LE SYSTÈME AXIOMATIQUE S, LES ENTIERS ET LES FONCTIONS REPRÉSENTABLES*

Luc Bélair

Table des matières

1 Une image des entiers dans S

On a déjà remarqué qu'on avait une *image* de chacun des entiers naturels $0, 1, 2, \ldots$ dans le système S grâce aux termes de la forme $0''''''$. Plus précisément, l'entier naturel n est représenté par le terme $0''^{\cdots\prime}$ où $'$ apparaît n fois. On note ce terme $\bar{n}$ ($\bar{0}$ n'est rien d'autre que 0). Dans le modèle naturel $(\mathbb{N}, =, 0, ', +, \cdot)$ de S, chaque entier n coïncide avec l'interprétation $\bar{n}^{\mathbb{N}}$, de son image $\bar{n}$ dans S. On a aussi remarqué que cette représentation était assez fidèle au sens où, par exemple, $\bar{2} \cdot \bar{5} = \overline{10}$ est démontrable dans S. Les résulats suivants mettent bien en évidence ce phénomène.

Proposition 3.5 [1]

(a) $\vdash_S \ t + \bar{1} = t'$ (en part. $\vdash_S \ \bar{n} + \bar{1} = \bar{n}'$)

(b) $\vdash_S \ t \cdot \bar{1} = t$

(c) $\vdash_S \ t + t = \bar{2} \cdot t$

(f) $\vdash_S \ t + s = \bar{1} \Rightarrow (t = 0 \wedge s = \bar{1}) \vee (t = \bar{1} \wedge s = 0)$

(g) $\vdash_S \ t \cdot s = \bar{1} \Rightarrow (t = \bar{1} \wedge s = \bar{1})$

---

*Séminaire de logique, UQAM, le 17 novembre 2005.

[1] Le numéro des propositions renvoient au livre de Mendelson, *Introduction to mathematical logic* (3e édition).

Proposition 3.6

(a) (i) Si $m \neq n$, alors $\vdash_S \ \bar{m} \neq \bar{n}$.

(ii) $\vdash_S \ \bar{m} + \bar{n} = \overline{m+n}$

$\vdash_S \ \bar{m} \cdot \bar{n} = \overline{mn}$

Proposition 3.7 [2]

(i) $\vdash_S \ 0 \leq t$

(j) $\vdash_S \ 0 < t'$

(n) $\vdash_S \ 0 < \bar{1}$, $\vdash_S \ \bar{1} < \bar{2}$, $\vdash_S \ \bar{2} < \bar{3}$

$\vdash_S \ \bar{m} < \bar{n}$, si $m < n$.

Proposition 3.8

(a) $\vdash_S \ x \leq \bar{k} \iff x = 0 \vee x = \bar{1} \vee \ldots \vee x = \bar{k}$

(a') $\vdash_S \ \forall x(x \leq \bar{k} \Rightarrow \mathcal{A}(x))$ si et seulement si $\vdash_S \ \mathcal{A}(0) \wedge \mathcal{A}(\bar{1}) \wedge \ldots \wedge \mathcal{A}(\bar{k})$

Proposition 3.10 [3]

(b) $\vdash_S \ \bar{1} \mid t$

(c) $\vdash_S \ t \mid 0$

$\vdash_S \ t \mid \bar{1} \Rightarrow t = \bar{1}$

2 Modèles de S

Le modèle naturel $(\mathbb{N}, =, 0,', +, \cdot)$ assure la cohérence de S. Que peut-on dire des autres modèles ?

Rappelons que dans le système axiomatique S, comme l'assure la proposition suivante, les prédicats $x < y$ et $x \leq y$ satisfont les propriétés axiomatiques de relation d'ordre total, où chaque élément a un successeur immédiat par rapport à l'ordre (à savoir x', voir (*) dans la proposition.).

Proposition 3.7

(a) $\vdash_S \ t \not< t$

(b) $\vdash_S \ t < s \Rightarrow (s < r \Rightarrow t < r)$

[2]Rappelons que $x < y$ est une abréviation de $\exists z(z \neq 0 \wedge z + x = y)$, et coïncide bien avec la relation habituelle d'ordre strict dans le modèle naturel, et que $x \leq y$ qui est une abréviation de $(x < y \vee x = y)$, et coïncide bien avec la relation habituelle d'ordre (au sens large) dans le modèle naturel.

[3]De même, $x \mid y$ est une abréviation de la formule $\exists z(x \cdot z = y)$, et coïncide avec la relation habituelle de divisibilité (x divise y) dans le modèle naturel.

(c) $\vdash_S \; t < s \Rightarrow s \nless t$

(e) $\vdash_S \; t \leq t$

(f) $\vdash_S \; t \leq s \Rightarrow (s \leq r \Rightarrow t \leq r)$

(z) $\vdash_S \; t \leq s \wedge s \leq t \Rightarrow s = t$

(o) $\vdash_S \; t = r \vee t < r \vee r < t$

(p) $\vdash_S \; t \leq r \vee r \leq t$

(k) $\vdash_S \; t < r \iff t' \leq r$

(l) $\vdash_S \; t \leq r \iff t < r'$

(*) $\vdash_S \; t \leq r \wedge r \leq t' \Rightarrow r = t \vee r = t'$

De sorte que dans tout modèle M de S, la relation binaire $<^M$, obtenue de l'interprétation du prédicat $x < y$ dans M, définit un ordre total où chaque élément $a \in M$ a un successeur immédiat par rapport à l'ordre, à savoir ${a'}^M$.

Un simple argument de compacité, c'est-à-dire qui utilise le théorème de compacité de la logique du premier ordre, assure l'existence d'au moins un modèle différent du modèle naturel. Rappelons ce théorème.

Théorème de compacité de la logique du premier ordre. Soit K une théorie d'un langage[4] du premier ordre. Alors K possède au moins un modèle si et seulement si toute partie finie de K en possède au moins un.

On peut le voir comme conséquence directe du théorème de complétude de Gödel[5] : la cohérence de K est manifestement équivalente à la cohérence de chacune de ses parties finies, et par complétude la cohérence est équivalente à l'existence d'un modèle.

Revenons à S et ses modèles. Soit $\mathcal{L}$ le langage de S et c un nouveau symbole de constante et posons $\mathcal{L}_c = \mathcal{L} \cup \{c\}$. Considérons la théorie suivante dans $\mathcal{L}_c$

$$S_c = S \cup \{c \neq \bar{n} : n \in \mathbb{N}\}$$

Toute partie finie de S_c est de la forme

$$S_0 \cup \{c \neq \bar{n}_1, \ldots, c \neq \bar{n}_k\}$$

où S_0 est une partie finie de S et k un certain entier. Mais alors $(\mathbb{N}, =, 0, ', +, \cdot)$ fournit un modèle de cette partie finie en interprétant c par un nombre naturel assez grand. Par le théorème de compacité de la logique du

[4]Rappelons qu'on travaille avec des langages de cardinalité dénombrable.

[5]Cf. les notes du premier exposé de Neil Kennedy, Cor. 2.9.

premier ordre, la théorie $S \cup \{c \neq \bar{n} : n \in \mathbb{N}\}$ possède un modèle, disons M. Alors les conditions $c^M \neq \bar{n}^M$ assurent que M ne peut être le modèle naturel, ni même une copie de celui-ci.

Par ailleurs, les propriétes formelles de l'ordre $<$ dans la théorie S, vues dans les propositions précédentes, assurent que le **modèle nonstandard** M est un ensemble totalement ordonné par $<^M$ tel que tout élément $x \in M$ a un successeur immédiat pour l'ordre $<^M$ qui n'est autre que x'^M, et que l'image des entiers dans M, les $\bar{n}^M$, en forment un segment initial.

Il s'ensuit qu'on doit avoir $\bar{n}^M < c^M$, pour tout $n \in \mathbb{N}$, par la Prop. 3.8 (a) et la propriété clé de c^M. Ainsi c^M est en quelque sorte **infini** par rapport à l'image des entiers que nous avons dans M.

Notons aussi que $0^M < c^M$, de sorte que c^M a un prédécesseur qu'on peut noter $c^M - \bar{1}^M$, par la Prop. 3.5(a). Or $c^M - \bar{1}^M$ doit aussi être *infini* : si $c^M - \bar{1}^M = \bar{n}^M$, alors $(c^M - \bar{1}^M)'^M = c^M = \overline{n+1}^M$, ce qui ne peut être le cas. De même $c^M - \bar{1}^M$ a un prédécesseur, et ainsi de suite.

$$\begin{array}{cccccccccc} \bullet & \bullet & \bullet & \bullet & \cdots & \cdots & \bullet & \bullet & \bullet & \cdots \\ \bar{0}^M & \bar{1}^M & \bar{2}^M & \bar{3}^M & & & c^M - \bar{1} & c^M & c^M + \bar{1} = c'^M & \end{array}$$

En particulier, **il n'y a pas de plus petit élément infini dans M.** Plus précisément, si on pose

$$\mathcal{J} = \{a \in M : \bar{n}^M <^M a, \text{ pour tout } n \in \mathbb{N}\}$$

alors $\mathcal{J}$ n'a pas de plus petit élément pour l'ordre $<^M$.

Or rappelons que c'est une propriété fondamentale[6] du modèle naturel $\mathbb{N}$ que toute partie non vide de $\mathbb{N}$ possède un plus petit élément. En plus, cette propriété persiste dans le système axiomatique S, *mais (que) pour les prédicats du premier ordre*, à savoir on a (cf. Mendelson)

Proposition 3.9
(b) Pour toute formule $\mathcal{A}(x)$, on a
$\vdash_S \ \exists x \mathcal{A}(x) \Rightarrow \exists y\, (\mathcal{A}(y) \wedge \forall z(\mathcal{A}(z) \Rightarrow z \leq y))$.

On en conclut qu'*il ne peut pas* y avoir de formule $\mathcal{A}(x)$ dans le langage de S dont $\mathcal{J}$ soit l'ensemble solution, c.-à-d. tel que $\mathcal{J} = \{a \in M : M \models \mathcal{A}(a)\}$.

[6] C'est une forme du principe d'induction.

3 Fonctions représentables

Rappelons qu'une **relation d'entiers d'arité** n est une partie du produit cartésien $\mathbb{N}^n = \mathbb{N} \times \ldots \times \mathbb{N}$, c'est-à-dire que c'est un ensemble de n-uplets $(k_1, \ldots, k_n)$ de nombres naturels $k_i \in \mathbb{N}$. On utlise la notation $R(k_1, \ldots, k_n)$ pour désigner le fait que $(k_1, \ldots, k_n)$ *satisfait* la relation R, ou encore *appartient* à la relation R.

Une **fonction d'entiers d'arité** n est une fonction de $\mathbb{N}^n$ dans $\mathbb{N}$, c'est-à-dire qui associe à chaque n-uplets de $\mathbb{N}^n$ une valeur dans $\mathbb{N}$. Ainsi, l'addition est une fonction d'entiers d'arité 2. [7]

Définition. Soit K une théorie dans le même langage que S, et R une relation d'entiers d'arité n. On dit que R est *représentable dans* K, si il existe au moins une formule $\mathcal{A}(x_1, \ldots, x_n)$ ayant n variables libres telle que pour tous entiers $k_1, \ldots, k_n \in \mathbb{N}$ on ait

(1) Si $R(k_1, \ldots, k_n)$ est vrai, alors $\vdash_K \ \mathcal{A}(\bar{k}_1, \ldots, \bar{k}_n)$.

(2) Si $R(k_1, \ldots, k_n)$ est faux, alors $\vdash_K \ \neg\mathcal{A}(\bar{k}_1, \ldots, \bar{k}_n)$.

Exemple.

(a) Soit $K = S$, la relation d'égalité est représentable par la formule $\mathcal{A}(x_1, x_2) : x_1 = x_2$. Pour tous entiers k_1, k_2,, si $k_1 = k_2$, alors $\bar{k}_1, \bar{k}_2$ *sont* le même terme et on a $\vdash_S \ \bar{k}_1 = \bar{k}_2$. Par ailleurs, si $k_1 \neq k_2$, alors par la Prop. 3.6 on a $\vdash_S \ \bar{k}_1 \neq \bar{k}_2$.

(b) Soit $K = S$, la relation d'ordre strict est représentable par la formule $\mathcal{A}(x_1, x_2) : \exists x_3(x_3 \neq 0 \wedge x_3 + x_1 = x_2)$, par la Prop. 3.7.

(c) Soit $K = S$, le graphe de l'addition est représentable par la formule $\mathcal{A}(x_1, x_2, x_3) : x_1 + x_2 = x_3$, par la Prop. 3.6.

(d) Soient R_1, R_2 de même arité et représentables dans K, disons R_i représentable par $\mathcal{A}_i(x_1, \ldots, x_n)$. Alors $R_1 \cap R_2$ est aussi représentable dans K, par la formule $\mathcal{A}_1(x_1, \ldots, x_n) \wedge \mathcal{A}_2(x_1, \ldots, x_n)$.

Définition. Soit K une théorie *avec égalité* [8] dans le même langage que S, et f une relation d'entiers d'arité n. On dit que f est *représentable dans* K, si il existe au moins une formule $\mathcal{A}(x_1, \ldots, x_n, x_{n+1})$ ayant $n + 1$ variables libres telle que pour tous entiers $k_1, \ldots, k_n, m \in \mathbb{N}$ on ait

[7] On ne considère donc que les fonctions qui sont définies pour tous les uplets. Ce qui fait en sorte que, stricto sensu, la soustraction n'est pas une fonction d'entiers.

[8] Au sens technique du livre de Mendelson : on a $\vdash_K \forall x_1(x_1 = x_1)$, et pour chaque formule $\mathcal{A}(x)$ on a $\vdash_K (x = y) \Rightarrow (\mathcal{A}(x) \Leftrightarrow \mathcal{A}(y))$, où y est libre pour x dans $\mathcal{A}(x)$ (cf les notes du premier exposé de Neil Kennedy). La théorie S elle-même est une telle théorie.

(1) Si $f(k_1, \ldots, k_n) = m$ est vrai, alors $\vdash_K \ \mathcal{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m})$.

(2) $\vdash_K \ \exists! x_{n+1} \mathcal{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m})$. [9]

Notons qu'une fonction d'entiers f est représentable dans S si et seulement si il existe une formule $\mathcal{A}(x_1, \ldots, x_{n+1})$ telle que pour tous entiers $k_1, \ldots, k_n, m \in \mathbb{N}$ on ait que si $f(k_1, \ldots, k_n) = m$ est vrai, alors $\vdash_K (\mathcal{A}(\bar{k}_1, \ldots, \bar{k}_n, x_{n+1}) \iff x_{n+1} = \bar{m})$. Ou encore si et seulement si le graphe[10] de f est une relation représentable dans S.

Exemple.

(a) La fonction constante nulle $Z(k) = 0$ est représentable par la formule $\mathcal{A}(x_1, x_2) : x_1 = x_1 \wedge x_2 = 0$. Pour tous entiers k_1, m, si $Z(k_1) = m$, alors m est 0 et on a $\vdash_K \ \bar{k}_1 = \bar{k}_1 \wedge \bar{0} = 0$. Par ailleurs, on vérifie que $\vdash_K \ \exists! x_{n+1}(\bar{k}_1 = \bar{k}_1 \wedge x_{n+1} = 0)$.

(b) La fonction successeur $P(k) = k + 1$ est représentable par la formule $\mathcal{A}(x_1, x_2) : x_2 = (x_1)'$. Si $P(k_1) = k_2$, alors k_2 est $k_1 + 1$ et $\bar{k}_2$ est le même terme que $\bar{k}_1'$ de sorte que $\vdash_K \ \bar{k}_2 = (\bar{k}_1)'$. On vérifie que $\vdash_K \ \exists! x_2(x_2 = (\bar{k}_1)')$.

(c) La fonction de projection $U_j^n(x_1, \ldots, x_n) = x_j$ représentable par la formule $\mathcal{A}(x_1, \ldots, x_n) : x_1 = x_2 \wedge \ldots \wedge x_n = x_n \wedge x_{n+1} = x_j$.

(d) Soient g, h deux fonctions d'arité 1 et représentables dans K, disons g représentable par $\mathcal{A}(x_1, x_2)$ et h par $\mathcal{B}(x_1, x_2)$. Alors la fonction composée $f(x) = h(g(x))$ est aussi représentable dans K, par la formule $\mathcal{C}(x_1, x_2) : \exists y(\mathcal{A}(x_1, y) \wedge \mathcal{B}_2(y, x_2))$.

(e) L'addition est représentable dans S par la formule $\mathcal{A}(x_1, x_2, x_3)$: $x_1 + x_2 = x_3$, par la Prop. 3.6 .

(f) La multiplication est représentable dans S par la formule $\mathcal{A}(x_1, x_2, x_3)$: $x_1 \cdot x_2 = x_3$, par la Prop. 3.6 .

On montrera éventuellement que la fonction d'exponentiation $\exp(m, n) = m^n$ est représentable. Notons que cette fonction peut se définir par une récursion simple à l'aide de la multiplication : $\exp(m, 0) = 1$, $\exp(m, n+1) = \exp(m, n) \cdot m$. On montrera aussi que la fonction suivante[11] définie par une double récursion est aussi représentable :

[9] $\exists! x \mathcal{B}(x)$ est une abréviation de $\exists x(\mathcal{B}(x) \wedge \forall y(\mathcal{B}(y) \Rightarrow y = x))$, c.-à-d. *il existe un unique x tel que $\mathcal{B}(x)$*. La notation de Mendelson est $\exists_1 x$.

[10] C.-à-d. la relation $\{(k_1, \ldots, k_n, k_{n+1}) \in \mathbb{N}^{n+1} : f(k_1, \ldots, k_n) = k_{n+1}\}$.

[11] Une variante de la fonction d'Ackermann.

(i) $\alpha(0, m) = 2^m$

(ii) $\alpha(n, 0) = 1$

(iii) $\alpha(n+1, m+1) = \alpha(n, \alpha(n+1, m))$

On peut noter que $\alpha(1, m) = \alpha(0, \alpha(1, m-1)) = 2^{\alpha(1,m-1)}$, de sorte que $\alpha(1,1) = 2, \alpha(1,2) = 2^2, \alpha(1,3) = 2^{2^2}$ etc.

Remarque Soit Pr les axiomes de l'arithmétique de Presburger et $\mathcal{L}_{Pr}$ son langage (le même que S mais sans la multiplication). On peut considérer la notion de fonction représentable par rapport à l'arithmétique de Presburger, c.-à-d. en remplaçant S par Pr. On peut montrer, à partir du théorème d'élimination des quantificateurs de Presburger[12], que la multiplication n'est pas représentable dans Pr, c'est-à-dire qu'il n'y a aucune formule $\mathcal{A}(x_1, x_2, x_3)$ de $\mathcal{L}_{Pr}$ telle que pour tous $k_1.k_2, k_3 \in \mathbb{N}$ on ait

(1) si $k_1 + k_2 = k_3$, alors $\vdash_{Pr}\ \mathcal{A}(\bar{k}_1, \bar{k}_2, \bar{k}_3)$

(2) $\vdash_{Pr} \exists! x_3 \mathcal{A}(\bar{k}_1, \bar{k}_2, x_3)$

Notons que la multiplication $m \cdot n$ peut être définie par une récursion simple à l'aide de l'addition : $m \cdot 0 = 0$, $m \cdot (n+1) = (m \cdot n) \cdot m$.

[12] Voir mon exposé précédent.