L'arithmétique de Presburger est décidable

22 octobre 2011

Théorème 1

Soit la théorie du premier ordre des entiers munis de l'addition. Sa syntaxe est

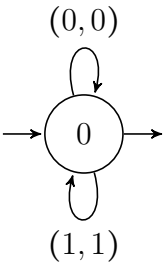
$$\phi, \phi' := (x = y) | (x + y = z) | \phi \vee \phi' | \neg\phi | \exists x \phi$$

Alors pour toute formule close (i.e sans variables libres) ϕ, il est décidable de savoir si ϕ est vraie.

Démonstation : Soit ϕ une formule close.

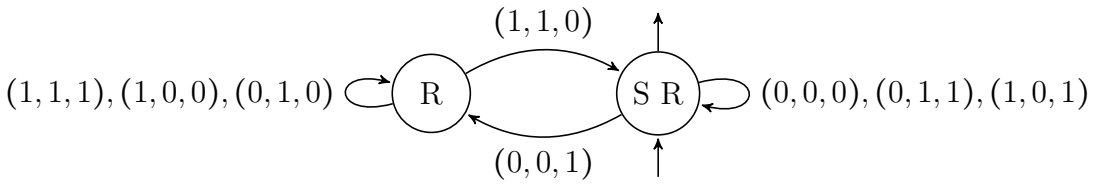
- On admet l'existence de la forme prenexe de ϕ : $\phi = Q_1 x_1 \cdots Q_n x_n \psi$ avec $\forall i, Q_i \in \{\exists, \neg\exists\}$.
- $\forall k \in [|0, n|]$, on pose $\phi_k = Q_{k+1} x_{k+1} \cdots Q_n x_n \psi$ avec $\phi_n = \psi$ et $\phi_0 = \phi$.
- Pour tout k on pose $\Sigma_k = \{0, 1\}^k$. Un mot de longueur m sur cet alphabet sera un m-uplet de k-uplet de bits. On peut donc pour tout k-uplet d'entier $(a_1, \ldots, a_k)$ lui associer son écriture binaire sur Σ_k : $((b_1^m, b_2^m, \ldots, b_k^m), \ldots, (b_1^0, b_2^0, \ldots, b_k^0))$ où $\forall i \geq k, a_i = \sum_{j=1}^{m} b_i^j * 2^j$. On a donc rajouter des 0 à gauche pour que tous les a_i aient la même longueur en écriture binaire.
- Pour $k \in [|0, n|]$, posons $X_k = \{(a_1, \ldots, a_k) \in \mathbb{N}^k | [|\phi_k|]_(a_1, \ldots, a_k) = 1\}$

1. Construisons $\mathcal{A}_n$ tel que $\mathcal{L}(\mathcal{A}) = X_n$: ψ est s'écrit par induction à partir des formules $(1) : x_i = x_j$ et $(2) : x_i + x_j = x_r$ et des opérations $\neg$ et $\vee$. L'automate $\mathcal{A}_{(1)}$ teste l'égalité bit à bit $x_i = x_j$:



où (a, b) = {transitions $(--, a, --, b, --)$, où a est le i-ème bit et b le j-ème}.

L'automate $\mathcal{A}_{(2)}$ teste la somme $x_i + x_j = x_r$ en testant commençant par les bit de plus haut poids :



Les transitions (a, b, c) sont définies de manière analogue que (a, b). L'état R est l'état dit "avec retenue", il est atteint depuis l'état sans retenue SR lorsque le plus grand des trois bit testés est celui de x_r.

Par exemple, si nous testons la somme $3 + 5 = 7$, nous avons $x_1 = 3, x_2 = 4, x_3 = 7$ en écriture binaire, (x_1, x_2, x_3) donne $((0, 0, 1), (1, 1, 1), (1, 0, 1))$. Nous commençons par tester $(0, 0, 1)$, nous allons dans l'état avec retenue car la somme est juste seulement si le dernier bit est issue d'une retenue. Ensuite nous testons $(1, 1, 1)$. Cette somme est vraie s'il y a une retenue ($1 + 1 = 10$, donc 11 s'il y avait une retenue), nous restons donc dans l'état avec retenue. Enfin, dans l'état avec retenue, nous ne pouvons pas avoir $1 + 0 = 1$, la somme formule est donc fausse pour cette valuation.

Maitenant que nous avons $\mathcal{A}_{(1)}$ et $\mathcal{A}_{(2)}$ pour tous les i, j, r, nous savons construire les négations des formules en prenant l'automate complémentaire et nous savons faire les disjonctions de formules en prenant l'union de deux automates. Par induction nous savons construire $\mathcal{A}_n$.

2. Construisons $\mathcal{A}_k$ tel que $\mathcal{L}(\mathcal{A}_k) = X_k$ à partir de $\mathcal{A}_{k+1}$.

$\phi_k = Q_{k+1} x_{k+1} \phi_k$. On peut supposer $\phi_k = \exists \phi_{k+1}$ car sinon $\phi_k =\neq \exists \phi_{k+1}$ et nous savons écrire la négation d'une formule avec les automates.
Nous avons $\mathcal{A}_{k+1} = (Q, \Sigma_{k+1}, \delta_{k+1}, I_{k+1}, F)$, nous posons alors $\mathcal{A}_k = (Q, \Sigma_k, \delta_k, I_k, F)$ avec $\pi_k : \Sigma_{k+1} \to \Sigma_k : (b_1, \ldots, b_{k+1}) \mapsto (b_1, \ldots, b_k)$ de la manière suivante :

$$\forall p, q \in Q, \forall x \in \Sigma_k, si\ \delta_{k+1}(p, a) = q\ alors\ on\ pose\ \delta_k(p, \pi_k(x)) = q$$

$$I_k = I_{k+1} \cup \{\delta_k(i, (0, \ldots, 0)), \forall i \in I_{k+1}\}$$

A_k va deviner le x_{k+1} tel que la formule est vraie, puisqu'à chaque fois nous avons le choix entre donner la valeur 0 ou 1 au $(k+1)$-ième bit. La deuxième partie de l'ensemble I_k sert à prendre en compte que l'entier x_{k+1} à deviner

pourrait être beaucoup plus grand que les autres entiers $(x_1, \ldots, x_k)$ et qu'il va donc falloir rajouter des 0 dans l'écriture binaire de $(x_1, \ldots, x_k, x_{k+1})$.

Dis autrement,

$$\begin{aligned}
(a_1, \ldots, a_m) \in \mathcal{L}(\mathcal{A}_k) \quad &\Leftrightarrow \quad \exists i \xrightarrow{a_1} p_1 \xrightarrow{a_2} \cdots \xrightarrow{am} q \in F \ dans \ \mathcal{A}_k \\
&\Leftrightarrow \quad \exists (b_0, \ldots, b_m) \in \{0,1\}^{m+1} et \ \tilde{i} \in I_{k+1}, \\
&\qquad \tilde{i} \xrightarrow{(0,\ldots,0,b_0)} i \xrightarrow{a_1 \cdot b_1} \ldots \xrightarrow{a_m \cdot b_m} q \in F \ dans \ \mathcal{A}_{k+1} \\
&\Leftrightarrow \quad \exists (b_0, \ldots, b_m) \in \{0,1\}^{m+1}, \\
&\qquad ((0, \ldots, 0, b_0), a_1 \cdot b_1, \ldots, a_m \cdot b_m) \in X_{k=1} \\
&\Leftrightarrow \quad (a_1, \ldots, a_m) \in X_k
\end{aligned}$$

3. Pour finir, nous construirons $\mathcal{A}_0 = (Q, \Sigma_0, \delta_0, I_0, F)$. Comme $\Sigma_0 = \{0,1\}^0 = \varnothing$, donc $\Sigma_0^* = \{\epsilon\}$. Du coup δ est défini sur l'ensemble vide, il n'y a donc aucune transition dans $\mathcal{A}_0$. Du coup $\mathcal{L}(\mathcal{A}_0) = \varnothing$ ou $\{\epsilon\}$, la deuxième solution n'est possible que si $I_0 \cap F \neq \varnothing$ et alors ϕ est vraie, sinon ϕ est fausse.