# Logique avancée

## 3 - Arithmétique de Presburger

Master Info Nice Sophia Antipolis
E. Lozes

23. avril 2019

# Contenu de la séance

- arithmétique de Presburger
- Mona
- complexité de certains problèmes de décision sur MSO

# Arithmétique de Presburger

## Définition

L'arithmétique de Presburger est la théorie du premier ordre des entiers sur le vocabulaire $\{+, <\}$. Autrement dit, les formules de l'arithmétique de Presburger sont définies par la grammaire suivante

$$\varphi ::= t = t \mid t < t \mid \varphi \wedge \varphi \mid \neg\varphi \mid \exists x.\varphi$$
$$t ::= 0 \mid x \mid t + t$$

où $x$ est une variable du premier ordre.

Une interprétation $I$ associe à chaque variable un entier $I(x)$.

# Exemples

- "$y$ est pair" : $\exists x.y = x + x$
- "$y$ est 1" : $\forall x.x < y \Rightarrow x = 0$
- "$y = r \mod 5$" : $\exists x.r < 5 \wedge y = x + x + x + x + x + r$
- "le système d'équations diophantiennes

$$\begin{aligned} x + y &= 13 \\ x - y &= 1 \end{aligned}$$

admet une solution $\exists x, y.x + y = 13 \wedge x - y = 1$

# Codage d'une interprétation comme un mot

Chaque variable $x$ définit une ligne d'une matrice de 0 et de 1. La ligne de $x$ contient l'entier $I(x)$ écrit sur une ligne en binaire en commençant par le bit de poids faible, et en complétant éventuellement avec des 0 sur les bits de poids forts pour que toutes les lignes fassent la même longueur. Le mot qui code $I$ est la suite des vecteurs colonnes de la matrice ainsi formée.

exemple :
$I(x) = 7 = 0b1101 \qquad I(y) = 1 = 0b0001 \qquad I(z) = 3 = 0b0011$

$x \prec y \prec z$

$$w(\prec, I) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

# Langage d'une formule

$L(\prec, \varphi)$ est l'ensemble des mots codant les interprétations des variables libres de $\varphi$ qui satisfont la formule

$$L(\prec, \phi) = \{w(\prec, I) \mid I \models \phi\}$$

## Théorème

$L(\prec, \phi)$ est régulier.

Preuve : par récurrence sur $\varphi$. Pour les formules $x < y$, $x = n$, et $x = y + z$, on définit un automate qui compare bit à bit le nombre $I(x)$ à $I(y)$ ou $n$ ou la somme bit à bit de $I(y)$ et $I(z)$. Pour les formules $\varphi \vee \psi$ et $\neg\varphi$ on utilise la clôture par union et complément des langages réguliers. Pour $\exists x\varphi$, cela correspond à effacer une ligne dans le codage de l'interprétation, et c'est la clôture par homomorphisme qui donne le résultat.

# Décidabilité de l'arithmétique de Presburger

Le problème de model-checking

- étant donnés $I$, $\phi$
- a-t-on $I \models \phi$ ?

est décidable

Le problème de satisfaisabilité

- étant donné $\phi$
- existe-t-il $I$ telle que $I \models \phi$ ?

est décidable

Le problème de validité

- étant donnée une formule close $\phi$
- $\phi$ appartient-elle à la théorie de l'arithmétique de Presburger ?

est décidable

# Arithmétique de Peano

L'arithmétique de Peano est la théorie du premier ordre des entiers naturels avec le vocabulaire $\{+, \times, <\}$.

Son fragment existentiel correspond aux équations diophantiennes (équations polynomiales sur les entiers).

Le 10ème problème de Hilbert consistait à résoudre les équations diophantiennes.

Youri Matiassevitch, en s'appuyant sur les travaux de Julia Robinson, a démontré qu'il s'agissait d'un problème indécidable.

# Arithmétique de Skolem

L'arithmétique de Skolem est la théorie du premier ordre des entiers naturels avec le vocabulaire $\{\times, =\}$.

L'arithmétique de Skolem est elle aussi décidable et on peut donner une preuve par réduction aux automates d'arbre qui ressemble beaucoup à celle que l'on vient de voir pour l'arithmétique de Presburger

# Entiers et automates

Soit $\varphi$ une formule de l'arithmétique de Presburger avec une variable libre. $L(\varphi)$ est l'ensemble des représentation binaires des entiers qui satisfont la formule, et c'est un langage régulier.

En utilisant les mêmes arguments, on montre que l'ensemble $L_b(\varphi)$ des représentation en base $b > 2$ des entiers qui satisfont $\varphi$ est régulier.

Théorème (Cobham,69)
Soit $S \subseteq \mathbb{N}$ tel que pour deux bases $b_1, b_2 \geq 2$, $b_1$ et $b_2$ premiers entre eux, les langages $L_1(S)$ et $L_2(S)$ des codages de $S$ en bases $b_1$ et $b_2$ sont réguliers.
Alors $S$ est définissable par une formule de l'arithmétique de Presburger

# Questions de complexité

# Quelle est la complexité de wMSO ? de Presburger ?

La complexité de wMSO est *non-élémentaire* : on peut décider si une formule de taille $n$ est valide en un temps proportionnel à une tour d'exponentielles de hauteur $n$.

La complexité de l'arithmétique de Presburger est **2EXPTIME** : on peut décider si une formule de taille $n$ est valide en un temps $\mathcal{O}(2^{2^n})$. Pour atteindre cette complexité, on utilise un algorithme d'élimination des quantificateurs.

# Taille du plus petit modèle

Démomtrer ces résultats supposerait de coder une exécution de machine de Turing en temps borné (et d'avoir suivi un cours de complexité).

On va s'intéresser à un problème très lié, mais plus simple :

**Problème** : étant donnée une formule $\varphi$ de wMSO, quelle est la taille du plus petit modèle de $\varphi$ ?

# Tour d'exponentielle

On note $2_n$ une tour d'exponentielle de taille $n$, autrement dit $2_0 = 1$ et $2_{n+1} = 2^{2_n}$.

On va construire une formule $\varphi$ de taille $n$ telle que le plus petit modèle de $\varphi$ est de taille $\geq 2_{O(n)}$.

Plus précisément on définit une suite de formules $\text{dist}_n(x, y)$ et une fonction $f$ telle que

- $f(n) \geq 2_n$,
- $\text{dist}_n(x, y) \Leftrightarrow y - x = f(n)$, et
- la taille de la formule $\text{dist}_n$ est en $\mathcal{O}(n)$

# Première tentative

$\mathrm{dist}_n(x, y) :=$

$$y - x = \underbrace{1 + 1 + \cdots + 1}_{f(n)}$$

où $\phi(1) := \exists z.\phi(z) \wedge \forall t.(t < z) \Rightarrow \exists u.u < t$

problème : la taille de $\mathrm{dist}_n(x, y)$ est $f(n)$, et non $O(n)$.

# Deuxième tentative

On construit la formule $\phi$ telle que

- $X$ code le début des blocs $B_0, \ldots B_{N-1}$, chacun de longueur $n$
- $x$ est le début du premier bloc $B_0$
- $y$ est le début du dernier bloc $B_{N-1}$
- $Y$ code un nombre entre 0 und $2^n - 1$ sur chaque bloc
- $B_0$ contient 0, $B_{N_1}$ contient $2^n - 1$
- $B_i$ et $B_{i+1}$ contiennent des nombres successifs

Ainsi $N = 2^n$, est la longueur du modèle est $nN = n2^n$

# Construction de $\text{dist}_n$ par récurrence

Supposons $\text{dist}_{n-1}$ déjà défini.

On veut construire $\text{dist}_n$ à l'aide de $\text{dist}_{n-1}$, mais on doit faire attention à

- n'utiliser $\text{dist}_{n-1}$ qu'une seule fois
- n'utiliser qu'un nombre constant (indépendant de $n$) de variables et de connecteurs logiques