Décidabilité de l'arithmétique de Presburger

Manon Ruffini

Attention !

Ce développement est tiré du Carton, qui est loin d'être rigoureux ! Je vous conseille de vous référer au David-Nour-Raffali pour commencer par donner un énoncé plus propre du résultat.
Ensuite, il ne faut pas oublier dans les cas de base de faire l'automate successeur et il faut savoir pourquoi ces cas de bases sont suffisants.
Une version très détaillée est disponible ici :
`http://minerve.bretagne.ens-cachan.fr/images/914_2015-2016.pdf`
Je ne suis pas sûre qu'il faille tout détailler dans le développement, mais il y a des choses auxquelles il faut avoir réfléchi avant de faire ce développement.
(Et attention aux conflits de notations !)

Théorème 1 (*Presburger*)

La théorie au premier ordre des entiers munis de l'addition et de l'égalité est décidable.

On veut montrer que pour toute formule φ close de la logique de Presburger, on peut décider si $\mathbb{N} \models \varphi$. On peut supposer que φ est sous forme prénexe : $\varphi = Q_1 x_1 ... Q_n x_n \psi$, où les Q_i sont des quantificateurs.
Pour tout entier k tel que $0 \leqslant k \leqslant n$, soit $\varphi_k = Q_{k+1} x_{k+1} ... Q_n x_n \psi$; avec les conventions $\varphi_0 = \varphi$ et $\varphi_n = \psi$. Pour $0 \leqslant k \leqslant n$, les variables $x_1, ..., x_k$ sont exactement les variables libres dans la formule φ_k, et on peut écrire $\varphi_k(x_1, ..., x_k)$.
On définit l'ensemble $X_k := \{(n_1, ..., n_k) | \, (\mathbb{N}, \{x_i := n_i\}_{1 \leqslant i \leqslant k}) \models \varphi_k(x_1, ..., x_k)\}$.
On va montrer par récurrence sur $n - k$ que l'ensemble X_k est un ensemble rationnel.
D'abord, on définit un codage qui permet d'écrire les k-uplets d'entiers :

- Chaque entier est écrit en binaire sur l'alphabet $\Sigma = \{0, 1\}$.
- Un k-uplet d'entier est écrit sur l'alphabet $\Sigma^k = \{0, 1\}^k$, en ajoutant éventuellement des zéros en tête des écritures pour les rendre de la même longueur.
  Si $\forall 1 \leqslant i \leqslant k, x_i$ est codé $x_i^1 x_i^2 ... x_i^r$, le k-uplet est codé $(x_1^1 x_2^1 ... x_k^1)(x_1^2 ... x_k^2)...(x_1^r ... x_k^r)$

Exemple 1

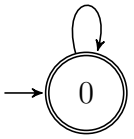
$2, 3$ et 7 sont codés respectivement sur Σ : (010), (011) *et* (111) *; et le triplet* $(2, 3, 7)$ *est codé* $(001)(111)(011)$

Pour tout $1 \leqslant k \leqslant n$, on construit un automate $\mathcal{A}_k$ qui accepte les écritures sur Σ^k des éléments de X_k. On le fait par récurrence sur $n - k$.

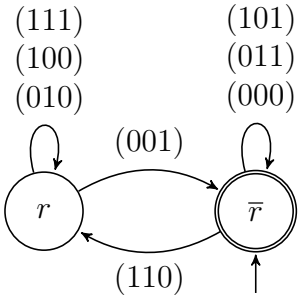
- Initialisation : construisons un automate $\mathcal{A}_n$ qui accepte exactement X_n, l'ensemble des n-uplets qui satisfont ψ. On le fait par induction sur la formule ψ.

  Si $\psi = (x_i = x_j)$: On construit facilement l'automate pour l'égalité :

$$(*...*, \overset{i}{1}, *...*, \overset{j}{1}, *...*)$$
$$(*...*, 0, *...*, 0, *...*)$$



Si $\psi = (x_i + x_j = x_k)$: On construit un automate comme s'il lisait de la droite vers la gauche. L'état r correspond à l'état avec retenue et l'état $\overline{r}$ correspond à l'état sans retenue. On n'écrit pas les $*$, pour plus de clarté (on suppose i, j, k distincts).



On en déduit facilement les automates pour i, j, k quelconques.

Si $\psi = \neg\psi_1$: Soit $\mathcal{A}_\psi$ l'automate qui accepte exactement les n-uplets satisfaisant ψ. On construit son complémentaire : il accepte exactement les n-uplets d'entiers qui satisfont $\neg\psi$.

Si $\psi = \psi_1 \wedge \psi_2$: On contruit l'automate de l'intersection de $\mathcal{A}_{\psi_1}$ et $\mathcal{A}_{\psi_2}$

Si $\psi = \psi_1 \vee \psi_2$: On contruit l'automate de l'union de $\mathcal{A}_{\psi_1}$ et $\mathcal{A}_{\psi_2}$

— Pour le passage de $\mathcal{A}_{k+1}$ à $\mathcal{A}_k$: Soit $1 \leqslant k < n$. On suppose construit l'automate $\mathcal{A}_{k+1}$. On a : $\varphi_k = Q_{k+1}x_{k+1}\varphi_{k+1}$, où Q_{k+1} est le quantificateur $\forall$ ou $\exists$. Dans le cas où Q_{k+1} est $\forall$, on utilise : $\varphi_k = \neg\exists x_{k+1}\neg\varphi_{k+1}$ et la stabilité des langages rationnels par complémentation. Il reste à traiter le cas $Q_{k+1} = \exists$.

On note : $\mathcal{A}_k = (M_k, \Sigma^k, M_k^0, F_k, E_k)$, et $\mathcal{A}_{k+1} = (M_{k+1}, \Sigma^{k+1}, M_{k+1}^0, F_{k+1}, E_{k+1})$, où : M_i correspond aux états, Σ^i à l'alphabet, M_i^0 aux états initiaux, F_i aux états finaux et $E_i \subset M_i \times \Sigma^i \times M_i$ aux transitions. Par hypothèse de récurrence, l'automate $\mathcal{A}_{k+1}$ est construit ; il accepte exactement X_{k+1}.

On définit $\mathcal{A}_k$ par :

$M_k = M_{k+1}$

$(p, (a_1...a_k), q) \in E_k$ si et seulement si $\exists a_{k+1}, (p, (a_1...a_k a_k + 1), q) \in E_{k+1}$

$F_k = F_{k+1}$

$M_k^0 = \{q \in M_k | q$ soit accessible depuis un état de M_{k+1}^0 en lisant $(0...0) \in \Sigma^k\}$, ce qui permet de prendre en compte les entiers x_{k+1} ayant une écriture binaire plus longue que celle des $x_1, ..., x_k$.

Par construction, l'automate $\mathcal{A}_k$ accepte exactement X_k.

Ainsi, on peut construire l'automate $\mathcal{A}_1$ qui accepte exactement $X_1 = \{n_1 \in \Sigma | (\mathbb{N}, x_1 := n_1) \models Q_1 n_1 \varphi_1(x_1)\}$.

Pour conclure :

— Si $\varphi = \forall x_1 \varphi_1(x_1) : \mathbb{N} \models \varphi$ ssi $\mathcal{L}(\mathcal{A}_1) = \{0, 1\}^*$

— Si $\varphi = \exists x_1 \varphi_1(x_1) : \mathbb{N} \models \varphi$ ssi $\mathcal{L}(\mathcal{A}_1) \neq \emptyset$

Références

[1] Olivier Carton, *Langages formels*. Vuibert, 2014.