varphi(\bar{b}_r)$
- Let $\bar{a}_r E^r_{m+1} \bar{b}_r$, then $\forall a_{r+1} \in A$, $\exists b_{r+1} \in A$ such that $(\bar{a}_r, a_{r+1}) E^{r+1}_m (\bar{b}_r, b_{r+1})$.

As a result any first-order formula with r free variables and quantifier-depth at most m cannot distinguish between tuples in the same E^r_m equivalence class. In [5] it is shown that in a first-order formula for several logics like Presburger Arithmetic quantifiers ranging over all elements of the domain can be restricted to finite subsets, hence obtaining space-constrained non-deterministic algorithms that exhaustively check the validity of these formulas with restricted quantification. The complexity of the decision procedures in [5] is closely related to that of deciding whether a predicate holds (usually simple) and the space required to enumerate these finite subsets, which depends on the size of the candidate b_{r+1}.

As we work on automatic presentations, the domain is a language and tuples of elements of the domain can also be seen as words. Thus we can consider the family of Ehrenfeucht-Fraïssé relations as a family of relations over languages and also impose that these relations are right-congruences allowing to relate equivalence classes with states of an automaton. This idea was used first by Ladner [12], working on monadic second-order and first-order logics on words, to deduce from the finiteness of the index the possibility to build a finite automaton. Recently Klaedtke [10] and then Eisinger [3] used this idea to give upper bounds on the size of automata for some (ω-)automatic structures. Our theorem below, not only bounds the size of automata but also allows us to establish an upper bound for the (time) complexity of the inductive construction of an r-variable automaton accepting solutions of a first-order

formula. This is possible since we can show that all automata inductively constructed satisfy the property that two words in the same equivalence class lead to the same state.

▶ **Theorem 5.** *Let $AP = (\Sigma, \mathcal{S}, A_D, A_=, (A_P)_{P\in\mathcal{S}})$ be a deterministic automatic presentation and (E^r_m) a family of* ***binary symmetric reflexive transitive relations*** *over $\hat{\Sigma}^*_r$ such that:*

1. *For any m, words of $\hat{\Sigma}^*_r$ that do not represent a convolution of words in Σ^* are alone in a same E^r_m equivalence class. The empty-word, ϵ, is alone in its E^r_m equivalence class.*
2. *Let uE^r_0v, if u is a convolution of r words in $L(A_D)$ then so is v and the r-tuples represented by u and v* ***satisfy the same atomic formulas*** *in the structure presented by AP.*
3. ***(back-and-forth)*** *If u is a convolution of r words in Σ^* and $uE^r_{m+1}v$, then for any $u_{r+1} \in \Sigma^*$, there exists $v_{r+1} \in \Sigma^*$ such that $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle E^{r+1}_m \langle \overline{v\Downarrow}_r, v_{r+1}\rangle$.*
4. *The E^r_m are* ***right-congruence*** *relations: $uE^r_m v$ implies $\forall w \in \hat{\Sigma}^*_r$, $uwE^r_m vw$.*
5. *The* ***index*** *of E^r_m is* ***bounded*** *by $f(m + r)$, for some function f.*

Then the following holds: For any first-order formula φ over $\mathcal{S}$ with quantifier depth at most m and r free variables, the inductive construction of a deterministic r-variable automaton for φ builds an automaton with at most $f(m + r)$ states and can be done within time bounded by $c_1\|\varphi\| \left(\|AP\|^{m+r} f(m + r)\right)^{c_2}$ for some constants c_1 and c_2.

Proof. We first remark that hypothesis 2 can be generalised to: for any m, if $uE^r_m v$ and u is a convolution of r words in $L(A_D)$, then so is v and the r-tuples represented by u and v satisfy the same atomic formulas (and even the same r-variables formulas with quantifier depth at most m). We show that by applying m times hypothesis 3 (with a valid u_{r+1}), and then discarding the m new components.

The proof is by structural induction over formulas φ. Each formula has some quantifier depth m and some number r of free variables. The bound on the number of states is shown by proving inductively that any two words in $\hat{\Sigma}^*_r$ in the same E^r_m equivalence class reach the same state in the constructed automaton. Hence the number of states of these automata is bounded by $f(m + r)$. We choose the constants c_1 and c_2 as the maximum of the constants needed to bound the construction of the automata below. Sizes of automata are always bounded by a fixed polynomial of $\|AP\|^{m+r} f(m + r)$, since the alphabet is bounded by $\|AP\|^{m+r}$, and the number of states by $f(m + r)$.

We start with the **case of atomic formulas**, i.e. φ is of the form $P(x_{j_1}, \ldots, x_{j_r})$ where P is a predicate with arity ar and $(j_k)_{1\leq k\leq ar}$ a family of ar integers in $[1, r]$. $A_{P(x_{j_1},\ldots,x_{j_r})}$ is built as a minimal automaton. If u and v are E^r_m equivalent, according to hypothesis 4, for any $w \in \hat{\Sigma}^*_r$, $uwE^r_m vw$. Thus with generalised hypothesis 2, this means that uw represents a solution of $P(x_{j_1}, \ldots, x_{j_r})$ iff vw does, so $uw \in L(A_{P(x_{j_1},\ldots,x_{j_r})})$ iff $vw \in L(A_{P(x_{j_1},\ldots,x_{j_r})})$. The Myhill-Nerode theorem allows us to conclude that u and v reach the same state in $A_{P(x_{j_1},\ldots,x_{j_r})}$ as it is minimal. The time to build this automaton is bounded by a fixed polynomial of $\|AP\|^r$.

The case of negation is $\varphi = \neg\psi$. A_φ is built as a product automaton between the complement of A_ψ and A_{D^r}. Let $u, v \in \hat{\Sigma}^*_r$ with $uE^r_m v$. Hypothesis 4 implies that for any $w \in \hat{\Sigma}^*_r$, $uwE^r_m vw$; according to generalised hypothesis 2 this implies that uw is a convolution of words in $L(A_D)$ (and thus $uw \in L(A_{D^r})$) iff vw also is. As A_{D^r} is minimal by construction, the Myhill-Nerode theorem ensures that u and v reach the same state in A_{D^r}. As u and v reach the same state in A_ψ by induction hypothesis, they also reach the same state in the corresponding product automaton, which therefore has at most $f(m + r)$ states. By induction hypothesis, it takes time less than $c_1(\|\varphi\| - 1)(\|AP\|^{m+r} f(m + r))^{c_2}$ to build A_ψ. A_ψ has at most $f(m + r)$ states, and an alphabet of size smaller than $\|AP\|^r$. Thus any

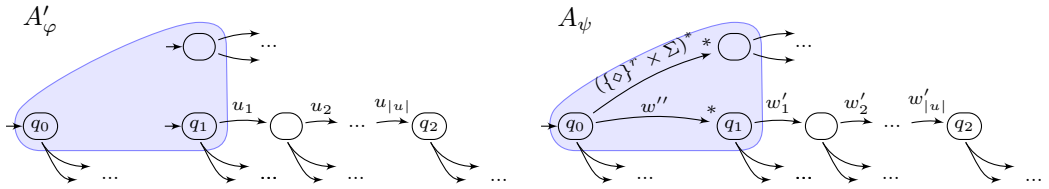

Figure 1 Getting a word $w''w' \in \hat{\Sigma}^*_{r+1}$ reaching q_2 in A_ψ from $u \in \hat{\Sigma}^*_r$ reaching q_2 from q_1 in A_φ.

manipulation over A_ψ will take time less than a fixed polynomial of $\|AP\|^{m+r} f(m+r)$, this includes its complementation and product with A_{D^r}.

The case of conjunction is $\varphi = \varphi_1 \wedge \varphi_2$. By induction hypothesis, $uE^r_m v$ implies that u and v reach the same state in A_{φ_1} and in A_{φ_2}, hence they will reach the same state in the product automaton (we don't even need to minimise A_φ to ensure this property). The time upper bound also holds as it takes total time less than $c_1(\|\varphi\| - 1)(\|AP\|^{m+r} f(m+r))^{c_2}$ to build both A_{φ_1} and A_{φ_2} whose sizes are bounded by a fixed polynomial of $\|AP\|^{m+r} f(m+r)$, hence it takes a total time less than $c_1\|\varphi\|(\|AP\|^{m+r} f(m+r))^{c_2}$ to build A_φ.

The last case is $\varphi = \exists y.\psi(\bar{x}_r, y)$, where ψ has $r+1$ free variables and quantifier-depth at most $m-1$. Its automaton $A_\psi = (Q_\psi, q_0, F_\psi, \delta_\psi)$ is inductively built within time $c_1(\|\varphi\| - 1)(\|AP\|^{m+r} f(m+r))^{c_2}$. We assume that the track corresponding to the variable y in A_ψ is the $(r+1)$-th. Let $A'_\varphi = (\hat{\Sigma}_r, Q_\varphi, Q_0, F_\varphi, \delta_\varphi)$ be the (non-deterministic) automaton as constructed in Section 2.3. We denote q_s the state of A_ψ reached by all words that are not convolutions of words in Σ^*. Let $uE^r_m v$. We show that u and v reach the same set of states in A'_φ. There are three cases: (1) u is not a convolution of words in Σ^*. Then nor is v and they obviously only reach the state q_s in A'_φ. (2) $u = \epsilon$, then $v = \epsilon$ and u and v are equal and clearly reach the same states. (3) $u \neq \epsilon$ (then $v \neq \epsilon$) and u is a convolution of words in Σ^* (then so is v). This first implies that both u and v can reach q_s in A'_φ as (for any $a \in \Sigma$) $\langle \overline{u\Downarrow}_r, a\diamond\rangle$ and $\langle \overline{u\Downarrow}_r, a\diamond\rangle$ are not convolutions of words in Σ^* so they both reach q_s in A_ψ. Assume now that u reaches a state $q_2 \neq q_s$ from q_1 (as depicted in Fig. 1). We can deduce w' and w'', such that $w'' \in (\{\diamond\}^r \times \Sigma)^*$ and for all $i \leq r$, $w'\downarrow_i = u\downarrow_i$, and $w''w'$ reaches q_2 from q_0 in A_ψ. As $w''w'$ does not reach q_s (in A_ψ), it is a convolution of words in Σ^* (induction hypothesis and hypothesis 1). Notice that $w''w'$ is the convolution of $(w\Downarrow_i)_{1\leq i\leq r}$ and $(w''w')\Downarrow_{r+1}$. According to hypothesis 3, there is a word $v' \in \Sigma^*$ such that $\langle \overline{v\Downarrow}_r, v'\rangle$ (the convolution of the $(v\Downarrow_i)_{1\leq i\leq r}$ and v') is E^{r+1}_{m-1} equivalent to $w''w'$. According to the induction hypothesis this implies $w''w'$ and $\langle \overline{v\Downarrow}_r, v'\rangle$ reach the same state in A_ψ, so there is a word reaching q_2 in A_ψ that is a convolution of the $(v\Downarrow_i)_{1\leq i\leq r}$ with another word in Σ^*, which means that v can also reach q_2 in A'_φ.

We have shown that any $u, v \in \hat{\Sigma}^*_r$ with $uE^r_m v$ reach the same set of states in A'_φ, hence by definition of the subset construction, they reach the same state in A_φ. Thus, A_ψ, A'_φ and A_φ each have at most $f(m+r)$ states over an alphabet bounded by $\|AP\|^{m+r}$ and it takes time polynomial w.r.t. the size of these automata to build A_φ from A_ψ, thus within time $c_1(\|AP\|^{m+r} f(m+r))^{c_2}$. That concludes the induction. ◀

Notice that we don't need to minimise any inductively-generated automaton during the construction. Furthermore remark that our approach only uses Ehrenfeucht-Fraïssé relations to prove an upper bound of the complexity of the automata construction (which might be much more efficient in particular cases), whereas Ferrante and Rackoff [5] need these relations to devise decision procedures.

4 Automata construction for structures of bounded degree

Automatic structures of bounded degree are structures whose uniform model-checking problem is known to be elementary [11]. Informally, a structure has bounded degree if there is a finite upper bound on the number of elements any element of the domain can be in relation with. We first formally define the necessary notions. The *Gaifman-graph* $G(\mathcal{A})$ of a relational structure $\mathcal{A} = (A, (P)_{P\in\mathcal{S}})$ is the graph $G(\mathcal{A}) = (A, \{(a,b) \in A \times A \mid \exists P \in \mathcal{S}\, \exists i,j.\, \exists \bar{a}_{ar_P} \in A^{ar_P}.\, a_i = a, a_j = b,$ and $P(\bar{a}_{ar_P})$ holds$\})$. A structure has *bounded degree* if its Gaifman-graph has bounded degree, i.e. there exist a constant δ such that every node of the graph is adjacent to at most δ other nodes. The minimal such δ is called the *degree* of $\mathcal{A}$. An automatic presentation AP is of bounded degree, if $\mathcal{A}(AP)$ is of bounded degree. Then, the degree of AP is the same as the degree of $\mathcal{A}(AP)$. The following proposition is from [11].

▶ **Proposition 6.** *Let AP be an automatic presentation of bounded degree. Its degree is bounded by $2^{2^{\|AP\|^c}}$ for some constant c. If AP is injective, then its degree is bounded by $2^{\|AP\|^c}$ for some constant c.*

The following theorem is an application of Theorem 5.

▶ **Theorem 7.** *The construction of the automaton for injective deterministic automatic structures AP with bounded degree leads to an automaton whose size is bounded by $f(m+r) = 2^{2^{3^{m+r+c_3\cdot\|AP\|+2}}}$ within time $c_1\|\varphi\|(\|AP\|^{m+r} f(m+r))^{c_2}$ for some constants c_1, c_2 and c_3 independent of AP.*

To prove the theorem we have to give Ehrenfeucht-Fraïssé relations satisfying the hypotheses of Theorem 5. Let us fix for the rest of this section an injective deterministic automatic presentation $AP = (\Sigma, \mathcal{S}, A_D, A_=, (A_P)_{P\in\mathcal{S}})$ of bounded degree δ. Thanks to Proposition 6 we know that $\delta \leq 2^{\|AP\|^c}$. We can furthermore assume that the automata are minimal. Let Q_D be the set of states of A_D and Q_P the set of states of each A_P. We denote ar_P the arity of each predicate P, and $ar_M = \max_{P\in\mathcal{S}} ar_P$.

Using $\mathcal{A}(AP)$ we define a structure $\mathcal{A}(AP)_{sat}$, for which it will be easier to express Ehrenfeucht-Fraïssé relations satisfying all the hypotheses of Theorem 5. For example, to show right-congruence it will be necessary to be able to distinguish words leading to different states in the automata of AP.

$\mathcal{A}(AP)_{sat}$ is defined as the structure $(\Sigma^*, (P)_{P\in\mathcal{S}'})$ with the following predicates in the signature $\mathcal{S}'$: an "empty-word" monadic predicate denoted P_ϵ which holds exactly for the empty word, a monadic predicate $P_{D,q}$ for each state $q \in Q_D$ holding exactly for words that reach q in A_D and a predicate $P_{P,q}$ with arity r for each predicate P with arity r and each state $q \in Q_P$ that is not a sink state (i.e. with empty residual). $P_{P,q}$ holds exactly for r-tuples whose convolution reaches q in A_P.

▶ **Lemma 8.** *The degree of the structure $\mathcal{A}(AP)_{sat}$ is bounded by $\delta' = \delta \sum_{P\in\mathcal{S}}((|Q_P|-1)ar_P^2)$.*

We prove this by contradiction: if x is in relation with too many words in $\mathcal{A}(AP)_{sat}$, too many ar_P-tuples containing x reach a state in A_P from which a final state can be reached. From this, we can deduce a word of $L(A_D)$ in relation with more than δ words in $\mathcal{A}(AP)$.

Before we define the Ehrenfeucht-Fraïssé relations we need the following definitions:

▶ **Definition 9.** For a relational structure $\mathcal{B}$ with domain B the Gaifman metric $d_{\mathcal{B}}(b_1, b_2)$ for $b_1, b_2 \in B$ is the distance between b_1 and b_2 in $G(\mathcal{B})$, that is the length of the shortest path connecting b_1 and b_2 in $G(\mathcal{B})$ (or $+\infty$ if b_1 and b_2 don't belong to the same connected

component). The $\mathcal{B}$-sphere of radius $d \in \mathbb{N}$ around $b \in B$ denoted by $\mathcal{S}_{\mathcal{B}}(b,d)$ is defined as the set $\{b' \in B \mid d_{\mathcal{B}}(b,b') \leq d\}$. We extend the notion of sphere around a point to spheres around r points, we call that the $\mathcal{B}$-neighbourhood of radius d around $\bar{b}_r$: for $\bar{b}_r \in B^r$ and $d \in \mathbb{N}$, $\mathcal{N}^r_{\mathcal{B}}(\bar{b}_r, d) = \bigcup_{1 \leq i \leq r} \mathcal{S}_{\mathcal{B}}(b_i, d)$. Finally, a $\mathcal{B}$-isomorphism ξ from $B_1 \subseteq B$ to $B_2 \subseteq B$ is a bijection that maps B_1 to B_2 such that for any predicate P of $\mathcal{B}$ with arity ar_P, and any ar_P-tuple $\bar{b}_{ar_P}$ of B_1, $P(b_1, \ldots, b_{ar_P})$ holds iff $P(\xi(b_1), \ldots, \xi(b_{ar_P}))$ holds. We will say that B_1 and B_2 are $\mathcal{B}$-isomorphic and write $B_1 \overset{\xi}{\simeq}_{\mathcal{B}} B_2$.

The Ehrenfeucht-Fraïssé relations that we define roughly state that r-tuples of words are equivalent when they have sufficiently large isomorphic neighbourhoods (i.e. of exponential radius) in the structure $\mathcal{A}(AP)_{sat}$.

▶ **Definition 10.** We define the equivalence relations E^r_m over $\hat{\Sigma}^*_r$ as follows: First we partition $\hat{\Sigma}^*_r$ in two disjoint subsets, V_r the set of words that are convolution of words in Σ^* and I_r the set of words that aren't. Then we define $uE^r_m v$ iff (1) u and v are in I_r, (2) or $u = v = \epsilon$ (3) or u and v are in $V_r \backslash \{\epsilon\}$ and $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m - 1)/2) \overset{\xi}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m - 1)/2)$ for some ξ such that $\xi(u\Downarrow_i) = v\Downarrow_i$.

It is clear that the relations E^r_m are symmetric, reflexive and transitive, and satisfy hypothesis 1 of Theorem 5. Due to space limitations, we just sketch here the proofs that this family of relations satisfy the other hypotheses of Theorem 5. To show it satisfies hypothesis 2 we essentially just need the fact that atomic formulas of $\mathcal{A}(AP)$ can be expressed as quantifier-free formulas in $\mathcal{A}(AP)_{sat}$. The back-and-forth property (hypothesis 3) is proved by exhibiting the v_{r+1} and extending the isomorphism. v_{r+1} is: (1) the image of u_{r+1} by the neighbourhood isomorphism, if u_{r+1} is "close" to $(\overline{u\Downarrow}_r)$ (i.e. distance smaller than 3^m) (2) u_{r+1}, if it is "far" from the $(\overline{v\Downarrow}_r)$ and the $(\overline{u\Downarrow}_r)$, (3) some iterated preimage of u_{r+1} by the neighbourhood isomorphism, if u_{r+1} is in the neighbourhood of radius 3^m around $(\overline{v\Downarrow}_r)$ but "far" from $(\overline{u\Downarrow}_r)$. The closure of this relation by appending arbitrary suffix (hypothesis 5) crucially relies on the additional predicates provided by $\mathcal{A}(AP)_{sat}$.

Finally the following lemma states an upper bound on the index of the E^r_m relations:

▶ **Lemma 11.** *The index of E^r_m is bounded by $2^{2^{2^{g(m,r,ar_M,\delta,\|AP\|)}}}$ with $g(m, r, ar_M, \delta, \|AP\|) = (m+2).\log_2(3) + \log_2(\log_2(r)) + 2\log_2(ar_M) + \log_2(\log_2(\delta)) + \log_2(\log_2 \|AP\|)$.*

This lemma can be proved noticing that as the degree of $G(\mathcal{A}(AP)_{sat})$ is bounded by δ' (Lemma 8), an $\mathcal{A}(AP)_{sat}$-neighbourhood of radius 3^m around r points has at most $r.\delta'^{3^{m+1}}$ elements. Thus there are at most $\prod_{P \in \mathcal{A}(AP)_{sat}} 2^{k^{ar_P}}$ non $\mathcal{A}(AP)_{sat}$-isomorphic k-elements sets. That concludes the picture of the proof of Theorem 7.

Notice that Theorem 7 only considers injective deterministic automatic presentations. Using Corollary 4.3 of [8] it is easy to see that an automatic presentation AP which is non-deterministic and not injective can be transformed into a deterministic injective presentation AP' such that $\|AP'\| \leq 2^{\|AP\|^c}$ for some constant c. Notice that the bound on the index of the E^r_m relations in Lemma 11 only depends exponentially on the size of the automatic presentation and it depends exponentially on its degree (which is bounded by a double exponential for a non-injective structure, see Proposition 6). Therefore we can obtain a deterministic automaton representing solutions of a formula φ in the structure $\mathcal{A}(AP')$ (which is isomorphic to $\mathcal{A}(AP)$) in triple exponential time. Therefore we obtain the following corollary improving the 3EXPSPACE upper bound of [11]. Moreover, we get easily in 3EXPTIME a non-deterministic automaton representing solutions in the structure $\mathcal{A}(AP)$.

▶ **Corollary 12.** *The model-checking problem for automatic presentations of bounded degree is in 3EXPTIME.*

5 Automata construction for Presburger Arithmetic

Presburger Arithmetic (PA) is the first-order theory over $\mathcal{A} = (\mathbb{Z}, +_{/3}, >_{/2})$, the structure over integers with addition and ordering. It was shown decidable [13] using quantifier elimination. Ferrante and Rackoff [5] gave the first definition of an Ehrenfeucht-Fraïssé relation over integers for PA. Büchi showed that PA was automatic [1] and Eisinger [3] showed that when using a suitable presentation based on most-significant digit first complement notation, Ferrante and Rackoff's relations are preserved by appending arbitrary suffixes allowing to obtain an upper bound on the size of the minimal automaton for a formula.

A common encoding of integer vectors is to use a binary representation and 0 (if the number is positive) or 1 (if it is negative) as padding symbols instead of $\diamond$. This leads to a non-injective presentation. Here, we use an injective automatic presentation of PA which is convenient for our purposes based on the binary most-significant digit first with complement notation: the alphabet is $\Sigma = \{0,1\}$ and valid encodings are in the language $D = \{0,1\} \cup 01\{0,1\}^* \cup 10\{0,1\}^*$. We denote by μ the isomorphism from elements of D to $\mathbb{Z}$. We have $\mu(0) = 0$, $\mu(1) = -1$ and $\mu(01w) = 2^{|w|} + \sum_{i=1}^{|w|} 2^{|w|-i} w[i]$, $\mu(10w) = -2^{|w|+1} + \sum_{i=1}^{|w|} 2^{|w|-i} w[i]$. It is easy to construct automata A_D with $L(A_D) = D$ and $A_>$ and A_+ for comparison and addition. Then, we get the injective deterministic automatic presentation for PA, $AP_{Pres} = (\Sigma, \{>, +\}, A_D, A_=, A_>, A_+)$ where $A_=$ accepts the identity relation over D.

The rest of the section is devoted to defining Ehrenfeucht-Fraïssé relations which satisfy the 5 hypotheses of Theorem 5. We first recall the Ehrenfeucht-Fraïssé relations of [3] for tuples of integers. We need to define inductively some families of integers and of sets of integers. Let B_m, B'_m, δ_m such that $B_0 = \{-2,-1,0,1,2\}$, $\delta_m = \operatorname{lcm} B_m$, $B'_m = \{\delta_m v/v' \mid v, v' \in B_m, v' \neq 0\}$ and $B_{m+1} = B_m \cup \{v + v' \mid v, v' \in B'_m\}$. Eisinger [3] defines an Ehrenfeucht-Fraïssé relation over tuples of integers inspired by Ferrante and Rackoff [5] as follows:

▶ **Definition 13.** ([3], Definition 1) For two k-tuples of integers $\bar{u}_k$ and $\bar{v}_k$ we define the equivalence relation F^r_m as $\bar{u}_k F^r_m \bar{v}_k$ iff for any i, $u_i \equiv v_i \mod \delta^2_m$ and for all $a_1, \ldots, a_r \in B_m$, and for all $c \in \mathbb{Z}$, with $|c| \leq (r+1)\delta^2_m$, $\sum_{i=1}^r a_i u_i + c \geq 0$ iff $\sum_{i=1}^r a_i v_i + c \geq 0$.

We adapt these relations (over integers) to relations over words of $\hat{\Sigma}^*_r$. This adaptation is slightly more involved than in [3] due to the presence of the padding symbol $\diamond$. Furthermore we have to distinguish convolutions of words according to which of their components can be ϵ or not. We partition $\hat{\Sigma}^*_r$ in three disjoint subsets: V_r the set of words that are convolution of words in $D \cup \{\epsilon\}$, S_r the set of words w that are convolution of words in Σ^* such that there is an i with $w\Downarrow_i \notin D \cup \{\epsilon\}$ and I_r the set of words that aren't convolutions of words of Σ^*. We further partition V_r and S_r into languages indexed by subsets of $[1,r]$: let $K \subseteq [1,r]$, we define $V_{r,K} = \{w \in V_r \mid w\Downarrow_i \neq \epsilon \text{ iff } i \in K\}$ and $S_{r,K} = \{w \in S_r \mid w\Downarrow_i \neq \epsilon \text{ iff } i \in K\}$. Clearly $V_r = \bigcup_{K \subseteq [1,r]} V_{r,K}$ and $S_r = \bigcup_{K \subseteq [1,r]} S_{r,K}$.

▶ **Definition 14.** We define a family of relations over words of $\hat{\Sigma}^*_r$. For $u, v \in \hat{\Sigma}^*_r$, $uE^r_m v$ iff:

- $u, v \in I_r$, or $u, v \in S_{r,K}$ for some $K \subseteq [1,r]$.
- $u, v \in V_{r,K}$ for some K (so if $i \in K$, $u\Downarrow_i$ and $v\Downarrow_i$ are in D and represent integers) and:
  - For all $i \in K$, $\mu(u\Downarrow_i) \equiv \mu(v\Downarrow_i) \mod \delta^2_m$
  - For all $b_1, \ldots, b_r \in B_m$, for all $c \in \mathbb{Z}$, $|c| \leq (r+1)\delta^2_m$, $c + \sum_{i \in K} b_i.\mu(u\Downarrow_i) \geq 0$ iff $c + \sum_{i \in K} b_i.\mu(v\Downarrow_i) \geq 0$

▶ **Lemma 15.** *E^r_m satisfies hypotheses 1 to 5 of Theorem 5, with $f(m+r) = 2^{2^{2^{c(m+r)}}}$, for some fixed c.*

Each hypothesis is proved similarly to the corresponding one of [3]. Thus, we have defined Ehrenfeucht-Fraïssé relations satisfying the 5 hypotheses of Theorem 5 and we obtain the following corollary.

▶ **Corollary 16.** *The inductive construction of an automaton A_φ representing all solutions of a Presburger Arithmetic formula φ is in 3EXPTIME.*

6 Conclusion and Perspectives

We have given a triple-exponential upper bound on the size of the automaton corresponding to the solutions of a first-order formula over automatic structures of bounded degree. An open problem is to find a matching lower bound. One can easily deduce a double-exponential lower bound from [11] and it might be possibly to adapt their proof of a 2EXPSPACE lower bound for the model-checking problem to obtain a formula and a structure for which the corresponding automaton must be of triple exponential size. Another interesting question is to study how our method can be extended to the case of tree automatic structures of bounded degree [11] as well as for ω-automatic structures.

Acknowledgement. We would like to thank Florian Horn for helpful comments.

References

1 J. Richard Büchi. Weak second-order Arithmetic and Finite Automata. *Zeitschrift fur Mathematische Logik und Grundlagen der Mathematik*, 6:66–92, 1960.

2 Antoine Durand-Gasselin and Peter Habermehl. On the Use of Non-deterministic Automata for Presburger Arithmetic. In *CONCUR*, volume 6269 of *LNCS*, pages 373–387. Springer, 2010.

3 Jochen Eisinger. Upper bounds on the automata size for integer and mixed real and integer linear arithmetic. In *CSL*, volume 5213 of *LNCS*, pages 431–445. Springer, 2008.

4 Calvin C. Elgot. Decision problems of finite automata design and related arithmetics. *Trans. Amer. Math. Soc.*, 98:21–51, 1961.

5 Jeanne Ferrante and Charles Weill Rackoff. *The computational complexity of logical theories*, volume 718 of *Lecture Notes in Mathematics*. Springer-Verlag, 1979.

6 Haim Gaifman. On local and non-local properties. In *Proc. of the Herbrand Symposium*, volume 107 of *Studies in Logic and the Foundations of Mathematics*, pages 105–135. Elsevier, 1982.

7 Bernard R. Hodgson. On direct products of automaton decidable theories. *Theoretical Computer Science*, 19(3):331–335, 1982.

8 Bakhadyr Khoussainov and Anil Nerode. Automatic presentations of structures. In *Logical and Computational Complexity*, volume 960 of *LNCS*, pages 367–392. Springer, 1994.

9 Felix Klaedtke. Bounds on the Automata Size for Presburger Arithmetic. *ACM Trans. Comput. Logic*, 9(2):1–34, 2008.

10 Felix Klaedtke. Ehrenfeucht-Fraïssé goes automatic for real addition. *Inf. Comput.*, 208(11):1283–1295, 2010.

11 Dietrich Kuske and Markus Lohrey. Automatic structures of bounded degree revisited. *J. Symb. Log.*, 76(4):1352–1380, 2011.

12 Richard E. Ladner. Application of model theoretic games to discrete linear orders and finite automata. *Information and Control*, 33(4):281–303, 1977.

13 Mojżesz Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du Premier Congres des Mathématiciens des Pays Slaves*, pages 92–101, 1929.

A Appendix

A.1 Proof of Lemma 8

Assume by contradiction that $x \in \Sigma^*$ is in relation (in $\mathcal{A}(AP)_{sat}$) with $1 + \delta \sum_{P \in \mathcal{S}}((|Q_P| - 1)ar_P^2)$ distinct elements. Then one of the $\sum_{P \in \mathcal{S}}(|Q_P| - 1)$ relations defined from the $(A_P)_{P \in \mathcal{S}}$, namely $P_{P',q}$, lets x be in relation with more than $\delta ar_{P'}^2$ distinct values, and we can find $j, j'(j \neq j')$ such that there are at least $1 + \delta$ distinct words in Σ^* (namely $y_1, \ldots, y_{\delta+1}$) such that $P_{P',q}$ holds with such a word in the j'-th position and x in the j-th position. Now, let's consider a tuple of words $\bar{u}_{ar_{P'}} \in (\Sigma^*)^{ar_{P'}}$ with x at the j-th position and y_k (for some $k \in [1, \delta+1]$) in the j'-th position such that $P_{P',q}$ holds in $\mathcal{A}(AP)_{sat}$. Then since there is a path from q to the final state in $A_{P'}$, we can find a word $w \in \hat{\Sigma}^*_{ar_{P'}}$ such that the convolution of $u_1(w \Downarrow_1), \ldots, u_{ar_{P'}}(w \Downarrow_{ar_{P'}})$ reaches a final state in $A_{P'}$. Therefore in $\mathcal{A}(AP)$, $[x(w \Downarrow_j)]$ is in relation with $[y_k(w \Downarrow_{j'})]$ for any k, $1 \leq k \leq \delta + 1$. As the $(y_k)_{1 \leq k \leq \delta+1}$ are all different, and AP is injective, the $[y_k(w \Downarrow_{j'})]$ are all distinct, and $[x(w \Downarrow_j)]$ is in relation with $1 + \delta$ distinct elements in $\mathcal{A}(AP)$ which contradicts the boundedness of the degree of $G(\mathcal{A}(AP))$ by δ. Hence x cannot be in relation with $\delta' + 1$ distinct elements, thus $\mathcal{A}(AP)_{sat}$ has degree bounded by δ'.

A.2 Proof of Theorem 7

Here we give the full proof of Theorem 7. It is done by showing that the equivalence relations E^r_m given in Definition 10 satisfy the hypotheses of Theorem 5. It is clear that they satisfy hypothesis 1.

A.2.1 Hypothesis 2

▶ **Lemma 17.** *Let uE^r_0v. If u is a convolution of r words in $L(A_D)$ then so is v and the r-tuples represented by u and v satisfy the same atomic formulas (in the structure $\mathcal{A}(AP)_{sat}$).*

Proof. If u is a convolution of words of $L(A_D)$, then u (and hence v) is a convolution of words in Σ^*, thus there exists a $\mathcal{A}(AP)_{sat}$-isomorphism ξ such that $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u \Downarrow_r}, 0) \overset{\xi}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{v \Downarrow_r}, 0)$, with $\xi(u \Downarrow_i) = \xi(v \Downarrow_i)$. For any i, $1 \leq i \leq r$, $u \Downarrow_i$ reaches a final state (namely q_i) of A_D, this means that the predicate P_{D,q_i} holds for $u \Downarrow_i$, and therefore P_{D,q_i} holds for $\xi(u \Downarrow_i) = v \Downarrow_i$ so v is a convolution of words of $L(A_D)$. Let us now consider an atomic formula $\varphi = P(x_{j_1}, \ldots, x_{j_{ar_P}})$, with $1 \leq j_k \leq r$, for $1 \leq k \leq ar_P$. If $\mathcal{A}(AP) \vDash \varphi([u \Downarrow_1], \ldots, [u \Downarrow_r])$, then $\langle u \Downarrow_{j_1}, \ldots, u \Downarrow_{j_{ar_P}} \rangle$ reaches a final state (namely q_f) in A_P. That means that P_{P,q_f} holds for $(u \Downarrow_{j_1}, \ldots, u \Downarrow_{j_{ar_P}})$, and so P_{P,q_f} holds for $(\xi(u \Downarrow_{j_1}), \ldots, \xi(u \Downarrow_{j_{ar_P}})) = (v \Downarrow_{j_1}, \ldots, v \Downarrow_{j_{ar_P}})$ as well. So $\langle v \Downarrow_{j_1}, \ldots, v \Downarrow_{j_{ar_P}} \rangle$ reaches q_f in A_P, thus $\mathcal{A} \vDash \varphi([v \Downarrow_1], \ldots, [v \Downarrow_r])$. Therefore the r-tuples represented by u and v satisfy the same atomic formulas. ◀

A.2.2 Hypothesis 3

▶ **Lemma 18.** *If u is a convolution of words in Σ^* and $uE^r_{m+1}v$, then for any $u_{r+1} \in \Sigma^*$, there exists $v_{r+1} \in \Sigma^*$ such that $\langle \overline{u \Downarrow_r}, u_{r+1} \rangle E^{r+1}_m \langle \overline{v \Downarrow_r}, v_{r+1} \rangle$.*

Proof. Let $uE^r_{m+1}v$. Then $u, v \in V_r$. We denote ξ the $\mathcal{A}(AP)_{sat}$-isomorphism between the $\mathcal{A}(AP)_{sat}$-neighbourhoods of radius $(3^{m+1} - 1)/2$ around $\overline{u \Downarrow_r}$ and $\overline{v \Downarrow_r}$. Let $u_{r+1} \in \Sigma^*$, we exhibit a suitable v_{r+1} and define an isomorphism ξ' between the new neighbourhoods. We need to distinguish 3 cases:

- If $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(u_{r+1}, u\Downarrow_i) \leq 3^m$ (u_{r+1} is close to other components), we choose $v_{r+1} = \xi(u_{r+1})$. In this case $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2) \subset \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^{m+1}-1)/2)$, so $\mathcal{N}^{r+1}_{\mathcal{A}(AP)_{sat}}((\overline{u\Downarrow}_r, u_{r+1}), (3^m-1)/2) \subset \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^{m+1}-1)/2)$, therefore we can define $\xi' = \xi|_{\mathcal{N}^{r+1}_{\mathcal{A}(AP)_{sat}}((\overline{u\Downarrow}_r, u_{r+1}), (3^m-1)/2)}$. ξ' is an $\mathcal{A}(AP)_{sat}$-isomorphism, so $\mathcal{N}^{r+1}_{\mathcal{A}(AP)_{sat}}((\overline{u\Downarrow}_r, u_{r+1}), (3^m-1)/2) \overset{\xi'}{\simeq}_{\mathcal{A}(AP)_{sat}} (\overline{(v\Downarrow}_r, v_{r+1}), (3^m-1)/2)$. As $\xi'(u\Downarrow_i) = v\Downarrow_i$ for $1 \leq i \leq r$, and $\xi'(u_{r+1}) = v_{r+1}$, we have $\langle\overline{u\Downarrow}_r, u_{r+1}\rangle E^{r+1}_m \langle\overline{v\Downarrow}_r, v_{r+1}\rangle$.
- If $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(u_{r+1}, u\Downarrow_i) > 3^m$ and $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(u_{r+1}, v\Downarrow_i) > 3^m$ (u_{r+1} is far from the other components), we take $v_{r+1} = u_{r+1}$. Clearly $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2) \cap \mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2) = \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{v\Downarrow}_r, (3^m-1)/2) \cap \mathcal{S}_{\mathcal{A}(AP)_{sat}}(v_{r+1}, (3^m-1)/2) = \emptyset$, thus we can define a bijection ξ' from $\mathcal{N}^{r+1}_{\mathcal{A}(AP)_{sat}}((\overline{u\Downarrow}_r, u_{r+1}), (3^m-1)/2)$ to $\mathcal{N}^{r+1}_{\mathcal{A}(AP)_{sat}}((\overline{v\Downarrow}_r, v_{r+1}), (3^m-1)/2)$, as ξ over $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2)$ and the identity over $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2)$. We have to show that ξ' is an $\mathcal{A}(AP)_{sat}$-isomorphism. Assume that a predicate P of $\mathcal{A}(AP)_{sat}$ holds for $\bar{a}_{ar_P}$, then either all the a_i are in $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2)$, or in $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2)$, as they can not be in both, since the distance between these sets is at least 2. Therefore ξ' is an $\mathcal{A}(AP)_{sat}$-isomorphism, so $\langle\overline{u\Downarrow}_r, u_{r+1}\rangle E^{r+1}_m \langle\overline{v\Downarrow}_r, v_{r+1}\rangle$.
- Finally, if $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(u_{r+1}, u\Downarrow_i) > 3^m$ and $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(u_{r+1}, v\Downarrow_i) \leq 3^m$. Clearly u_{r+1} is in the domain of ξ^{-1}, so we can define $v^{(1)} = \xi^{-1}(u_{r+1})$. While $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(v^{(n)}, v\Downarrow_i) \leq 3^m$, (thus $v^{(n)}$ is in the domain of ξ^{-1}) we define $v^{(n+1)} = \xi^{-1}(v^{(n)})$. Let us show that there is always a n such that $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(v^{(n)}, v\Downarrow_i) > 3^m$. First we show that for any n, $u_{r+1} \neq v^{(n)}$. As there is a i such that $d_{\mathcal{A}(AP)_{sat}}(v^{(n)}, v\Downarrow_i) \leq 3^m$ and $v^{(n)}$, $v\Downarrow_i$ and the shortest path from $v\Downarrow_i$ to $v^{(n)}$ are in the domain of ξ^{-1}, we have $d_{\mathcal{A}(AP)_{sat}}(v^{(n+1)}, u\Downarrow_i) \leq 3^m$, which is not the case for u_{r+1}, thus clearly $u_{r+1} \neq v^{(n)}$. As ξ^{-1} is a bijection, it should be clear that all the $v^{(n)}$ are pairwise distinct. Since spheres of finite radius are finite, $v^{(n)}$ can only take finitely many values.
  Thus $(v^{(n)})_n$ is a finite sequence, let us denote n_c the greatest n such that $v^{(n)}$ is defined, we take $v_{r+1} = v^{(n_c)}$. By definition $\min_{i\leq r} d_{\mathcal{A}(AP)_{sat}}(v_{r+1}, v\Downarrow_i) > 3^m$, so $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2) \cap \mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2) = \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{v\Downarrow}_r, (3^m-1)/2) \cap \mathcal{S}_{\mathcal{A}(AP)_{sat}}(v_{r+1}, (3^m-1)/2) = \emptyset$. Therefore we can define the bijection ξ' as ξ over $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2)$ and as ξ^{-n_c} over $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2)$ (it is easy to see that ξ^{-n_c} is defined over $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2)$ and that its image by ξ^{-n_c} is $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(v_{r+1}, (3^m-1)/2)$). ξ' is a bijection and it is also an isomorphism as the distance between $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2)$ (respectively $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{v\Downarrow}_r, (3^m-1)/2)$) and $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(u_{r+1}, (3^m-1)/2)$ (respectively $\mathcal{S}_{\mathcal{A}(AP)_{sat}}(v_{r+1}, (3^m-1)/2)$) is greater than 2. Thus we conclude that $\langle\overline{u\Downarrow}_r, u_{r+1}\rangle E^{r+1}_m \langle\overline{v\Downarrow}_r, v_{r+1}\rangle$.

◀

A.2.3 Hypothesis 4

▶ **Lemma 19.** *Let $uE^r_m v$ for $u, v \in \hat{\Sigma}^*_r$. For any word w in $\hat{\Sigma}^*_r$, $uwE^r_m vw$.*

Proof. Let $uE^r_m v$. First assume $u \in I_r$, then $v \in I_r$ and for all $w \in \hat{\Sigma}_r$, $uw, vw \in I_r$. Hence $uwE^r_m vw$. Now, assume $u = \epsilon$ then $v = \epsilon$. Hence $uw = vw$ and $uwE^r_m vw$. Now, assume $u \in V_r\backslash\{\epsilon\}$. Let us show that for all $w \in \hat{\Sigma}_r$, $uw \in I_r$ implies $vw \in I_r$. As u and v belong to $V_r\backslash\{\epsilon\}$, this means that $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m-1)/2) \overset{\xi}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{v\Downarrow}_r, (3^m-1)/2)$ for some ξ such that $\xi(u\Downarrow_i) = v\Downarrow_i$. Thanks to the empty-word predicate of $\mathcal{A}(AP)_{sat}$, this implies that $u\Downarrow_i = \epsilon$ iff $v\Downarrow_i = \epsilon$. uw in I_r implies there is a i such that $uw\Downarrow_i \notin \Sigma^*$, if $u\Downarrow_i \neq \epsilon$ then $w\Downarrow_i \notin \Sigma^*$, as $v\Downarrow_i \neq \epsilon$, $uw\Downarrow_i \notin \Sigma^*$; if $u\Downarrow_i = \epsilon$, then $v\Downarrow_i = \epsilon$, and $uw\Downarrow_i = vw\Downarrow_i$ so $vw \in I_r$.

The last case is where u, v, uw are non-empty and convolutions of words in Σ^*. This implies that vw is a convolution of words in Σ^* (we have shown that $vw \in I_r$ implies $uw \in I_r$). There is an $\mathcal{A}(AP)_{sat}$-isomorphism ξ such that $\xi(u \Downarrow_i) = v \Downarrow_i$ and $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m - 1)/2) \overset{\xi}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{v\Downarrow}_r, (3^m - 1)/2)$. To show $uwE^r_m vw$ we have to build an isomorphism between neighbourhoods of uw and vw. To build it we will use ξ. We need first some definitions. For any finite word s over a finite alphabet, we denote $\mathrm{pref}_k\, s$ the prefix of size k of s ($\mathrm{pref}_k\, s = s$ if $k \geq |s|$, $\mathrm{pref}_k\, s = \epsilon$ if $k \leq 0$) and $\mathrm{suff}_k\, s$ the suffix of size k of s ($\mathrm{suff}_k\, s = s$ if $k \geq |s|$, $\mathrm{suff}_k\, s = \epsilon$ if $k \leq 0$). For any k, we have $s = \mathrm{pref}_{|s|-k}\, s.\mathrm{suff}_k\, s$. Furthermore, for any n words $s_1, \ldots, s_n$ in Σ^*, we have $\langle \mathrm{suff}_k(s_1), \ldots, \mathrm{suff}_k(s_n)\rangle = \mathrm{suff}_k\langle \bar{s}_n\rangle$, thus $\langle \mathrm{pref}_{|s_1|-k}(s_1), \ldots, \mathrm{pref}_{|s_n|-k}(s_n)\rangle = \mathrm{pref}_{|\langle \bar{s}_n\rangle|-k}\langle \bar{s}_n\rangle$.

In the following we define ξ_w as a partial function from Σ^* to Σ^* : if $\mathrm{pref}_{|x|-|w|}\, x \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, (3^m - 1)/2)$, then $\xi_w(x)$ is defined and $\xi_w(x) = \xi(\mathrm{pref}_{|x|-|w|}\, x).\mathrm{suff}_{|w|}\, x$. Notice that $\xi_w(x) = \epsilon$ iff $x = \epsilon$. Notice also that as ξ is bijective, ξ_w is bijective over its domain of definition.

We prove by recurrence over n (for any $n \leq (3^m - 1)/2$) the following two statements: (1) for any $x \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n)$, $\mathrm{pref}_{|x|-|w|}\, x \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, n)$, (so ξ_w is defined over $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n)$) (2) $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n) \overset{\xi_w}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{vw\Downarrow}_r, n)$.

When $n = 0$ we recall that $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, 0) = (\overline{uw\Downarrow}_r)$. Clearly for any i, we have $\mathrm{pref}_{|uw\Downarrow_i|-|w|}\, uw \Downarrow_i = u \Downarrow_i \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, 0)$. So ξ_w is defined over $(\overline{uw\Downarrow}_r)$ and $\xi_w(uw\Downarrow_i) = vw\Downarrow_i$.

We next show that $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, 0) \overset{\xi_w}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{vw\Downarrow}_r, 0)$. Assume a predicate $P_{P,q}$ of $\mathcal{A}(AP)_{sat}$ (with arity ar_P) holds for $(uw\Downarrow_{j_1}, \ldots, uw\Downarrow_{j_{ar_P}})$ (with $1 \leq j_k \leq r$ for $1 \leq k \leq ar_P$), then the run of $x = \langle uw \Downarrow_{j_1}, \ldots, uw \Downarrow_{j_{ar_P}}\rangle$ in A_P leads to q, this means that $\mathrm{pref}_{|x|-|w|}\, x = \langle u \Downarrow_{j_1}, \ldots, u \Downarrow_{j_{ar_P}}\rangle$ leads to a non sink state (namely q') in A_P; as $(\overline{u\Downarrow}_r) \overset{\xi}{\simeq}_{\mathcal{A}(AP)_{sat}} (\overline{v\Downarrow}_r)$ then $y = \langle v \Downarrow_{j_1}, \ldots, v \Downarrow_{j_{ar_P}}\rangle$ also reaches q' in P. Since A_P is deterministic $(y.\mathrm{suff}_{|w|}\, x) = \langle vw \Downarrow_{j_1}, \ldots, vw \Downarrow_{j_{ar_P}}\rangle$ necessarily reaches q, so $P_{P,q}$ also holds for $(\xi_w(uw \Downarrow_{j_1}), \ldots, \xi_w(uw \Downarrow_{j_{ar_P}}))$. Conversely, assume $P_{P,q}$ does not hold for $(uw \Downarrow_{j_1}, \ldots, uw \Downarrow_{j_{ar_P}})$, then either there exists a q' such that $P_{P,q'}$ holds for $(uw\Downarrow_{j_1}, \ldots, uw\Downarrow_{j_{ar_P}})$, then $P_{P,q'}$ holds for $(vw\Downarrow_{j_1}, \ldots, vw\Downarrow_{j_{ar_P}})$, and hence $P_{P,q}$ does not hold for $(vw \Downarrow_{j_1}, \ldots, vw \Downarrow_{j_{ar_P}})$; or there exists no q' such that $P_{P,q'}$ holds, which means that $\langle uw \Downarrow_{j_1}, \ldots, uw \Downarrow_{j_{ar_P}}\rangle$ reaches the sink state of A_P, from which we can deduce that $\langle vw \Downarrow_{j_1}, \ldots, vw \Downarrow_{j_{ar_P}}\rangle$ also reaches the sink state of A_P and hence $P_{P,q}$ does not hold for $(vw\Downarrow_{j_1}, \ldots, vw\Downarrow_{j_{ar_P}})$.

Therefore any predicate of $\mathcal{A}(AP)_{sat}$ holds on elements of $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, 0)$ iff their image by ξ_w holds, which concludes the initialisation of our recurrence.

Assume that the two statements hold for some $n < (3^m - 1)/2$, let us show they then hold for $n + 1$.

Let $x \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n + 1)$, then there is a predicate $P_{P,q}$ of $\mathcal{A}(AP)_{sat}$ (with arity ar_P), and ar_P words $\bar{x}_{ar_P}$ such that there exists a j such that $x = x_j$ and a j' such that $x_{j'} \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n)$, and $P_{P,q}$ holds for $\bar{x}_{ar_P}$ which means that $\langle \bar{x}_{ar_P}\rangle$ reaches q in A_P, from which we can deduce that $\mathrm{pref}_{|\langle \bar{x}_{ar_P}\rangle|-|w|}\langle \bar{x}_{ar_P}\rangle$ reaches another non-sink state in A_P, thus the $\mathrm{pref}_{|x_i|-|w|}\, x\Downarrow_i$ are in relation in $\mathcal{A}(AP)_{sat}$, and as $\mathrm{pref}_{|x_{j'}|-|w|}\, x_{j'} \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, n)$ then $\mathrm{pref}_{|x_j|-|w|}\, x_j \in \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{u\Downarrow}_r, n+1)$. Therefore ξ_w is defined over $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n + 1)$.

If a predicate $P_{P,q}$ of $\mathcal{A}(AP)_{sat}$ holds for $\bar{x}_{ar_P}$ (ar_P elements in $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n+1)$), then it will also hold for their image by ξ_w. Indeed, from the semantics of $P_{P,q}$ we deduce that

$x' = \text{pref}_{|\langle \bar{x}_r \rangle|-w}\langle \bar{x}_r \rangle$ reaches a (non-sink) state q' in A_P, and hence that there is a predicate $P_{P,q'}$ that holds for $\overline{x'\Downarrow}_{ar_P}$. Any $x'\Downarrow_i = \text{pref}_{|x_i|-|w|}\, x_i$ is in $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw}_{ar_P}, n+1)$ so $P_{P,q'}$ also holds for $(\xi(x'\Downarrow_1), \ldots, \xi(x'\Downarrow_{ar_P}))$ thus $\langle \xi_w(x_1), \ldots, \xi_w(x_{ar_P})\rangle = \langle \xi(x'\Downarrow_1), \ldots, \xi(x'\Downarrow_{ar_P})\rangle . \text{suff}_{|w|}\langle \bar{x}_{ar_P}\rangle$ also holds for $P_{P,q}$. Conversely if $P_{P,q}$ does not hold for $\bar{x}_{ar_P}$, it won't hold for its image by ξ_w. Thus $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, n+1) \overset{\xi_w}{\simeq}_{\mathcal{A}(AP)_{sat}} \mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{vw\Downarrow}_r, n+1)$, which concludes our recurrence.

We have explicitly built the $\mathcal{A}(AP)_{sat}$-isomorphism between $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{uw\Downarrow}_r, (3^m-1)/2)$ and $\mathcal{N}^r_{\mathcal{A}(AP)_{sat}}(\overline{vw\Downarrow}_r, (3^m-1)/2)$ which maps any $uw\Downarrow_i$ to $vw\Downarrow_i$, therefore $uwE^r_m vw$, which concludes the proof. ◀

A.2.4 Hypothesis 5: Proof of Lemma 11

As the degree of $G(\mathcal{A}(AP)_{sat})$ is bounded by δ', it is clear that a $\mathcal{A}(AP)_{sat}$-sphere of radius $(3^m-1)/2$ has at most $V(m) = \frac{\delta'^{\frac{3^m+1}{2}}-1}{\delta'-1}$ elements, thus a $\mathcal{A}(AP)_{sat}$-neighbourhood of radius $(3^m-1)/2$ around r elements has at most $r.V(m)$ elements.

We now give an upper bound over the number of non $\mathcal{A}(AP)_{sat}$-isomorphic sets of k elements. From a combinatorial point of view, for any predicate P of $\mathcal{A}(AP)_{sat}$ with arity ar_P, we have to distinguish for any ar_P elements of the set whether the relation holds or not. Hence there are at most $D(k) = \prod_{P\in\mathcal{S}'} 2^{k^{ar_P}}$ non-isomorphic k-elements sets. As the number of predicates of $\mathcal{S}'$ is bounded by the number of states in all automata in AP, and by definition $ar_P \leq ar_M$, we have $D(k) \leq 2^{\|AP\|.k^{ar_M}}$.

We also need to determine which element of the set is a component from which the neighbourhood is obtained, thus we multiply by k^r. The number of distinct $\mathcal{A}(AP)_{sat}$-neighbourhoods of radius around r $(3^m-1)/2$ elements is thus bounded by $\sum_{k=1}^{r.V(m)} k^r.D(k)$.

The total number of equivalence classes of E^r_m is two (the "empty-word" equivalence class, and the equivalence class for I_r) more than this sum. We get :

$$idx(E^r_m) \leq 2 + \sum_{k=1}^{r.V(m)} k^r.D(k)$$

If $m \geq 1$ we have $idx(E^r_m) \leq r^r.V(m)^r.D(r.V(m))$. Then, by replacing D we have $idx(E^r_m) \leq r^r.V(m).2^{\|AP\|.(r.V(m))^{ar_m}}$. For the sake of readability, we apply $\log_2$:

$$\log_2(idx(E^r_m) \leq r.(\log_2(r) + \log_2(V(m))) + \|AP\|.r^{ar_M}.V(m)^{ar_M}$$

$V(m) = \frac{\delta'^{\frac{3^m+1}{2}}-1}{\delta'-1} \leq \frac{\delta'^{\frac{3^m}{2}}\sqrt{\delta'}}{\delta'-1}$, when δ' is larger than 3, $\delta'-1 \geq \sqrt{\delta'}$, thus $V(m) \leq \sqrt{\delta'}^{3^m}$. We know that $\delta' \leq \delta \sum_{P\in\mathcal{S}}(|Q_P|-1)ar_P^2$, so $\delta' \leq \delta.ar_M^2.\|AP\|$. Thus $V(m) \leq (\delta.ar_M.\|AP\|)^{3^m}$. We replace V :

$$\log_2(idx(E^r_m)) \leq r.(\log_2(r) + 3^m \log_2(\delta.ar_M.\|AP\|)) + \|AP\|.r^{ar_M}.(\delta.ar_M.\|AP\|)^{ar_M.3^m}$$

As a sum is smaller than a product,

$$\log_2(idx(E^r_m)) \leq r.(\log_2(r)3^m \log_2(\delta.ar_M).\log_2(\|AP\|))) + \|AP\|.r^{ar_M}.(\delta.ar_M.\|AP\|)^{ar_M.3^m}$$

As $\log_2(x)$ is smaller than x,

$$\log_2(idx(E^r_m)) \leq r^2.\|AP\|.3^m.\log_2(\delta.ar_M) + \|AP\|.r^{ar_M}.(\delta.ar_M.\|AP\|)^{ar_M.3^m}$$

$$\log_2(idx(E^r_m)) \leq r^2.\|AP\|.(\delta.ar_M)^{3^m} + \|AP\|.r^{ar_M}.(\delta.ar_M.\|AP\|)^{ar_M.3^m}$$

If we assume $ar_M \geq 2$, we have

$$\log_2(idx(E_m^r)) \leq r^{ar_M}.\|AP\|.((\delta.ar_M)^{3^m} + (\delta.ar_M.\|AP\|)^{ar_M.3^m})$$

$$\log_2(idx(E_m^r)) \leq r^{ar_M}.\|AP\|.(\delta.ar_M.\|AP\|)^{(ar_M+1).3^m}$$

To further improve readability, we apply another $\log_2$:

$$\log_2(\log_2(idx(E_m^r))) \leq ar_M \log_2(r) + \log_2(\|AP\|) + (ar_M+1).3^m.\log_2(\delta.ar_M.\|AP\|)$$

The sum of three terms is smaller than three times a lower bound of the terms, hence

$$\log_2(\log_2(idx(E_m^r))) \leq 3.(ar_M+1).3^m.log_2(\delta.ar_M.\|AP\|).\log_2(r)$$

A product of $\log_2$ is greater than a $\log_2$ of products, therefore

$$\log_2(\log_2(idx(E_m^r))) \leq 3.(ar_M+1).3^m.\log_2(\delta).\log_2(ar_M).\log_2(\|AP\|).\log_2(r)$$

Since $(ar_M+1).\log_2(ar_M) \leq 2.ar_M^2$,

$$\log_2(\log_2(idx(E_m^r))) \leq 6.ar_M^2.3^m.\log_2(\delta).\log_2(\|AP\|).\log_2(r)$$

We keep improving readability:

$$\log_2(\log_2(\log_2(E_m^r))) \leq (m+2).\log_2(3)+2\log_2(ar_M)+\log_2(\log_2(\delta))+\log_2(\log_2\|AP\|)+\log_2(\log_2(r))$$

We conclude and bound the index of E_m^r by $f(m+r) = 2^{2^{3^{m+r+c_3.\|AP\|+2}}}$. Clearly $ar_M \leq \|AP\|$ (so $\log_2(ar_M) \leq \|AP\|$); according to Proposition 6, $\delta \leq 2^{\|AP\|^c}$ for some c, thus $\log_2(\log_2(\delta)) \leq \log_2(c) + \log_2(\|AP\|) \leq c'.\|AP\|$ for some c'; $\log_2(\log_2(\|AP\|)) \leq \|AP\|$ and finally $\log_2(\log_2(r)) \leq r.\log_2(3)$. Therefore we have the desired result that the index of E_m^r is bounded by $f(m+r)$, for some fixed constant c_3 which does not depend on AP.

A.3 Proof of Lemma 15

We recall here the 5 hypotheses we have to prove for E_m^r.

1. Words that are not convolutions of words in Σ^* are alone in a same E_m^r equivalence class. ϵ is alone in its E_m^r equivalence class.
2. Let uE_0^rv. If u is a convolution of words in $L(A_D)$ then so is v and the r-tuples presented by u and v satisfy the same atomic formulas.
3. If uE_{m+1}^rv, and u is a convolution of words in Σ^*, then for all $u_{r+1} \in \Sigma^*$, there is a $v_{r+1} \in \Sigma^*$ such that $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle E_m^{r+1} \langle \overline{v\Downarrow}_r, v_{r+1}\rangle$.
4. The index of E_m^r is bounded by $2^{2^{2^{c(m+r)}}}$ for some fixed c.
5. For any $u, v \in \hat{\Sigma}_r^*$ if uE_m^rv, then for any $w \in \hat{\Sigma}_r^*$, uwE_m^ruw

By definition of E_m^r, hypothesis 1 holds, as for any m, words of $\hat{\Sigma}_r^*$ that are not a convolution of words in Σ^* (that is words in I_r) are alone in a same E_m^r equivalence class and ϵ is the only element of $V_{r,\emptyset}$ and hence is alone in its E_m^r equivalence class.

A.3.1 Hypothesis 2

Let $uE_0^r v$, with u a convolution of r words in D, then $u \in V_{r,[1,r]}$ thus $v \in V_{r,[1,r]}$ i.e. v is also a convolution of r words in D.

Up to relabelling there are 7 distinct atomic formulas in the structure of Presburger Arithmetic: $+(x,y,z)$, $+(x,x,y)$, $+(x,y,x)$, $+(x,y,y)$, $+(x,x,x)$, $>(x,y)$, $>(x,x)$. Each of them is equivalent to a conjunction of statements over the positiveness of some linear combinations, with coefficients in B_0. For example, since $uE_0^r v$ we know that $\mu(u\Downarrow_i) + \mu(u\Downarrow_j) - \mu(u\Downarrow_k) \geq 0$ iff $\mu(v\Downarrow_i) + \mu(v\Downarrow_j) - \mu(v\Downarrow_k) \geq 0$ and $-\mu(u\Downarrow_i) - \mu(u\Downarrow_j) + \mu(u\Downarrow_k) \geq 0$ iff $-\mu(v\Downarrow_i) - \mu(v\Downarrow_j) + \mu(v\Downarrow_k) \geq 0$, hence $\mu(u\Downarrow_i) + \mu(u\Downarrow_j) = \mu(u\Downarrow_k)$ iff $\mu(v\Downarrow_i) + \mu(v\Downarrow_j) = \mu(v\Downarrow_k)$. Therefore we can deduce from the E_0^r equivalence of u and v that they satisfy the same atomic formulas.

A.3.2 Hypothesis 3

Let $uE_m^r v$ with $u \notin I_r$, we will prove this lemma with a careful case analysis.

Assume $u \in S_{r,P}$ for some P, there is a $i \in P$ such that $u\Downarrow_i \notin D \cup \{\epsilon\}$, hence for any word u_{r+1}, $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle \in S_{r+1,P\cup\{r+1\}}$. As $u \in S_{r,P}$, $v \in S_{r,P}$ so there is a $i' \in P$ such that $v\Downarrow_i \notin D \cup \{\epsilon\}$, hence $\langle \overline{v\Downarrow}_r, u_{r+1}\rangle \in S_{r+1,P\cup\{r+1\}}$. Then take $v_{r+1} = u_{r+1}$, and we have $\langle \overline{u\Downarrow}_r, u_{r+1}, \rangle E_m^{r+1} \langle \overline{v\Downarrow}_r, v_{r+1}\rangle$.

Assume $u \in V_{r,P}$, for some P, and $u_{r+1} \notin D \cup \{\epsilon\}$, then $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle \in S_{r+1,P\cup\{r+1\}}$. Then take $v_{r+1} = u_{r+1}$, so $\langle \overline{v\Downarrow}_r, v_{r+1}\rangle \in S_{r+1,P\cup\{r+1\}}$, hence $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle E_m^{r+1} \langle \overline{v\Downarrow}_r, v_{r+1}\rangle$.

Assume $u \in V_{r,P}$, for some P, and $u_{r+1} = \epsilon$, then $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle \in V_{r+1,P}$. Take $v_{r+1} = \epsilon$, then (as $v \in V_{r,P}$) $\langle \overline{v\Downarrow}_r, v_{r+1}\rangle \in V_{r+1,P}$. Also as $uE_{m+1}^r v$, for all $b_1, \ldots, b_r \in B_{m+1}$, for all $c \in \mathbb{Z}$, $|c| \leq (r+1)\delta_{m+1}^2$, $c + \sum_{i\in P} b_i.\mu(u\Downarrow_i) \geq 0$ iff $c + \sum_{i\in P} b_i.\mu(v\Downarrow_i) \geq 0$. As $\delta_{m+1} > 2\delta_m$ and $B_m \subset B_{m+1}$ and $r+1 \notin P$, for all $b_1, \ldots, b_{r+1} \in B_m$, for all $c \in \mathbb{Z}$, $|c| \leq (r+2)\delta_m^2$, $c + \sum_{i\in P} b_i.\mu(\langle \overline{u\Downarrow}_r, u_{r+1}\rangle \Downarrow_i) \geq 0$ iff $c + \sum_{i\in P} b_i.\mu(\langle \overline{v\Downarrow}_r, v_{r+1}\rangle \Downarrow_i) \geq 0$. Thus $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle E_m^{r+1} \langle \overline{v\Downarrow}_r, v_{r+1}\rangle$.

Finally, let's assume $u \in V_{r,P}$, for some P, and $u_{r+1} \in D$ (then $v \in V_{r,P}$). Let us define $\bar{x}_r \in \mathbb{Z}^r$ (resp. $\bar{y}_r$) as: $x_i = \mu(u\Downarrow_i)$ (resp. $y_i = \mu(v\Downarrow_i)$) if $i \in P$, and $x_i = 0$ (resp. $y_i = 0$) if $i \notin P$. It should be clear that $\bar{x}_r F_{m+1}^r \bar{y}_r$, hence according to lemma 2 in [3], we can find $y_{r+1} \in \mathbb{Z}$ such that $(\bar{x}_r, u_{r+1}) F_m^{r+1} (\bar{y}_r, y_{r+1})$. Take v_{r+1} the presentation of that y_{r+1}. As both $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle$ and $\langle \overline{v\Downarrow}_r, v_{r+1}\rangle$ are in $V_{r+1,P\cup\{r+1\}}$ and $(\bar{x}_r, \mu(u_{r+1})) F_m^{r+1} (\bar{y}_r, \mu(v_{r+1}))$, we have that $\langle \overline{u\Downarrow}_r, u_{r+1}\rangle E_m^{r+1} \langle \overline{v\Downarrow}_r, v_{r+1}\rangle$.

A.3.3 Hypothesis 4

According to Lemma 4 in [3] the index of F_m^r is bounded by $2^{2^{2^{c'(m+r)}}}$ for some c'. Hence the number of equivalence classes within $V_{r,[1,r]}$ is bounded by $2^{2^{2^{c(m+r)}}}$. The number of equivalence classes within each $V_{r,P}$ is also bounded by $2^{2^{2^{c(m+r)}}}$, hence the number of E_m^r equivalence classes is bounded by $1 + 2^r + 2^r 2^{2^{2^{c'(m+r)}}}$, thus it is bounded by $2^{2^{2^{c(m+r)}}}$ for some c.

A.3.4 Hypothesis 5

We prove this lemma by case analysis.

Assume $u \in I_r$ (so $v \in I_r$) then clearly $uw \in I_r$ (and $vw \in I_r$), so $uwE_m^r vw$.

Assume $u \in S_{r,K}$ for some K (so $v \in S_{r,K}$), and $uw \in I_r$, then there is a i such that $uw\Downarrow_i \notin \Sigma^*$. If $i \notin K$ this implies $w\Downarrow_i \notin \Sigma^*$, and thus $vw\Downarrow_i \notin \Sigma^*$, so $vw \in I_r$; if $i \in K$ this implies $w\downarrow_i \notin \Sigma^*$, so $vw\Downarrow_i \notin \Sigma^*$ and hence $vw \in I_r$. So $uwE^r_m vw$.

Assume $u \in S_{r,K}$ for some K (so $v \in S_{r,K}$), and $uw \notin I_r$, this implies $uw \in S_{r,K'}$ for some $K' \supset K$. Notice that for any $i \notin K'$, $w\Downarrow_i = \epsilon$, so $vw\Downarrow_i = \epsilon$; for any $i \in K'\backslash K$, $w\Downarrow_i \in \Sigma^+$, so $vw\Downarrow_i \in \Sigma^+$; and for any $i \in K$, $w\downarrow_i \in \Sigma^+$, so $vw\Downarrow_i \in \Sigma^+$, therefore vw is either in $S_{r,K'}$ or $V_{r,K'}$. As $v \in S_{r,K}$, there is a i such that $v\Downarrow_i \in \Sigma^+\backslash D$ so $vw\Downarrow_i \notin D$, therefore $vw \in V_{r,K'}$, so $uwE^r_m vw$.

Assume $u \in V_{r,K}$ for some K (so $v \in V_{r,K}$) and $uw \in I_r$, this means that there is a i such that $uw\Downarrow_i \notin \Sigma^*$. If $u\Downarrow_i = \epsilon$ (then $v\Downarrow_i = \epsilon$) this means that $uw\Downarrow_i = vw\Downarrow_i$ thus vw is also in I_r; if $u\Downarrow_i \neq \epsilon$ (then also $v\Downarrow_i \neq \epsilon$) this implies $w\downarrow_i \notin \Sigma^*$, thus $vw\Downarrow_i \notin \Sigma^*$, i.e. $vw \in I_r$. So if $uw \in I_r$, $vw \in I_r$ and thus $uwE^r_m vw$.

Assume that $u \in V_{r,K}$ for some K and $uw \in S_{r,K'}$ for some $K' \supset K$, as we showed before, this implies that vw is in $V_{r,K'}$ or $S_{r,K'}$. As $uw \in S_{r,K'}$, there is a $i \in K'$ such that $uw\Downarrow_i \in \Sigma^+\backslash D$. If $u\Downarrow_i = \epsilon$ then $w\Downarrow_i \in \Sigma^+\backslash D$, as $v\Downarrow_i = \epsilon$, we have $vw\Downarrow_i \in \Sigma^+\backslash D$ so $vw \in S_{r,K'}$; if $u\Downarrow_i = 1$ (resp. 0), then $v\Downarrow_i = 1$ (resp. 0) because $\mu(u\Downarrow_i) = \mu(v\Downarrow_i) = -1$ (resp. 0), so $w\downarrow_i$ starts with 1 (resp. 0), so $vw\Downarrow_i \in \Sigma^+\backslash D$. Remark $|u\Downarrow_i|$ can't be larger than 1 otherwise either $u \in S_r$ or $uw \in V_r$. Thus uw and vw are in $S_{r,K'}$, so $uwE^r_m vw$.

The last case left is when $u \in V_{r,K}$ for some K and $uw \in V_{r,K'}$ for some $K' \supset K$. In a similar manner as in the previous case, we show that $vw \in V_{r,K'}$. Let us define the r-tuples of integers $\overline{x}_r$, $\overline{x'}_r$, $\overline{y}_r$ and $\overline{y'}_r$ as follows: for i in K, $x_i = \mu(u\Downarrow_i)$, $y_i = \mu(v\Downarrow_i)$, for $i \notin K$, $x_i = y_i = 0$; for i in K', $x'_i = \mu(uw\Downarrow_i)$, $y'_i = \mu(vw\Downarrow_i)$, for $i \notin K'$, $x'_i = y'_i = 0$. One can notice that for any i, $2^{|w|}.x_i - x'_i = 2^{|w|}.y_i - y'_i$ and $|2^{|w|}.x_i - x'_i| \leq 2^{|w|-1}$. Hence for $i \in K'$, $\mu(uw\Downarrow_i) = \mu(vw\Downarrow_i)$.

Let $b_1, \ldots, b_r \in B_m$, and assume that for any $|c| \leq (r+1)\delta_m^2$, $\sum_i b_i.x_i + c > 0$, this means that both $\sum_i b_i.x_i$ and $\sum_i b_i.y_i$ are strictly greater than $(r+1)\delta_m^2$. As all the b_i are smaller than δ_m we also have $|\sum_i b_i.(2^{|w|}.x_i - x'_i)| = |\sum_i b_i.(2^{|w|}.x_i - x'_i)| \leq r.\delta_m.2^{|w|-1}$. So by triangle inequality we have $\sum_i b_i.x'_i > 2^{|w|-1}(r+1)\delta_m^2$ and $\sum_i b_i.x'_i > 2^{|w|-1}(r+1)\delta_m$. So for any c, $|c| \leq (r+1)\delta_m^2$, $\sum_i b_i.x'_i + c \geq 0$ and $\sum_i b_i.y'_i + c \geq 0$.

Let $b_1, \ldots, b_r \in B_m$, and assume that there exists any $|c| \leq (r+1)\delta_m^2$ such that $\sum_i b_i.x_i + c = 0$, then $\sum_i b_i.y_i + c$. From that we clearly deduce that $\sum_i b_i.x'_i = \sum_i b_i.y'_i$, so for any c, $|c| \leq (r+1)\delta_m^2$, $\sum_i b_i.x'_i + c \geq 0$ iff $\sum_i b_i.y'_i + c \geq 0$.

We therefore deduce that for any $b_1, \ldots, b_r \in B_m$, and for any $|c| \leq (r+1)\delta_m^2$, $\sum_i b_i.x'_i + c \geq 0$ iff $\sum_i b_i.y'_i + c \geq 0$.

We can finally conclude that $uwE^r_m vw$.