Décidabilité de l'arithmétique de Presburger

Pierron Théo

12 avril 2014

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

Démonstration. On veut pouvoir décider si une formule close est valide. Soit φ une formule close. On peut la supposer sous forme prénexe i.e. $\varphi = Qx_1 \dots Qx_n\psi$.

On va définir un automate A qui reconnaît les n-uplets satisfaisant ψ. L'alphabet de A est $\{0,1\}^n$. On va encoder les n-uplets d'entiers par des mots sur cet alphabet.

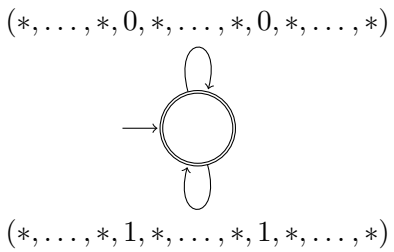
Soit $(x_1, \dots, x_n) \in \mathbb{N}^n$. On écrit chaque x_i en binaire, le bit de poids faible à gauche et on complète à droite par des 0 pour avoir la même taille : chaque x_i s'écrit $x_{i,1} \dots x_{i,k}$ sous cette forme. On encode alors $(x_1, \dots, x_n)$ par le mot

$$(x_{1,1}, \dots, x_{n,1}) \dots (x_{1,k}, \dots, x_{n,k})$$

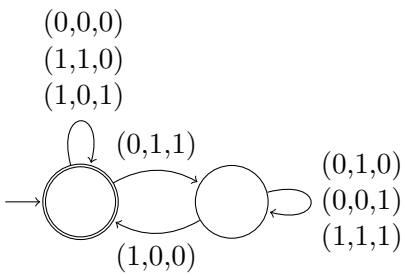
Exemple $(3,5,6)$ devient $(110, 101, 011)$ puis le mot $(1,1,0)(1,0,1)(0,1,1)$.

On construit A par induction sur ψ :

- Cas $x_i = x_j$



- Cas $x_i = x_j + x_k$. Pour des raisons de lisibilité, on n'écrit pas les étoiles cette fois



  On en déduit les automates pour i, j et k non nécessairement distincts.
- Cas $F \vee G$: on fait l'automate de l'union entre A_F et A_G
- Cas $\neg F$: on fait l'automate du complémentaire de A_F
- Cas $F \wedge G$: on fait l'automate de l'intersection entre A_F et A_G

On construit à partir de A_ψ par récurrence sur n un automate pour $Qx_2 \dots Qx_n\psi$.

- Si le i-ème quantificateur est un $\forall$, on se ramène au cas suivant en utilisant l'équivalence sémantique $\forall x_i F = \neg\exists x_i \neg F$.

- Si on construit l'automate de $\exists x_i \phi$, soit A_ϕ l'automate de ϕ. Pour chaque transition étiquetée par $(\alpha_1, \ldots, \alpha_i)$, on va effacer la dernière composante. Autrement dit, $A_{\exists x_i \phi} = (Q_\phi, \{0,1\}^{i-1}, I_\phi, F_\phi, \delta')$ avec

$$q' \in \delta'(q, (\alpha_1, \ldots, \alpha_{i-1})) \quad \text{ssi} \quad \exists \alpha_i \in \{0,1\}, q' \in \delta(q, (\alpha_1, \ldots, \alpha_i))$$

Il reste maintenant à conclure :

- Si $\varphi = \forall x_1 \phi(x_1)$, alors φ est valide ssi $L(A_\phi) = \{0,1\}^*$.
- Si $\varphi = \exists x_i \phi(x_1)$, alors φ est valide ssi $L(A_\phi) \neq \varnothing$.

Ces deux problèmes étant décidables, la validité de φ est décidable. (Noter qu'en revanche la complexité n'est pas élémentaire.) ■

Remarque *On aurait pu construire l'automate A_φ qui serait en fait un graphe orienté, et tester l'accessibilité d'un état final à partir d'un état initial.*