LA REPRÉSENTABILITÉ DES FONCTIONS ET DE RELATIONS RÉCURSIVES

Neil Kennedy, UQÀM

10 février, 2006

1. La représentation : rappel

Rappelons qu'une relation arithmétique $R(x_1, x_2, ..., x_n)$ est *représentable* dans S s'il existe une formule $\mathcal{A}(x_1, ..., x_n)$ de S telle que pour tous nombres $k_1, k_2, ..., k_n$

(1) Si $R(k_1, k_2, ..., k_n)$ alors $\vdash_S \mathcal{A}(\overline{k}_1, ..., \overline{k}_n)$,

(2) Si non-$R(k_1, k_2, ..., k_n)$ alors $\vdash_S \neg\mathcal{A}(\overline{k}_1, ..., \overline{k}_n)$.

Une fonction arithmétique $f(x_1, x_2, ..., x_n)$ est *représentable* dans S s'il existe une formule $\mathcal{A}(x_1, ..., x_n, x_{n+1})$ de S telle que pour tous nombres $k_1, k_2, ..., k_n$ et m

(1) Si $f(k_1, k_2, ..., k_n) = m$ alors $\vdash_S \mathcal{A}(\overline{k}_1, ..., \overline{k}_n, \overline{m})$,

(2) $\vdash_S \exists_1 x_{n+1} \mathcal{A}(\overline{k}_1, ..., \overline{k}_n, x_{n+1})$.

Si la deuxième condition est remplacée par

(3) $\vdash_S \exists_1 x_{n+1} \mathcal{A}(x_1, ..., x_n, x_{n+1})$,

on dit que $f(x_1, x_2, ..., x_n)$ est *fortement représentable*.[1]

Il y a un lien étroit entre une la représentabilité d'une relation et celle de sa fonction caractéristique :

Proposition 3.12. Soit K une théorie avec égalité ayant les même symboles que S et telle que $\vdash_K 0 \neq \overline{1}$. Alors une relation arithmétique R est représentable dans K (en tant que relation) si et seulement si C_R, sa fonction caractéristique, est représentable dans K (en tant que fonction).

Rappelons également le contenu de la proposition 3.6(a) (p. 124), laquelle nous donne de l'information sur la représentabilité de l'égalité, de l'addition et de la multiplication :

Proposition 3.6(a). Soient m et n des nombres naturels. Alors

(i) Si $m \neq n$, alors $\vdash_S \overline{m} \neq \overline{n}$,

(ii) $\vdash_S \overline{m+n} = \overline{m} + \overline{n}$ et $\vdash_S \overline{m \cdot n} = \overline{m} \cdot \overline{n}$.

De la proposition 3.6(a) découle le corollaire suivant :

Corollaire. La relation d'égalité et les fonctions d'addition et de multiplication sont représentables.

---

[1] Dans le texte de Mendelson, on dit qu'une relation est *exprimable* (en anglais : *expressible*) et qu'une fonction est *représentable* (en anglais : *representable*). Je n'ai pas cru bon ici de reprendre cette discrimination terminologique.

PREUVE. Commençons par la relation d'égalité. Si $m = n$, c'est que m est n, donc les termes $\overline{m}$ et $\overline{n}$ sont identiques. Ainsi, par proposition 3.2(a), $\vdash_S \overline{m} = \overline{n}$. Si $m \neq n$, alors nous appliquons la proposition 3.6(a)(i) pour obtenir $\vdash_S \overline{m} \neq \overline{n}$. L'égalité est donc une relation représentable dans *S*.

Montrons que la fonction addition est représentable dans *S* par la formule $x_1 + x_2 = x_3$. Si $m + n = p$, nous avons d'après la proposition 3.6(a)(ii) que $\vdash_S \overline{m} + \overline{n} = \overline{p}$. Nous pouvons également montrer que $\vdash_S \exists_1 x_3 x_1 + x_2 = x_3$.

Le cas de la multiplication est analogue. La formule qui représente cette fonction est évidemment $x_1 \cdot x_2 = x_3$. Si $m \cdot n = p$, alors d'après la proposition 3.6(a)(ii) $\vdash_S \overline{m} \cdot \overline{n} = \overline{p}$. (J'omets la démonstration de $\vdash_S \exists_1 x_3 x_1 \cdot x_2 = x_3$). □

2. La représentabilité des fonctions initiales

Il est assez simple de montrer que les fonctions initiales introduites au début de la section 3 sont représentables (ces démonstrations se trouvent aux pp. 130-1) :

Fonction zéro. La fonction $Z(x) = 0$ est fortement représentable par la formule $x_1 = x_1 \wedge x_2 = 0$. En effet, si $Z(k_1) = k_2$ alors $k_2 = 0$. Or, $\vdash_S \overline{k_1} = \overline{k_1}$ et $\vdash_S 0 = 0$ donc

$$\vdash_S \overline{k_1} = \overline{k_1} \wedge 0 = 0.$$

Par ailleurs, $\vdash_S \exists_1 x_2 (x_1 = x_1 \wedge x_2 = 0)$. □

Fonction successeur. La fonction $N(x) = x + 1$ est fortement représentable par la formule $x_2 = x_1'$. Pour tous k_1 et k_2, si $N(k_1) = k_2$ c'est que $k_2 = k_1 + 1$ et donc que $\vdash_S \overline{k_2} = \overline{k_1}'$. Aussi, $\vdash_S \exists_1 x_2 x_2 = x_1'$. □

Fonction projection. La fonction $U_j^n(x_1, ..., x_n) = x_j$ (avec $1 \leq j \leq n$) est fortement représentable par la formule $x_1 = x_1 \wedge x_2 = x_2 \wedge \cdots \wedge x_n = x_n \wedge x_{n+1} = x_j$. En effet, si $U_j^n(k_1, ..., k_n) = k_{n+1}$ c'est que $k_{n+1} = k_j$ et donc que $\vdash_S \overline{k_{n+1}} = \overline{k_j}$. De même, $\vdash_S \overline{k_i} = \overline{k_i}$ pour $i = 1, ..., n$, donc

$$\vdash_S \overline{k_1} = \overline{k_1} \wedge \overline{k_2} = \overline{k_2} \wedge \cdots \wedge \overline{k_n} = \overline{k_n} \wedge \overline{k_{n+1}} = \overline{k_j}.$$

Nous pouvons également montrer que

$$\vdash_S \exists_1 x_{n+1} (x_1 = x_1 \wedge x_2 = x_2 \wedge \cdots \wedge x_n = x_n \wedge x_{n+1} = x_j). \text{ □}$$

3. La représentabilité de la substitution et de l'opérateur μ

Montrons à présent que la substitution et l'opérateur μ sont des opérations qui « préservent » la représentabilité des fonctions. Il ne restera qu'à montrer que l'opération de récursivité en fait de même. (La première démonstration est à la p. 131 et la seconde à la p. 145.)

<u>La substitution</u>. Soient $g(x_1,...,x_m)$, $h_1(x_1,...,x_n),...,h_m(x_1,...,x_n)$ des fonctions (fortement) représentables par les formules $\mathcal{B}(x_1,...,x_{m+1})$, $\mathcal{A}_1(x_1,...,x_{n+1}),...,\mathcal{A}_m(x_1,...,x_{n+1})$ et soit

$$f(x_1,...,x_n) = g(h_1(x_1,...,x_n),...,h_m(x_1,...,x_n)) .$$

Montrons que *f* est (fortement) représentable par la formule $\mathcal{C}(x_1,...,x_{n+1})$:

$$\exists y_1 \cdots \exists y_m \left(\mathcal{A}_1(x_1,...,x_n,y_1) \wedge \cdots \wedge \mathcal{A}_m(x_1,...,x_n,y_m) \wedge \mathcal{B}(y_1,...,y_m,x_{n+1}) \right).$$

Supposons que $f(k_1,...,k_n) = p$. Si $h_i(k_1,...,k_n) = r_i$ pour $1 \le i \le m$, nous avons que $g(r_1,...,r_m) = p$ par la définition de *f*. Puisque $\mathcal{B}, \mathcal{A}_1,...,\mathcal{A}_m$ représentent $g, h_1,...,h_m$, nous avons que $\vdash_S \mathcal{A}_i(\overline{k}_1,...,\overline{k}_n,\overline{r}_i)$ pour $1 \le i \le m$ et $\vdash_S \mathcal{B}(\overline{r}_1,...,\overline{r}_m,\overline{p})$. Par conséquent,

$$\vdash_S \mathcal{A}_1(\overline{k}_1,...,\overline{k}_n,\overline{r}_1) \wedge \cdots \wedge \mathcal{A}_m(\overline{k}_1,...,\overline{k}_n,\overline{r}_m) \wedge \mathcal{B}(\overline{r}_1,...,\overline{r}_m,\overline{p})$$

d'où $\vdash_S \mathcal{C}(\overline{k}_1,...,\overline{k}_n,\overline{p})$ par l'introduction de quantificateurs existentiels.

Pour la démonstration de la deuxième condition, il suffirait de démontrer l'unicité puisque nous avons déjà établi l'existence, c'est-à-dire, démontrer

$$\vdash_S \mathcal{C}(x_1,...,x_n,u) \wedge \mathcal{C}(x_1,...,x_n,v) \Rightarrow y = z$$

dans le cas de la représentation forte. □

<u>L'opérateur μ</u>. Supposons que pour tous $x_1,...,x_n$ il existe un *y* tel que $g(x_1,...,x_n,y) = 0$ et supposons que *g* est représentable par dans *S* par la formule $\mathcal{D}(x_1,...,x_{n+2})$. Montrons que la fonction

$$f(x_1,...,x_n) = \mu(g(x_1,...,x_n,y) = 0)$$

est représentable dans *S* par la formule $\mathcal{E}(x_1,...,x_{n+1})$:

$$\mathcal{D}(x_1,...,x_{n+1},0) \wedge \forall y(y < x_{n+1} \Rightarrow \neg\mathcal{D}(x_1,...,x_n,y,0)) .$$

Supposons que $f(k_1,...,k_n) = m$. Il s'ensuit que $g(k_1,...,k_n,m) = 0$ et que pour tout $k < m$, $g(k_1,...,k_n,k) \ne 0$. Par la représentabilité de la fonction *g*, nous avons donc que $\vdash_S \mathcal{D}(\overline{k}_1,...,\overline{k}_n,\overline{m},0)$ et $\vdash_S \neg\mathcal{D}(\overline{k}_1,...,\overline{k}_n,\overline{k},0)$, pour $k < m$. Par la proposition 3.8(b') (p. 125), nous avons $\vdash_S \forall y(y < \overline{m} \Rightarrow \neg\mathcal{D}(\overline{k}_1,...,\overline{k}_n,y,0))$ d'où $\vdash_S \mathcal{E}(\overline{k}_1,...,\overline{k}_n,\overline{m})$ en combinant les résultats.

Encore une fois, il suffit de démontrer l'unicité. Supposons que *u* est telle que $\vdash_S \mathcal{D}(\overline{k}_1,...,\overline{k}_n,u,0) \wedge \forall y(y < u \Rightarrow \neg\mathcal{D}(\overline{k}_1,...,\overline{k}_n,y,0))$. Montrons que $\vdash_S \overline{m} = u$ en utilisant le fait que $\vdash_S \overline{m} < u \vee \overline{m} = u \vee \overline{m} > u$. D'abord, $\vdash_S \overline{m} < u$ est impossible car nous avons que $\vdash_S \mathcal{D}(\overline{k}_1,...,\overline{k}_n,\overline{m},0)$. D'autre part, puisque $\vdash_S \forall y(y < \overline{m} \Rightarrow \neg\mathcal{D}(\overline{k}_1,...,\overline{k}_n,y,0))$, nous ne pouvons avoir $\vdash_S u < \overline{m}$. Il faut donc que $\vdash_S \overline{m} = u$. □

4. La fonction beta

Nous voulons définir une fonction arithmétique $\beta(x,y,z)$ avec la propriété suivante : pour toute suite de nombres naturels $a_0,a_1,...,a_n$ (*n* est variable aussi), il existe *a* et *b* tels que

$$\beta(a,b,i) = a_i, \text{ pour } i = 0,1,...,n.$$

Pour ce faire nous aurons besoin du résultat suivant :

Théorème du reste chinois. Soient $m_0, m_1, ..., m_n$ des nombres naturels relativement premiers deux à deux (qui deux à deux n'ont aucun facteur premier en commun) et $a_0, a_1, ..., a_n$ des nombres naturels quelconques. Il existe alors une solution au système suivant de congruences modulo :

$$\begin{cases} x \equiv a_0 \bmod m_0 \\ x \equiv a_1 \bmod m_1 \\ \quad \vdots \\ x \equiv a_n \bmod m_n \end{cases}$$

<u>Remarque</u> : $x \equiv a \bmod m$ si et seulement si m divise $x - a$. On dit que x est congru à a modulo m. Il s'agit d'une relation d'équivalence.

PREUVE. Pour $i = 0,1,...,n$, posons

$$p_i = \prod_{j \neq i} m_j .$$

Nous avons alors que $p_i \equiv 0 \bmod m_j$ lorsque $j \neq i$ et p_i relativement premier de m_i. On peut montrer que si p et m sont relativement premiers, il existe x tel que $px \equiv 1 \bmod m$. Soient $q_1, ..., q_n$ tels que $p_i q_i \equiv 1 \bmod m_i$. Considérons

$$x = \sum_i a_i p_i q_i .$$

Nous avons que $x \equiv \sum_i a_i p_i q_i \equiv a_j p_j q_j \equiv a_j 1 \equiv a_j \bmod m_j$ pour tout $j = 0,1,...,n$, donc x est la solution recherchée. □

Retournons maintenant à la fonction $\beta(x, y, z)$. Soit $a_0, a_1, ..., a_n$ une suite de nombres quelconque. Si nous avions des nombres $m_0, m_1, ..., m_n$ relativement premiers deux à deux et tels que $a_i < m_i$, pour tout $0 \leq i \leq n$, nous pourrions appliquer le théorème du reste chinois pour obtenir un nombre $a = \sum_i a_i p_i q_i$ ayant la propriété suivante : pour chaque $0 \leq i \leq n$, a_i est le reste de la division de a par m_i (car $a_i < m_i$). Il suffirait donc de définir une suite de nombres $m_0, m_1, ..., m_n$ avec les propriétés voulues à partir d'un seul nombre b et nous aurions terminé.

Posons $b = M!$ où $M = \max(n, a_0, a_1, ..., a_n)$. Nous allons montrer que les nombres $m_i = 1 + (i+1)b$, pour $i = 0, ..., n$, sont tous relativement premiers (deux à deux). Pour $0 \leq i < j \leq n$, si un premier p divise m_i et m_j, il divise leur différence $(j - i)b$. Si p divise b, il divise 1 (car il divise $m_i = 1 + (i+1)b$), ce qui est impossible. Il divise donc $j - i$. Mais $j - i \leq M$, donc $j - i$ divise $M! = b$ et par transitivité p diviserait b, ce qui est contradictoire. Les m_i sont donc relativement premiers. Nous sommes donc dans les conditions du théorème du reste chinois. Il existe un nombre *a* tel que

$$a \equiv a_i \bmod m_i\ ,$$

c'est-à-dire que m_i divise $a - a_i$. Puisque a_i est plus petit que m_i, a_i est le reste de la division de *a* par m_i.

Récapitulons. À partir d'une suite $a_0, a_1, ..., a_n$, nous pouvons trouver des nombres *a* et *b* tels que a_i est le reste de la division de *a* par $1+(i+1)b$. Ainsi, nous n'avons qu'à définir $\beta(x, y, z)$ comme

$$\beta(x, y, z) = rm(1+(z+1)y, x)\ ,$$

où $rm(s,t)$ est le reste de la division de *t* par *s*. Nous avons :

Proposition 3.22. Pour toute suite de nombres $a_0, a_1, ..., a_n$, il existe des nombres naturels *a* et *b* tels que $\beta(a,b,i) = a_i$, pour $0 \le i \le n$.

Preuve. La preuve suit immédiatement de la discussion précédente.

Remarque. $\beta(x, y, z)$ est primitivement récursive par la proposition 3.15(n) (p. 135).

5. La représentabilité de la fonction beta

La fonction $\beta(x, y, z)$ est non seulement primitivement récursive, elle est également fortement représentable.

Proposition 3.21. $\beta(x, y, z)$ est fortement représentable dans *S* par la formule $Bt(x_1, x_2, x_3, x_4)$:

$$\exists w(x_1 = (1+(x_3+1)x_2)w + x_4 \wedge x_4 < 1+(x_3+1)x_2)\ .$$

PREUVE. Supposons que $\beta(k_1, k_2, k_3) = k_4$. Nous avons donc que $k_1 = (1+(k_3+1)k_2)k + k_4$ pour un certain *k* et $k_4 < 1+(k_3+1)k_2)$. Ainsi $\vdash_S \overline{k}_1 = (1+(\overline{k}_3+1)\overline{k}_2)\overline{k} + \overline{k}_4$ par la proposition 3.6(a) et $\vdash_S \overline{k}_4 < 1+(\overline{k}_3+1)\overline{k}_2)$ par la proposition 3.6(a) et la représentabilité de « < ». Nous avons donc

$$\vdash_S \overline{k}_1 = (1+(\overline{k}_3+1)\overline{k}_2)\overline{k} + \overline{k}_4 \wedge \overline{k}_4 < 1+(\overline{k}_3+1)\overline{k}_2)$$

et, en introduisant un quantificateur existentiel à la place de *k*, $\vdash_S Bt(\overline{k}_1, \overline{k}_2, \overline{k}_3, \overline{k}_4)$. Enfin, par la proposition 3.11 (p. 128), $\vdash_S \exists_1 x_4 Bt(x_1, x_2, x_3, x_4)$. $\beta(x, y, z)$ est donc fortement représentable par $Bt(x_1, x_2, x_3, x_4)$.

6. La représentabilité des fonctions récursives

Tout ce travail converge vers le théorème suivant :

Proposition 3.23. Toute fonction récursive est représentable dans *S*.

PREUVE. Nous avons vu qu'il restait seulement à montrer que l'opération de récursivité préservait la représentabilité. Supposons que les fonctions $g(x_1,...,x_n)$ et $h(x_1,...,x_n,y,z)$ sont représentables dans *S* par les formules $\mathcal{A}(x_1,...,x_n,x_{n+1})$ et $\mathcal{B}(x_1,...,x_{n+3})$, et soit *f* la fonction

$$f(x_1,...,x_n,0)=g(x_1,...,x_n)$$
$$f(x_1,...,x_n,y+1)=h(x_1,...,x_n,y,f(x_1,...,x_n,y))$$

Remarquons que $f(x_1,...,x_n,y)=z$ si et seulement s'il existe une suite finie de nombres b_0, b_1,..., b_y tels que $b_0=g(x_1,...,x_n)$ et $b_{w+1}=h(x_1,...,x_n,w,b_w)$ pour $w<y$ et $b_y=z$. C'est ici qu'intervient la fonction $\beta(x,y,z)$.

Nous allons montrer que la fonction *f* est représentable dans *S* par la formule $\mathcal{C}(x_1,...,x_{n+2})$:

$$\exists u\exists v\big(\exists w(Bt(u,v,0,w)\wedge\mathcal{A}(x_1,...,x_n,w))\wedge Bt(u,v,x_{n+1},x_{n+2})\wedge$$
$$\forall w(w<x_{n+1}\Rightarrow\exists y\exists z(Bt(u,v,w,y)\wedge Bt(u,v,w',z)\wedge\mathcal{B}(x_1,...,x_n,w,y,z)))\big)$$

Supposons que $f(k_1,...,k_n,p)=m$. Nous voulons montrer que $\vdash_S \mathcal{C}(\overline{k_1},...,\overline{k_n},\overline{p},\overline{m})$. Si $p=0$, alors $m=g(k_1,...,k_n)$. Considérons la suite composée seulement du nombre *m*. Par la proposition 3.22, il existe *a* et *b* tels que $\beta(a,b,0)=m$. Ainsi, par la proposition 3.21

(#) $\quad\vdash_S Bt(\overline{a},\overline{b},0,\overline{m})$.

De même, puisque $m=g(k_1,...,k_n)$, nous avons $\vdash_S \mathcal{A}(\overline{k_1},...,\overline{k_n},\overline{m})$. Ainsi, par E4 (la règle d'introduction pour les quantificateurs existentiels),

(##) $\quad\vdash_S \exists w(Bt(\overline{a},\overline{b},0,w)\wedge\mathcal{A}(x_1,...,x_n,w))$.

Enfin, puisque $\vdash_S w\not<0$, il s'ensuit par une tautologie et la règle de généralisation que

(###) $\quad\vdash_S \forall w(w<0\Rightarrow\exists y\exists z(Bt(\overline{a},\overline{b},w,y)\wedge Bt(\overline{a},\overline{b},w',z)\wedge\mathcal{B}(\overline{k_1},...,\overline{k_n},w,y,z))$.

En appliquant la règle E4 à la conjonction de (#), (##) et (###), nous obtenons $\vdash_S \mathcal{C}(\overline{k_1},...,\overline{k_n},0,\overline{m})$.

Maintenant, si $p>0$, $f(k_1,...,k_n,p)=m$ est calculée en $p+1$ étapes. Soit $r_i=f(k_1,...,k_n,i)$. Pour la suite de nombres $r_0,r_1,...,r_p$, il existe d'après la proposition 3.22 des nombres *a* et *b* tels que $\beta(a,b,i)=r_i$ pour $0\le i\le p$. Par la proposition 3.21, $\vdash_S Bt(\overline{a},\overline{b},\overline{i},\overline{r_i})$. En particulier, $\beta(a,b,0)=r_0=f(k_1,...,k_n,0)=g(k_1,...,k_n)$, ainsi $\vdash_S Bt(\overline{a},\overline{b},0,\overline{r_0})\wedge\mathcal{A}(\overline{k_1},...,\overline{k_n},\overline{r_0})$ et par la règle E4

(|) $\quad\vdash_S \exists wBt(\overline{a},\overline{b},0,w)\wedge\mathcal{A}(\overline{k_1},...,\overline{k_n},w)$.

Par ailleurs, puisque $r_p=f(k_1,...,k_n,p)=m$, nous avons $\beta(a,b,p)=m$. Par conséquent

(||) $\quad \vdash_S Bt(\overline{a}, \overline{b}, \overline{p}, \overline{m})$.

Pour $0 \leq i \leq p-1$, $\beta(a,b,i) = r_i = f(k_1, ..., k_n, i)$ et

$$\beta(a,b,i+1) = r_{i+1} = f(k_1, ..., k_n, i+1) = h(k_1, ..., k_n, i, f(k_1, ..., k_n, i)) = h(k_1, ..., k_n, i, r_i).$$

Ainsi, nous avons que $\vdash_S Bt(\overline{a}, \overline{b}, \overline{i}, \overline{r_i}) \wedge Bt(\overline{a}, \overline{b}, \overline{i}', \overline{r_{i+1}}) \wedge \mathcal{B}(\overline{k_1}, ..., \overline{k_n}, \overline{i}, \overline{r_i}, \overline{r_{i+1}})$ et, par la règle E4, que $\vdash_S \exists y \exists z (Bt(\overline{a}, \overline{b}, \overline{i}, y) \wedge Bt(\overline{a}, \overline{b}, \overline{i}', z) \wedge \mathcal{B}(\overline{k_1}, ..., \overline{k_n}, \overline{i}, y_i, z))$. Enfin, par la proposition 3.8 (b'), nous avons

(|||) $\quad \vdash_S \forall w (w < \overline{p} \Rightarrow \exists y \exists z (Bt(\overline{a}, \overline{b}, \overline{i}, y) \wedge Bt(\overline{a}, \overline{b}, \overline{i}', z) \wedge \mathcal{B}(\overline{k_1}, ..., \overline{k_n}, \overline{i}, y_i, z)))$.

En appliquant la règle E4 deux fois à la conjonction de (|), (||) et (|||), nous avons finalement que $\vdash_S \mathcal{C}(\overline{k_1}, ..., \overline{k_n}, \overline{p}, \overline{m})$, ce qui vérifie la condition (1) de la représentabilité.

Il suffit maintenant de montrer la condition (2). Puisque nous avons déjà démontré l'existence, il suffit de montrer l'unicité, ce que je laisse en exercice. ∎

Nous avons :

Corollaire 3.24. Toute relation récursive est représentable dans *S*.

PREUVE. Soit $R(x_1, ..., x_n)$ une relation récursive. Par définition (p. 137), sa fonction caractéristique C_R est récursive. Par la proposition 3.23, C_R est représentable dans *S*, ce qui entraîne par la proposition 3.12 que *R* est représentable dans *S*. ∎