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

Arthur MILCHIOR

IRIF, Université Paris Diderot, France
LACL, UPEC, Créteil, France

22 juin 2016

Logique : histoire rapide et simplifiée

Hilbert 1900, 10ème problème Soit [un problème]. Trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra décider si [il existe une solution].

Logique : histoire rapide et simplifiée

Hilbert 1900, 10ème problème Soit [un problème]. Trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra décider si [il existe une solution].

Gödel 1931, théorème d'incomplétude Formalisation des mathématiques. Cela permet de montrer qu'il existe des énoncés mathématiques dont on ne peut ni prouver qu'ils sont vrais, ni qu'ils sont faux.

Logique : histoire rapide et simplifiée

Hilbert 1900, 10ème problème Soit [un problème]. Trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra décider si [il existe une solution].

Gödel 1931, théorème d'incomplétude Formalisation des mathématiques. Cela permet de montrer qu'il existe des énoncés mathématiques dont on ne peut ni prouver qu'ils sont vrais, ni qu'ils sont faux.

Turing, Church, 1936 Description de ce qui est calculable (i.e. qui admet une méthode, au moyen d'un nombre fini d'opérations). Preuve que certains problèmes n'admettent aucune telle méthode.

Logique : histoire rapide et simplifiée

Hilbert 1900, 10ème problème Soit [un problème]. Trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra décider si [il existe une solution].

Gödel 1931, théorème d'incomplétude Formalisation des mathématiques. Cela permet de montrer qu'il existe des énoncés mathématiques dont on ne peut ni prouver qu'ils sont vrais, ni qu'ils sont faux.

Turing, Church, 1936 Description de ce qui est calculable (i.e. qui admet une méthode, au moyen d'un nombre fini d'opérations). Preuve que certains problèmes n'admettent aucune telle méthode.

Matiassevitch 70 Le 10ème problème de Hilbert n'admet aucune méthode.

Plan

Langages et logiques
- Définissabilité
- Satisfiabilité finie

Spectres

Relations d'entiers et logiques

Logique et automates

Logique sur les mots

$$\phi := \exists m.\ m \times 2 = \text{fin} \wedge \forall y.P_b(y) \iff y = m$$

"Il existe ($\exists$) un nombre m (représentant le milieu) tel que $2m$ soit la fin du mot et toutes ($\forall$) les lettres en position y sont des b si et seulement si ($\iff$) $y = m$."

Non satisfait par :

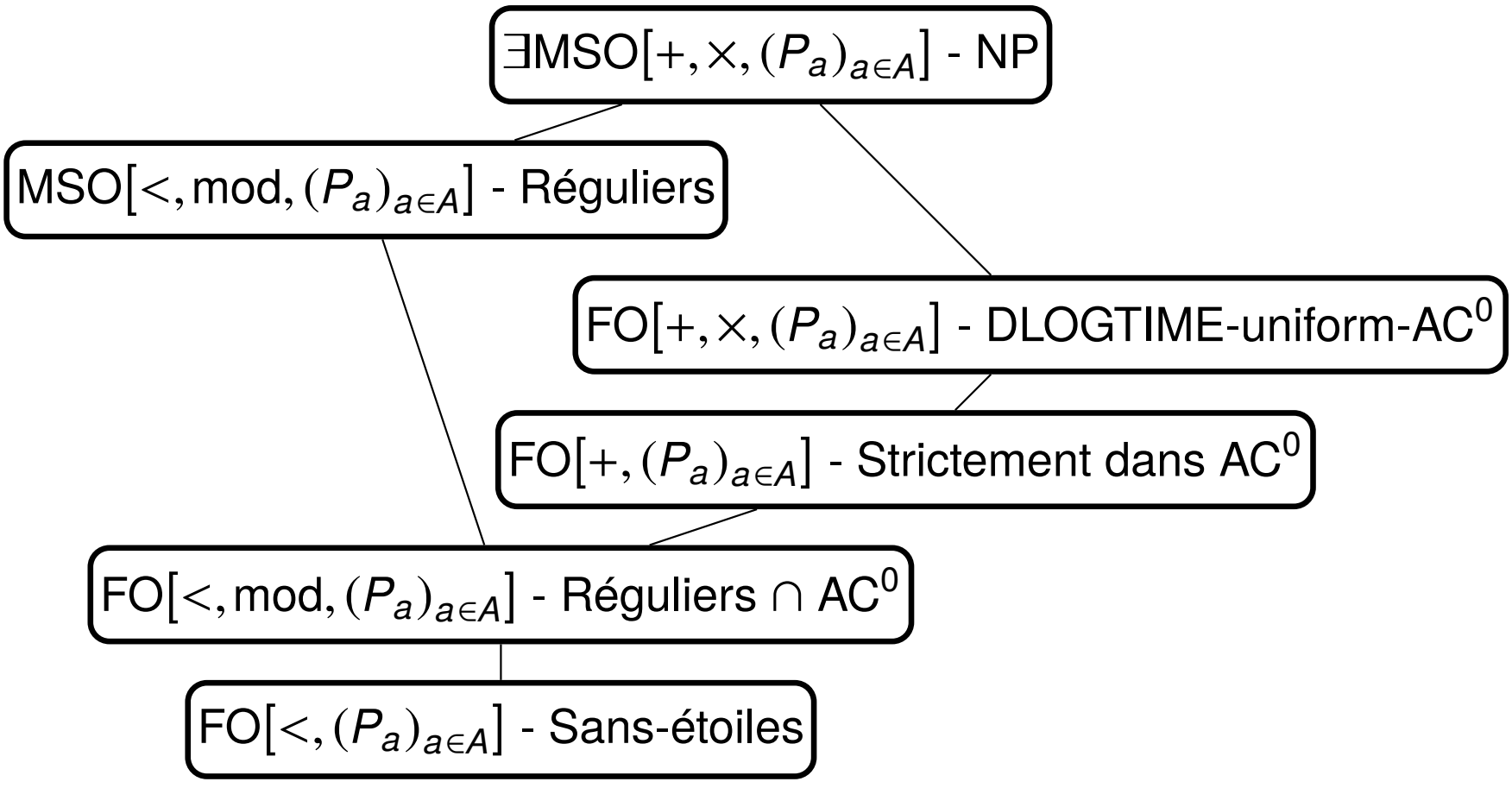
a	a	a	a
0	1	2	3

Satisfait par :

a	a	b	a	a
0	1	2	3	4
		m		

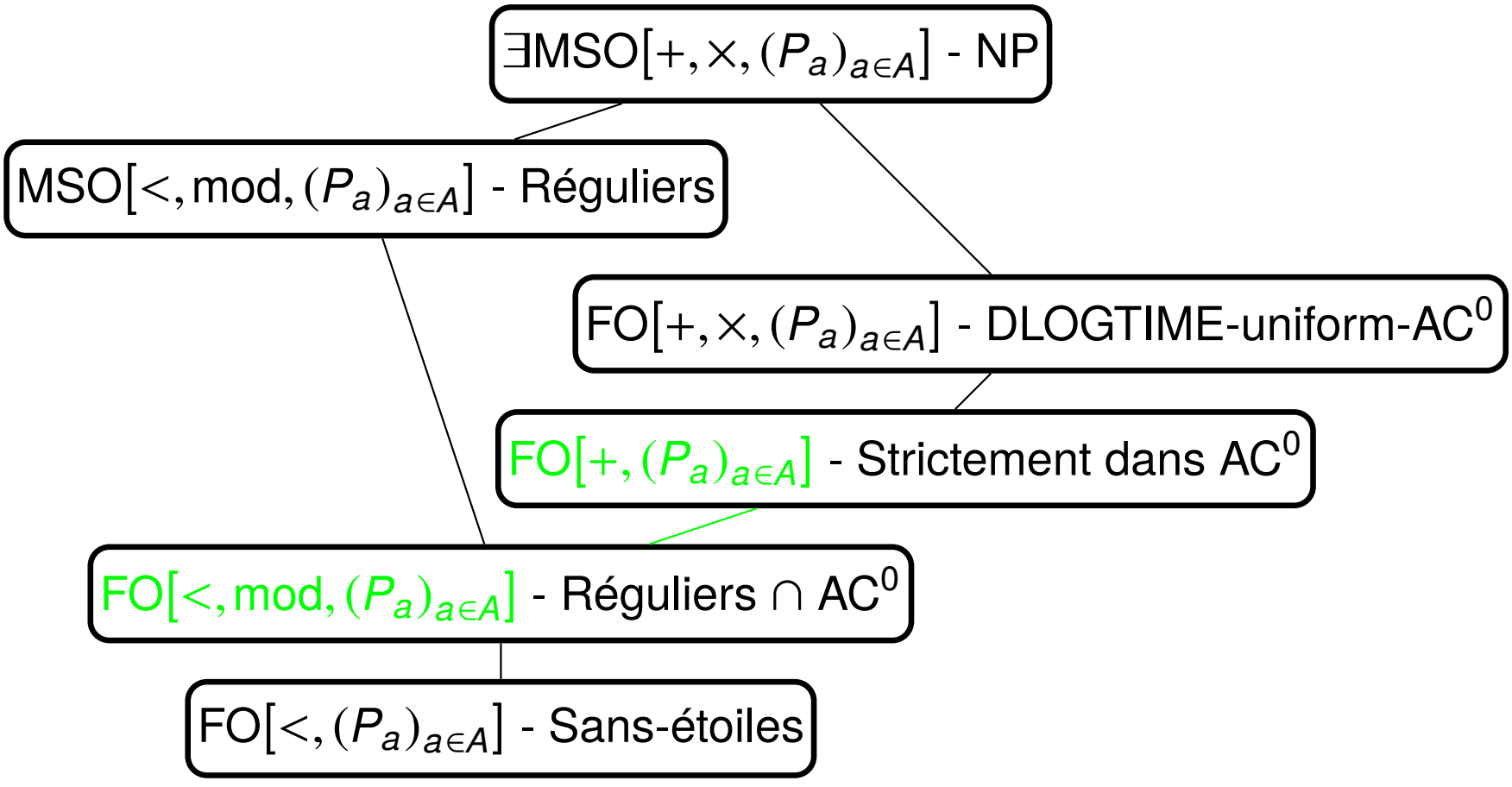
Le mot *aabaa* satisfait cette formule. La formule est donc *satisfiable*.

Logiques et classes de langages



Logiques et classes de langages

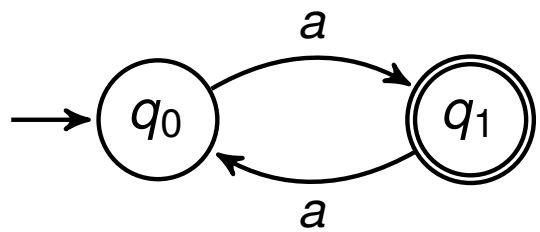
Logiques considérées dans cette thèse



Caractérisation

Théorème (Büchi 60)

Les langages réguliers sont exactement les langages $\mathrm{MSO}[<, \mathrm{mod}, (P_a)_{a\in A}]$*-définissables.*



$a(aa)^*$ - $\exists P \subseteq \mathbb{N}.\ \{0 \in P \wedge \forall n.\ [n \in P \iff \neg(n+1) \in P] \wedge \mathrm{fin} \in P\}$

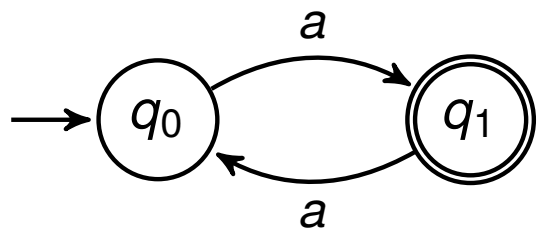
Régulier au delà de FO[<, mod]

Quelle relation R peut on rajouter pour que $\mathrm{FO}[<, \mathrm{mod}, R, (P_a)_{a\in A}]$ ne définisse que des réguliers ?

Caractérisation

Théorème (Büchi 60)

Les langages réguliers sont exactement les langages $\mathrm{MSO}[<, \mathrm{mod}, (P_a)_{a\in A}]$*-définissables.*



$a(aa)^*$ - $\exists P \subseteq \mathbb{N}.\ \{0 \in P \wedge \forall n.\ [n \in P \iff \neg(n+1) \in P] \wedge \mathrm{fin} \in P\}$

Théorème (Péladeau 1992)

La classe $\mathcal{R}$ *des relations* $\mathrm{FO}[<, \mathrm{mod}]$*-définissables est maximale telle que* $\mathrm{FO}[\mathcal{R}, (P_a)_{a\in A}]$ *ne définisse que des langages réguliers.*

Résultats concernant la satisfiabilité

Théorème

La satisfiabilité de	*est*	
$\mathrm{FO}[+, (P_a)_{a\in A}]$	*indécidable*	*(Lange 2004)*
$\mathrm{FO}[<, \times 2, (P_a)_{a\in A}]$	*?*	
$\mathrm{FO}[<, \mathrm{mod}, (P_a)_{a\in A}]$	*decidable*	*(Büchi 1960)*

Théorème

La satisfiabilité (finie) de $\mathrm{FO}[+1, f(n)]$ *avec* $f : \mathbb{N} \to \mathbb{N}$ *non-interprétée (existentiellement quantifiée) est indécidable.*

Résultats concernant la satisfiabilité

Théorème

La satisfiabilité de	*est*	
$\mathrm{FO}[+, (P_a)_{a\in A}]$	*indécidable*	*(Lange 2004)*
$\mathrm{FO}[<, \times 2, (P_a)_{a\in A}]$	*indécidable*	
$\mathrm{FO}[<, \mathrm{mod}, (P_a)_{a\in A}]$	*decidable*	*(Büchi 1960)*

Théorème

La satisfiabilité (finie) de $\mathrm{FO}[+1, f(n)]$ *avec* $f : \mathbb{N} \to \mathbb{N}$ *non-interprétée (existentiellement quantifiée) est indécidable.*

Théorème

La classe $\mathcal{R}$ *des ensembles* $\mathrm{FO}[<, \mathrm{mod}]$*-définissables est le fragment maximal de* $\mathrm{FO}[+]$ *tel que la satisfiabilité (finie) de* $\mathrm{FO}[<, \mathcal{R}, (P_a)_{a\in A}]$ *est indécidable.*

Plan

Langages et logiques

Spectres

Relations d'entiers et logiques

Logique et automates

Spectres - Introduction

Définition

Le spectre d'une formule est l'ensemble des cardinaux des modèles finis de cette formule.
Le spectre d'un langage est l'ensemble des longueurs des mots.

Exemple

– *Le spectre de* $a(aa)^*$ *est* $2\mathbb{N}+1$.

– *Le spectre de la théorie des corps fini est* $\left\{p^n \mid p \text{ premier}, n \in \mathbb{N}^{>0}\right\}$.

Spectres - Résultats

Théorème

Les ensemble finis ou co-finis sont exactement les spectres de $\mathrm{FO}[+1]$.

Théorème

Les ensembles ultimement périodiques sont exactement les spectres de :

$\mathrm{FO}[+]$	*Conséquence de Presburger 27*
$\mathrm{MSO}[<, \mathrm{mod}, (P_a)_{a\in A}]$	*Conséquence de Büchi 60*
$\mathrm{FO}[f(x)]$ *avec* f *non interprétée*	*Durand, Fagin, Loescher 98*
$\mathrm{MSO}[f(x)]$ *avec* f *non interprétée*	*Gurevich, Shelah 03*

En mélangeant des logiques ?

Et $\mathrm{FO}[+1, f(x)]$? $\mathrm{FO}[+1, \times 2, (P_a)_{a\in A}]$?

Spectres - Résultats

Théorème

Les ensemble finis ou co-finis sont exactement les spectres de $\mathrm{FO}[+1]$.

Théorème

Les ensembles ultimement périodiques sont exactement les spectres de :

$\mathrm{FO}[+]$	*Conséquence de Presburger 27*
$\mathrm{MSO}[<, \mathrm{mod}, (P_a)_{a\in A}]$	*Conséquence de Büchi 60*
$\mathrm{FO}[f(x)]$ *avec* f *non interprétée*	*Durand, Fagin, Loescher 98*
$\mathrm{MSO}[f(x)]$ *avec* f *non interprétée*	*Gurevich, Shelah 03*

Théorème

On peut encoder les temps de calcul d'une machine à 2 compteurs non déterministe dans le spectre d'une $\mathrm{FO}[+1, \times 2, (P_a)_{a\in A}]$*-formule (respectivement, d'une* $\mathrm{FO}[+1, f(x)]$*,* f *non-interpétée).*

Plan

Langages et logiques

Spectres

Relations d'entiers et logiques
- Résultats à la Muchnik
- Résultats à la Michaux-Villemaire

Logique et automates

Élimination des Quantificateurs

Théorème

Les logiques suivantes admettent l'élimination des quantificateurs :

$\mathrm{FO}[+, <, \mathrm{mod}]$, *Presburger 29*

$\mathrm{FO}[\{n \mapsto n + c \mid c \in \mathbb{Z}\}, <, \mathrm{mod}]$. *Conséquence de Presburger 29*

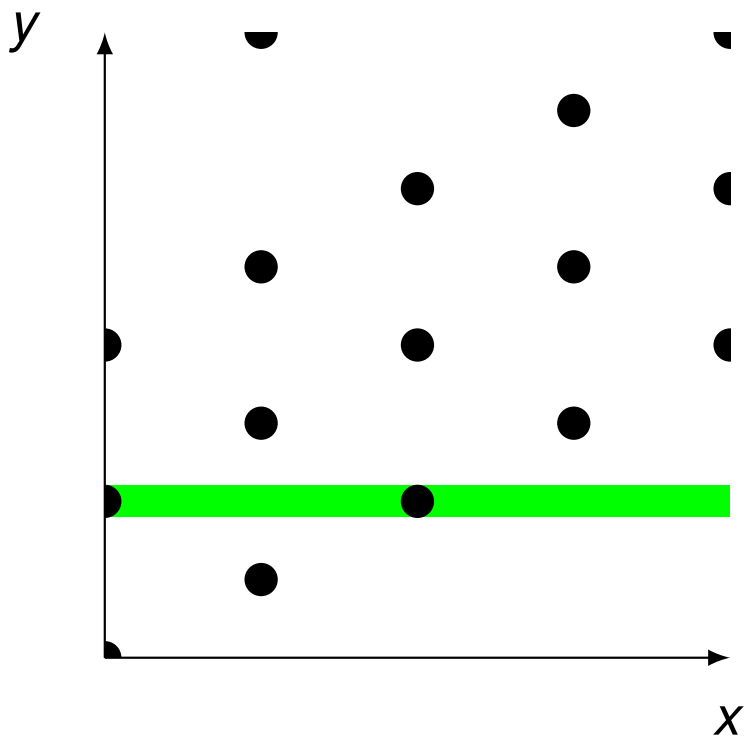
Example

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

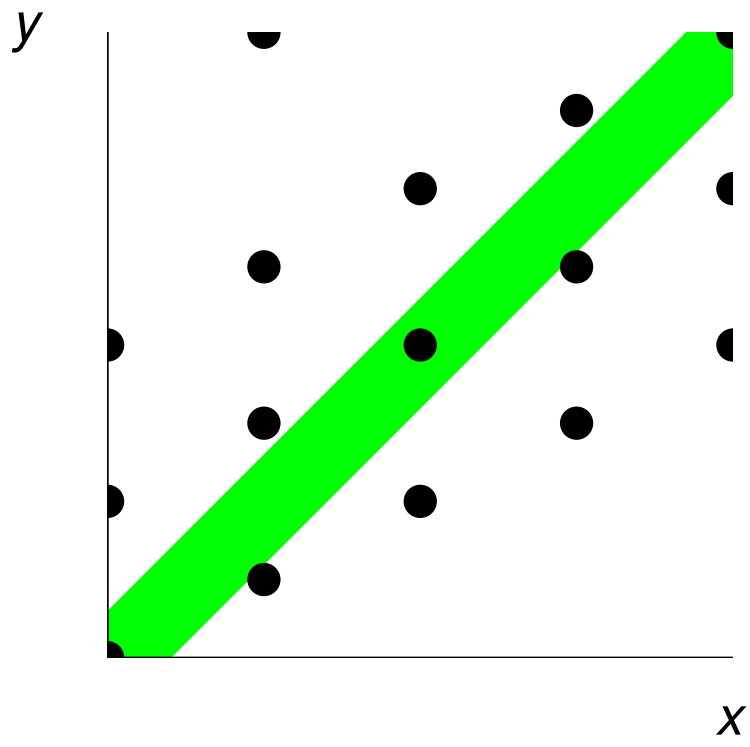
est équivalent à :

$$\bigvee_{i=-2}^{2} \{(\ i = y \wedge\ i = 0) \vee (\ i \leq y - 4 \wedge\ i \equiv 0 \mod 2)\} \vee$$
$$\bigvee_{i=-6}^{2} \{(y+i = y \wedge y+i = 0) \vee (y+i \leq y - 4 \wedge y+i \equiv 0 \mod 2)\}.$$

Sections et diagonales



Section $y = 5$



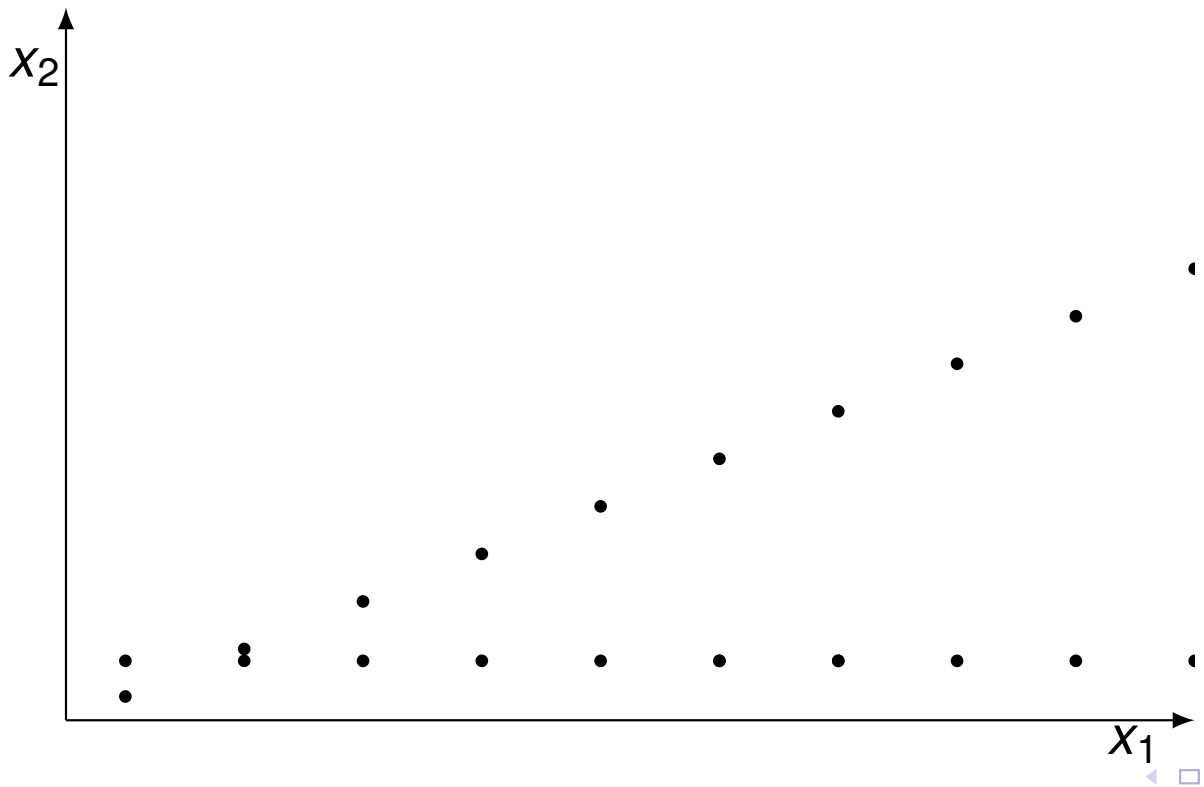
diagonal $x = y$

Caractérisations récursives et locales - $R \subseteq \mathbb{N}^d$

Théorème (Muchnik 91)

(1) *R est* FO[+]*-définissable si et seulement si*

(2) *–chaque section de R est* FO[+]*-définissable,*
–chaque sous-ensemble S borné de R, suffisamment éloigné de 0, est $(p_{1,S}, \ldots, p_{d,S})$-périodique, et les $p_{i,S}$ sont bornés.



Caractérisations récursives et locales - $R \subseteq \mathbb{N}^d$

Théorème (Muchnik 91)

(1) *R est* FO[+]*-définissable si et seulement si*

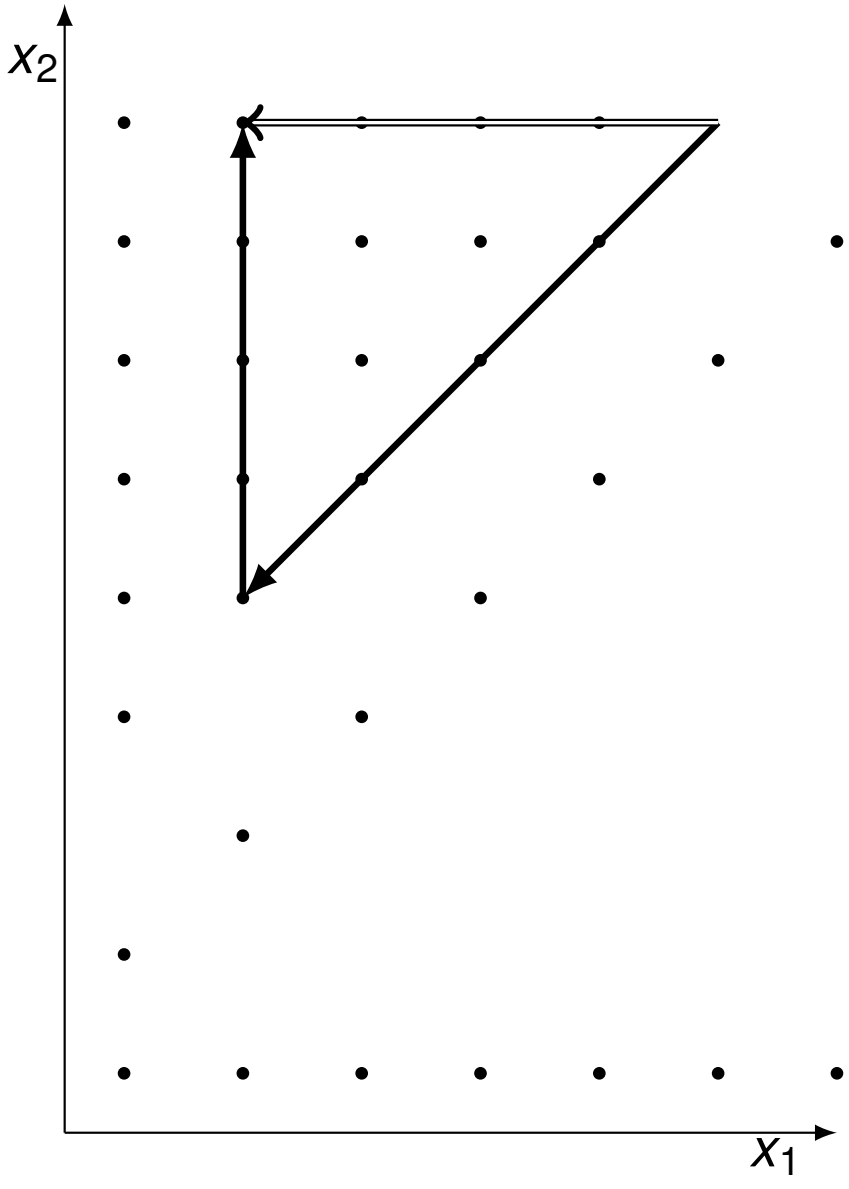
(2) *–chaque section de R est* FO[+]*-définissable,*
–chaque sous-ensemble S borné de R, suffisamment éloigné de 0, est $(p_{1,S},\ldots,p_{d,S})$-périodique, et les $p_{i,S}$ sont bornés.

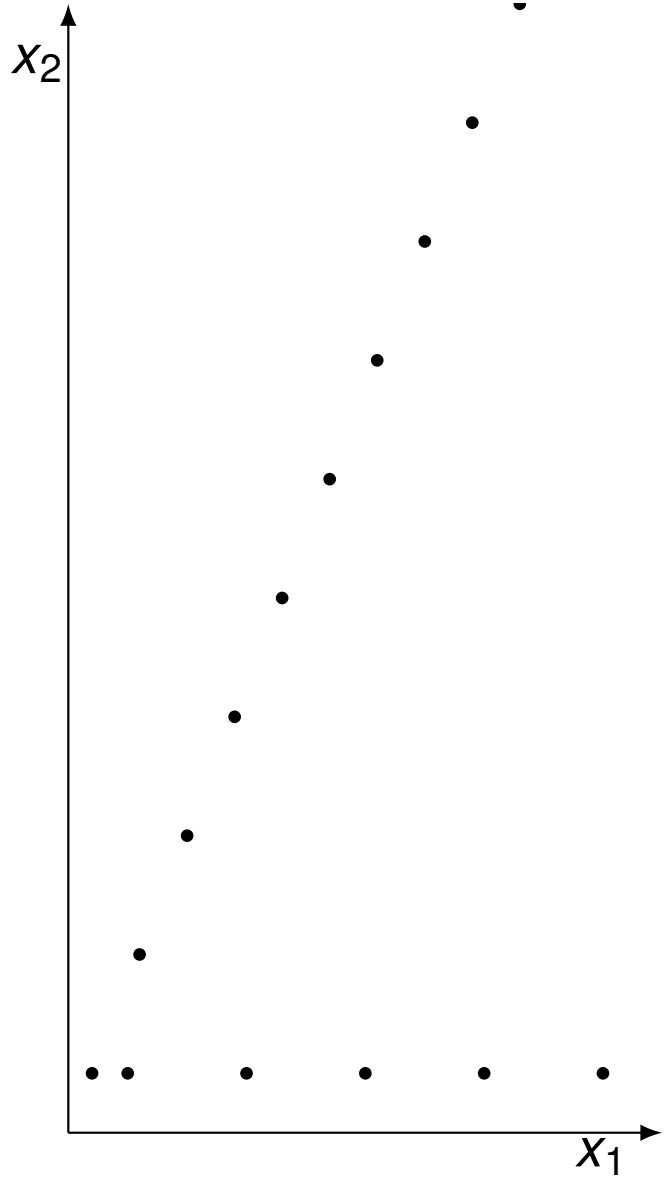
Théorème

(1) *$R \in$ FO$[<, \mathrm{mod}\, m]$, si et seulement si*

(2) *–Chaque section et chaque diagonale de R sont* FO$[<, \mathrm{mod}\, m]$*-définissable et,*
–chaque sous-ensemble borné de R, suffisamment éloigné de 0, est $(m,\ldots,m)$-périodique.

Morceau de preuve de la caractérisation de FO$[<, \mathrm{mod}\, m]$





Réduire la dimension dans FO[+]

Théorème (Michaux-Villemaire 96)

Pour tout $R \subseteq \mathbb{N}^d$ *qui n'est pas* FO[+]*-définissable,*
il existe une FO[+, R]*-formule* $\phi(x)$ *telle que*
l'ensemble d'entiers défini par $\phi(x)$ *n'est pas* FO[+]*-définissable.*

Question algorithmique

Peut on calculer $\phi(x)$ en fonction de R ?

Réduire la dimension dans FO[+]

Théorème (Michaux-Villemaire 96)

Pour tout $R \subseteq \mathbb{N}^d$ *qui n'est pas* FO[+]*-définissable,*
il existe une FO[+, R]*-formule* $\phi(x)$ *telle que*
l'ensemble d'entiers défini par $\phi(x)$ *n'est pas* FO[+]*-définissable.*

Théorème

Il existe une FO[+, R]*-formule* $\phi(x)$ *telle que*
pour tout $R \subseteq \mathbb{N}^d$ *qui n'est pas* FO[+]*-définissable,*
l'ensemble d'entiers défini par $\phi(x)$ *n'est pas* FO[+]*-définissable.*

Réduire la dimension dans FO[<, mod m] et FO[<, mod]

Théorème

Soit $m > 0$. Pour tout $R \subseteq \mathbb{N}^d$ qui n'est pas FO[<, mod m]*-définissable, il existe une* FO[<, R]*-formule $\phi(x)$ telle que l'ensemble d'entiers défini par $\phi(x)$ n'est pas* FO[<, mod m]*-définissable.*

Théorème

Pour tout $R \subseteq \mathbb{N}^d$ qui est FO[+]*-définissable mais qui n'est pas* FO[<, mod]*-définissable, il existe une* FO[<, R]*-formule $\phi(x,y)$ telle que la fonction entière, de la forme $n \mapsto rn + g(n)$ avec $r > 1$ et g bornée, défini par $\phi(x,y)$ n'est pas* FO[<, mod]*-définissable.*

Plan

Langages et logiques

Spectres

Relations d'entiers et logiques

Logique et automates

Résultats connus reliant la logique et les automates

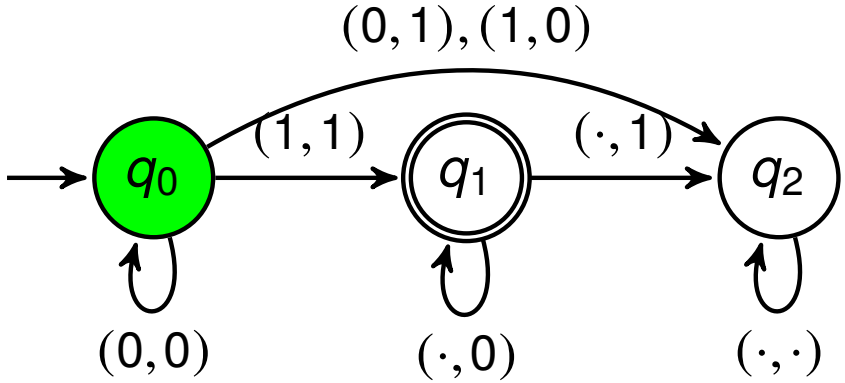
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Résultats connus reliant la logique et les automates

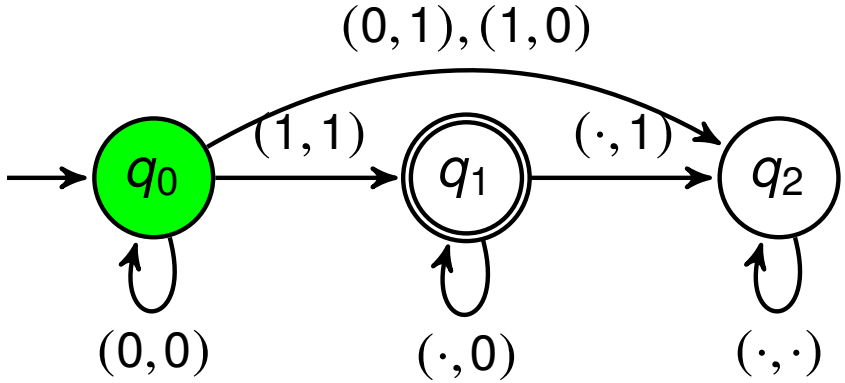
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Résultats connus reliant la logique et les automates

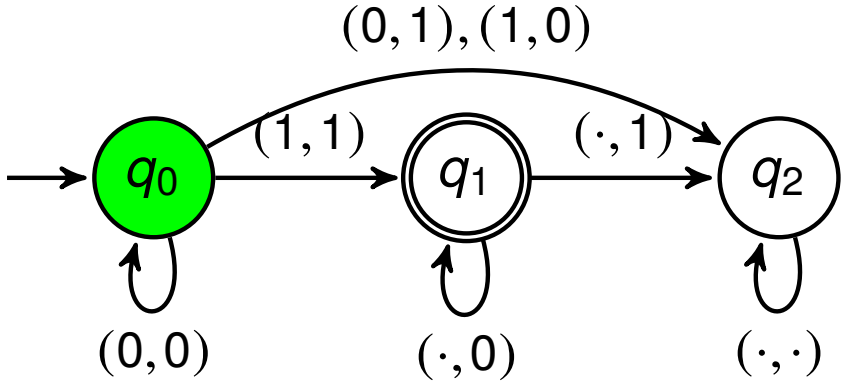
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Résultats connus reliant la logique et les automates

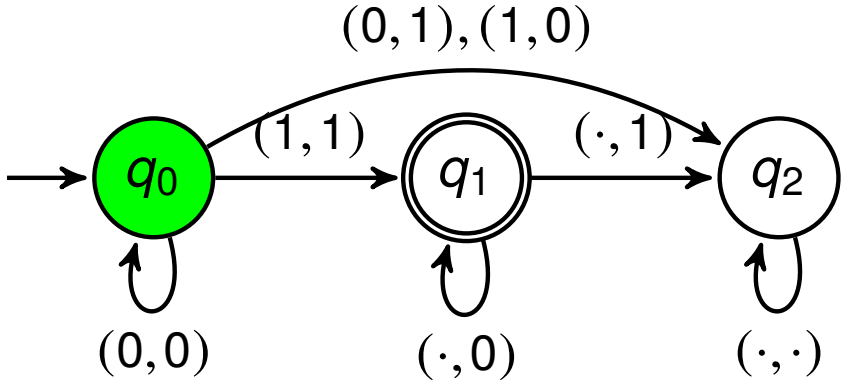
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Résultats connus reliant la logique et les automates

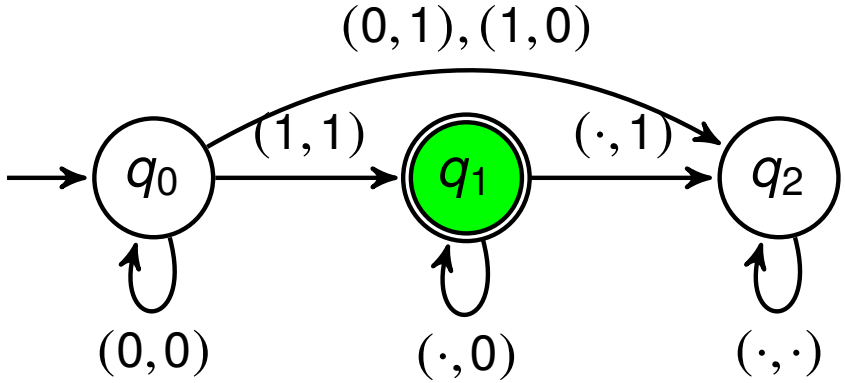
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Résultats connus reliant la logique et les automates

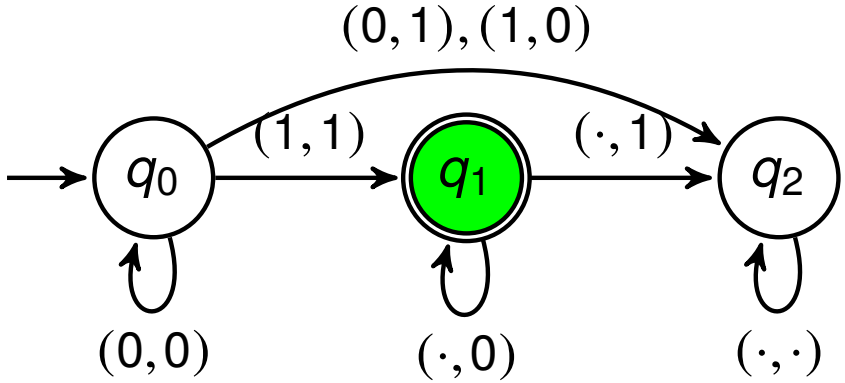
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Résultats connus reliant la logique et les automates

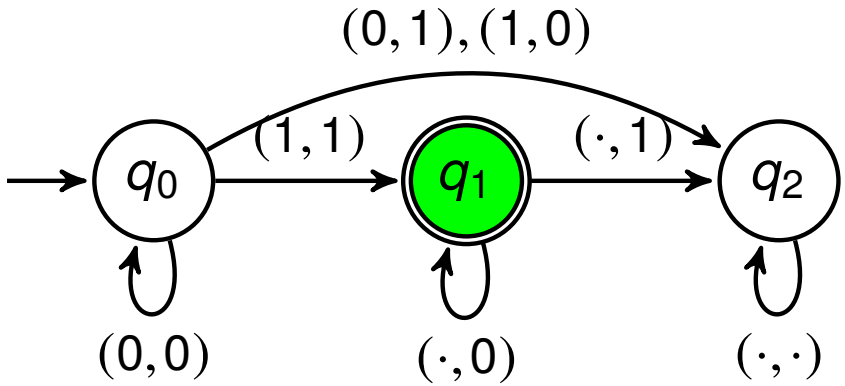
Logique	Automate en base	
FO$[+, V_b]$	$b \geq 2$	Büchi 60, Bruyère 85
FO$[+]$ Rationnel Semilinéaire	tout $b \geq 2$	Cobham 69, Semenov 77 (Michaux-Villemaire 96)
FO$[<, \mathrm{mod}]$	1	Straubing 91

$V_b(n)$ est la plus grande puissance de b qui divise n.

Exemple :

$V_2(000101_2) = 000100_2$.

$11111_1 = 5$



Des automates aux formules

Soit $R \subseteq \mathbb{N}^d$ acceptée par un automate synchrone minimal $\mathcal{A}$ avec n états.

Théorème

On peut décider si R est FO[+]*-définissable.*

Dimension d	*Complexité en temps*	
1		*(Honkala 86)*
toutes	*4EXP*	*(Muchnik 91)*
toutes	*polynomiale*	*(Leroux 05)*
1	*linéaire*	*(Marsault-Sakarovitch 13)*

Et FO[$<$, mod] ?

Des automates aux formules

Soit $R \subseteq \mathbb{N}^d$ acceptée par un automate synchrone minimal $\mathcal{A}$ avec n états.

Théorème

On peut décider si R est FO[+]*-définissable.*

Dimension d	*Complexité en temps*	
1		*(Honkala 86)*
toutes	*4EXP*	*(Muchnik 91)*
toutes	*polynomiale*	*(Leroux 05)*
1	*linéaire*	*(Marsault-Sakarovitch 13)*

Théorème

On peut décider en temps linéaire si R est FO[$<$, mod]*-définissable.*

Théorème

Si R est FO[$<$, mod]*-définissable on peut calculer en temps $O(n^3 \log n)$ une* FO[$<$, mod]*-formule qui définit R.*

Perspectives

Automates

Considérer FO$[<]$.

Considérer les chiffres les plus significatifs en premier.

Considérer les automates lisant des réels.

Caractérisation

Adapter la caractérisation à FO$[+1, \mathrm{mod}]$.

Satisfiabilité

Critères pour la décidabilité de la satisfiabilité de FO$[R, (P_a)_{a \in A}]$ quand R n'est pas FO$[+]$-définissable.

Satisfiabilité

Théorème

La satisfiabilité (finie) de $\mathrm{FO}[+1, g(n), (P_a)_{a \in A}]$ *avec* $g : \mathbb{N} \to \mathbb{N}$ *croissante et* $g(n) - n$ *non borné est indécidable.*

Spectres - b-reconnaissables

Théorème

Les ensembles b-reconnaissable sont des $\mathrm{FO}^2[+1, \times b, (P_a)_{a\in A}]$*-spectre.*

Théorème

Les ensembles b-reconnaissable sont des $\mathrm{FO}[+1, f]$*-spectre, où* $f : \mathbb{N} \to \mathbb{N}$ *est non interprétée.*

Théorème

Il existe une $\mathrm{FO}[+1, f(x)]$*-formule qui définit* $n \mapsto c \uparrow^d n$*, pour tout* $c, d \in \mathbb{N}$.

Avec $a \uparrow^1 b = a^b$ et $a \uparrow^d b = a \uparrow^{d-1} (a \uparrow^{d-1} \ldots a)$, b fois.

Morceau de la preuve

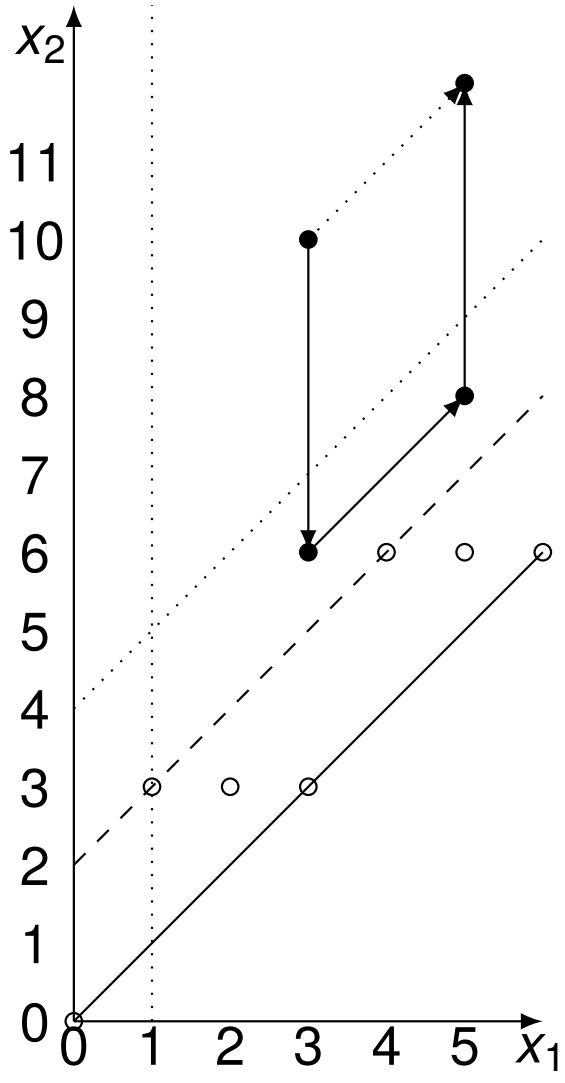
Lemma

Soit $R \subseteq \mathbb{N}^d$ tel que :

–pour tout $(x_1, \ldots, x_d) \in R$, $x_i \leq x_{i+1}$ pour tout $0 < i < d$,

–toutes les sections sont FO$[<, \mathrm{mod}\, m]$*-définissable.*

Soit s_n le seuil de la section $x_1 = n$. La suite $s_n - n$ est bornée si et seulement si R est FO$[<, \mathrm{mod}\, m]$*-définissable.*



Des fonctions aux ensembles

Lemme

Soit $m > 0$ *et* $f : \mathbb{N} \to \mathbb{N}$ *qui n'est pas* $\mathrm{FO}[<, \mathrm{mod}\, m]$*-définissable. On peut* $\mathrm{FO}[<, \mathrm{mod}\, m, f]$*-définir un ensemble d'entier qui n'est* $\mathrm{FO}[<, \mathrm{mod}\, m]$*-définissable.*

Pour $m = 2$:

– Soit $f^{\mathcal{S}}(n) = 4n$. On prend l'image de f.

– Soit $f^{\mathcal{S}}(n) = \left\lfloor \frac{n}{2} \right\rfloor$. On prend l'inverse de $2\mathbb{N}$ par f.

– Soit $f^{\mathcal{S}}(n) = 2\left\lfloor \frac{n}{4} \right\rfloor$. On prend $\{x \in \mathbb{N} \mid f(x) = f(x+2)\} = 4\mathbb{N} \cup (4\mathbb{N} + 1)$.

Lemme

Si $R \subseteq \mathbb{N}$ *est ultimement* m'*-périodique, avec* m' *minimal, alors* $m'\mathbb{N}$ *est* $\mathrm{FO}[<, R]$*-définissable.*

Des fonctions aux ensembles

Lemme

Soit $m > 0$ *et* $f : \mathbb{N} \to \mathbb{N}$ *qui n'est pas* $\mathrm{FO}[<, \mathrm{mod}\, m]$*-définissable. On peut* $\mathrm{FO}\left[<, \mathrm{mod}\, m, f\right]$*-définir un ensemble d'entier qui n'est* $\mathrm{FO}[<, \mathrm{mod}\, m]$*-définissable.*

Pour $m = 2$:

- Soit $f^{\mathcal{S}}(n) = 4n$. On prend l'image de f.
- Soit $f^{\mathcal{S}}(n) = \left\lfloor \frac{n}{2} \right\rfloor$. On prend l'inverse de $2\mathbb{N}$ par f.
- Soit $f^{\mathcal{S}}(n) = 2\left\lfloor \frac{n}{4} \right\rfloor$. On prend $\{x \in \mathbb{N} \mid f(x) = f(x+2)\} = 4\mathbb{N} \cup (4\mathbb{N} + 1)$.

Lemme

Si $R \subseteq \mathbb{N}$ *est ultimement* m'*-périodique, avec* m' *minimal, alors* $m'\mathbb{N}$ *est* $\mathrm{FO}[<, R]$*-définissable.*