DÉCIDABILITÉ DE L'ARITHMÉTIQUE DE PRESBURGER.

Leçons : 909, 914, 924.

Références : Carton, Langages formels Calculabilité et Complexité p. 179.

Théorème

L'arithmétique de Presburger est la théorie du premier ordre des entiers munis de l'addition mais pas de la multiplication.

Cette théorie est décidable.

Note

Pour la culture, l'arithmétique de Presburger est la théorie contenant les symboles +, 0 et 1, ainsi que les axiomes suivants :

- $\forall x \quad \neg(0 = x+1)$
- $\forall x,y \quad (x+1 = y+1) \Longrightarrow x = y.$
- $\forall x \quad x + 0 = x$
- $\forall x,y \quad (x+y)+1 = x+(y+1).$
- $\forall \bar{x} \, (P(0,\bar{x}) \wedge (\forall y \, P(y,\bar{x}) \rightarrow P(y+1,\bar{x}))) \longrightarrow \forall y \, P(y,\bar{x})$ pour toute formule $P(y, x_1, \dots, x_n)$.

Résumé (On montre que le langage des n-uplets qui satisfont une formule φ est rationnel)

I – Soit φ une formule close que l'on écrit sous forme pré-nexe :

$$\varphi = Q_1 x_1 Q_2 x_2 \cdots Q_n x_n \psi \quad \text{où } Q_1, \dots, Q_n \text{ sont des quantificateurs.}$$

On encode ensuite une séquence d'arguments pour définit X_k.

II – Automate qui reconnait le langage correspondant à ψ.

III – On prouve par récurrence qu'on peut rajouter les quantificateurs.

IV – Un exemple : automate pour $x \equiv 0 \mod 3$.

I/ On a $\varphi = Q_1 x_1 \cdots Q_n x_n \psi$.

• Définissons $\varphi_k = Q_{k+1} x_{k+1} \cdots Q_n x_n \psi$.

avec $\varphi_0 = \varphi$ et $\varphi_n = \psi$.

Dans φ_k, $x_1, \ldots, x_k$ sont libres et on écrit donc $\varphi_k(x_1, \ldots, x_k)$.

• Pour reconnaître φ_k, on a besoin d'utiliser un codage. Pour cela, on écrit chacun des $x_1, \ldots, x_k$ en binaire (sur $\Sigma = \{0,1\}$).

Un k-uplet d'entiers peut alors s'écrire sur Σ_2^k quitte à ajouter des zéros à la fin pour avoir des nombres de même longueur:

$$(1, 4, 10) \text{ s'écrit } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in (\Sigma^k)^*.$$

• On peut alors définir le langage reconnu par φ_k:

$$X_k = \{(x_1, \ldots, x_k) \in (\Sigma^k)^* \mid \varphi_k(x_1, \ldots, x_k) \text{ est vraie}\}.$$

II/

• Construisons l'automate $\mathcal{A}_n$ qui reconnaît X_n, i.e. "quand ψ est vraie ?"

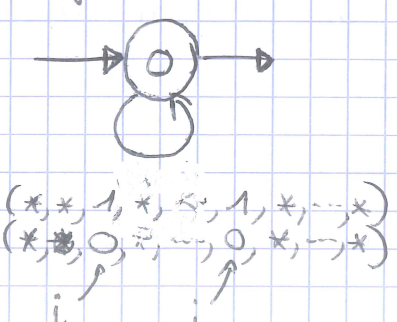
• ψ s'écrit comme une combinaisons booléennes de formules de type :

i) $x_i = x_j$ ou ii) $x_i + x_j = x_k$.

• La classe des langages rationnels est close pour les opérations booléennes. Il suffit donc de construire des automates pour les formules de type i) et ii)

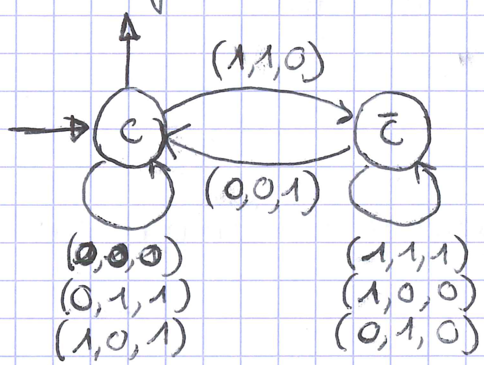
i) Pour l'égalité, on définit l'automate suivant:

$x_i = x_j$:



ii) Et pour l'addition :

$x_i + x_j = x_k$.



où $\bar{c}$ correspond à la retenue.

(on s'épargne l'écriture des variables inutiles)

→ on a ainsi un automate qui reconnaît X_n.

III • Montrons qu'on peut rajouter un quantificateur, c'est-à-dire que étant donné A_k reconnaissant X_k, on peut construire A_{k-1}, reconnaissant X_{k-1}.

■ Supposons alors que Q_k est un quantificateur d'existence $\exists$.

• Définissons avant tout l'opérateur de projection :

$$\pi_k : \begin{array}{ccc} \Sigma_k & \longrightarrow & \Sigma_{k-1} \\ (x_1,\dots,x_k) & \longmapsto & (x_1,\dots,x_{k-1}) \end{array}.$$

• Cela permet de définir l'automate A_{k-1} dont :

- l'ensemble d'états est le même que pour A_k.
- les états finaux sont les mêmes que pour A_k.
- les états initiaux sont ceux de A_k, auxquels on rajoute les états obtenus en lisant $(0,\dots,0)$
- la fonction de transition est telle que

$$p \xrightarrow{x} q \text{ dans } A_k \quad \text{ssi} \quad p \xrightarrow{\pi_k(x)} q$$

→ en quelque sorte, l'automate A_{k-1} devine une valeur qui conviendrait à x_k (ou plutôt il fait semblant d'oublier !), ce qui correspond bien au quantificateur ~~universel~~ existentiel

- N'oublions pas que Q_k peut aussi être un quantificateur universel $\forall$.

→ en fait, on a déjà gagné, parce que :

$$\varphi_{k-1} = \forall x_k \ \varphi_k$$
$$= \neg \exists x_k (\neg \varphi_k)$$

Et la clôture par complémentation des langages rationnels donne le résultat.

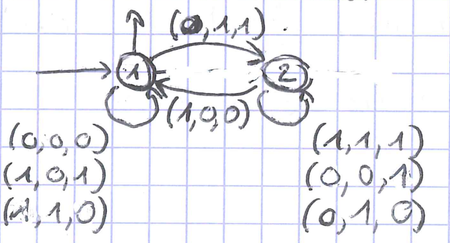
⇒ Pour finir, il suffit de remarquer que A_0 reconnaît au moins un mot si et seulement si φ est vraie !

$\boxed{\text{IV}}$ • L'expression $x \equiv 0 \bmod 3$, c'est en fait l'expression :

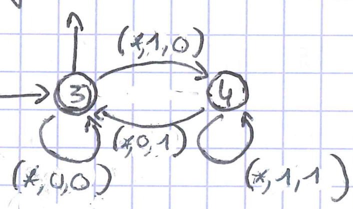
$$\exists y \ \exists z \ (x = y + z) \wedge (z = y + y).$$

Cela donne les automates suivants :

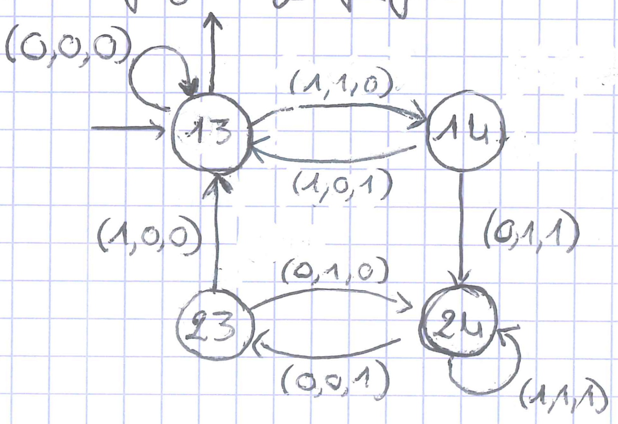
$\underline{x = y + z}$



$\underline{z = y + y}$



$\underline{(x = y + z) \wedge (z = y + y)}$



$\underline{\exists y \exists z \ (x = y + z) \wedge (z = y + y)}$