Fonctions représentables

Il s'agit de justifier que l'arithmétique de Peano permet d'exprimer toutes les fonctions récursives primitives.

Note : Il s'agit d'un chapitre technique. Le lecteur pressé peut juste se concentrer sur le résultat énoncé au début. Cependant, il s'agit aussi d'un chapitre charnière puisqu'on va faire le lien entre la sémantique (le monde des entiers) et la syntaxe (le langage de l'arithmétique de Peano). On y trouve aussi une des prouesses techniques de Gödel : la fonction β. Elle permet de coder une liste quelconque de nombres à l'aide de seulement deux entiers.

1. Un prédicat récursif primitif est représentable

1.1. Prédicat représentable

Pour $p \geqslant 1$ fixé, on note $\mathbf{x} = (x_1, \ldots, x_p)$. Si $\mathbf{n} = (n_1, \ldots, n_p) \in \mathbb{N}^p$, on note $\overline{\mathbf{n}} = (\overline{n}_1, \ldots, \overline{n}_p)$ la suite des numéraux correspondants.

Définition.
Un prédicat $R(\mathbf{x})$ à p places est ***représentable*** s'il existe une formule $\mathcal{P}(\mathbf{x})$ du langage $\mathcal{L}_0$ telle que pour tout $\mathbf{n} \in \mathbb{N}^p$:

- si $R(\mathbf{n})$ est vrai alors : $\quad \mathcal{PA} \vdash \mathcal{P}(\overline{\mathbf{n}})$
- si $R(\mathbf{n})$ est faux alors : $\quad \mathcal{PA} \vdash \neg\mathcal{P}(\overline{\mathbf{n}})$

Remarque : la dénomination complète est « prédicat fortement représentable par la théorie $\mathcal{PA}$ de l'arithmétique de Peano ».
Noter bien le passage d'un entier au numéral ; par exemple si $p = 1$, le prédicat s'évalue en $R(n)$ (avec $n \in \mathbb{N}$), la formule $\mathcal{P}$ s'évalue en $\mathcal{P}(\overline{n})$, avec le numéral $\overline{n} = SSS\ldots S0$ représentant n dans $\mathcal{L}_0$.

Exemple.
Le prédicat $R(x)$: « x est un entier pair » est représentable grâce à la formule suivante :

$$\mathcal{P}(x) \ : \quad \exists y \ \ x = \overline{2} \times y$$

La vérification de cette propriété pour un entier précis est un processus fini, qui peut être traduit pas à pas sous forme de preuve au sein de $\mathcal{PA}$.

1.2. Théorème

Voici le théorème qui sera utile pour la suite des chapitres. Il sera appliqué pour le prédicat « est_preuve(N, n) » qui détermine si les formules du super-nombre de Gödel N forment bien une preuve de la formule de nombre de Gödel n.

Théorème 1.
Si R est un prédicat récursif primitif, alors R est représentable.

On rappelle qu'un prédicat est récursif primitif si sa fonction caractéristique est récursive primitive. De même, un prédicat sera représentable si sa fonction caractéristique est représentable. Dans la suite, on va donc définir et étudier cette notion plus générale de fonction représentable, indispensable pour démontrer le théorème ci-dessus.

2. Fonctions représentables

2.1. Définition

Définition.
Une fonction $f : \mathbb{N}^p \to \mathbb{N}$ est ***représentable*** s'il existe une formule $\mathcal{P}(\mathbf{x}, y)$ telle que pour tout $\mathbf{n} = (n_1, \ldots, n_p) \in \mathbb{N}^p$, on ait :

$$\mathcal{PA} \quad \vdash \quad \forall y \quad \left[\mathcal{P}(\overline{\mathbf{n}}, y) \leftrightarrow y = \overline{f(\mathbf{n})}\right]$$

Remarques :

- La terminologie complète est « fonction fortement représentable par la théorie $\mathcal{PA}$ ».
- Encore une fois, cette définition fait le lien entre un entier $k \in \mathbb{N}$ et son numéral $\overline{k}$ dans $\mathcal{L}_0$.
- Il faut comprendre la formule $\mathcal{P}$ comme le graphe de f. C'est une façon équivalente de définir la fonction.

> **Exemple.**
> La fonction $f : \mathbb{N} \to \mathbb{N}$ définie par $f(x) = 2x + 1$ est représentable. En effet, considérons la formule :
>
> $$\mathcal{P}(x, y) \ : \ y = 2x + 1$$
>
> Il est donc exact (et démontrable dans l'arithmétique de Peano) que $\mathcal{P}(x, y)$ est vérifiée ssi $y = f(x)$. Autrement dit, quel que soit $n \in \mathbb{N}$, $\mathcal{P}(n, y)$ est vrai ssi $y = f(n)$.
> Mais attention, on n'a pas tout à fait construit l'expression dans le langage $\mathcal{L}_0$. En effet, l'entier 2 n'existe pas, il faut l'écrire $\overline{2} = SS0$. La bonne formule de $\mathcal{L}_0$ est donc :
>
> $$\mathcal{P}(x, y) \ : \ y = S(SS0 \times x)$$
>
> Et l'équivalence est, quel que soit $n \in \mathbb{N}$:
>
> $$\forall y \quad \left[\mathcal{P}(\overline{n}, y) \leftrightarrow y = \overline{f(n)}\right]$$
>
> (où $\overline{n} = SS\ldots S0$ est le numéral de l'entier n et $\overline{f(n)} = SS\ldots S0$ est le numéral de l'entier $f(n)$).
> C'est donc bien un passage du monde des entiers au langage $\mathcal{L}_0$.

2.2. Définition équivalente

Afin de mieux comprendre la définition de fonction représentable, voici une définition équivalente.

Définition.
Une fonction $f : \mathbb{N}^p \to \mathbb{N}$ est une fonction ***représentable*** s'il existe une formule $\mathcal{P}(\mathbf{x}, y)$ telle que pour tout $\mathbf{n} \in \mathbb{N}^p$ et en posant $m = f(\mathbf{n})$, on ait :

1. $\mathcal{PA} \vdash \mathcal{P}(\overline{\mathbf{n}}, \overline{m})$ *exactitude*
2. $\mathcal{PA} \vdash \forall y \ \left[\mathcal{P}(\overline{\mathbf{n}}, y) \rightarrow y = \overline{m}\right]$ *unicité*

L'exactitude signifie que la formule $\mathcal{P}$ permet bien de retrouver la valeur m de $f(\mathbf{n})$. L'unicité est indispensable, car une fonction ne peut bien sûr prendre qu'une seule valeur.
Justifions que cette seconde définition est équivalente à la première. Dans la définition originale, on a une équivalence. L'unicité est exactement l'implication $\rightarrow$. Partons de la définition originale, en spécialisant le $\forall$ en $y = \overline{m}$, on obtient exactement $\mathcal{P}(\overline{\mathbf{n}}, \overline{m})$. Réciproquement, en partant de la seconde définition, on a $\mathcal{P}(\overline{\mathbf{n}}, \overline{m})$ ce qui implique que $y = \overline{m} \rightarrow \mathcal{P}(\overline{\mathbf{n}}, y)$. On introduit alors le $\forall y$ pour obtenir l'implication inverse ($\leftarrow$).
On verra en exercice des contre-exemples de formules ne satisfaisant pas l'exactitude ou l'unicité.

2.3. Prédicat représentable

Revenons sur la notion de prédicat représentable.

Proposition 1.
Un prédicat $R(\mathbf{x})$ est un prédicat représentable si et seulement si sa fonction caractéristique $\chi_R(\mathbf{x})$ est une fonction représentable.

On rappelle que par définition $\chi_R(\mathbf{x}) = 1$ si $R(\mathbf{x})$ est vrai, et $\chi_R(\mathbf{x}) = 0$ sinon.
Pour simplifier l'écriture des preuves, ici et souvent dans la suite, on écrira les preuves avec le minimum de variables possibles, par exemple avec $p = 1$. Pour obtenir la preuve générale, il suffirait bien sûr de changer x en $\mathbf{x}$ et n en $\mathbf{n}$. De plus, on écrira à la fois n pour l'entier et son numéral $\overline{n}$ car il n'y a pas d'ambiguïté.
La preuve suivante est assez technique et peut être passée en première lecture.

Démonstration.

- $\Rightarrow$
  Hypothèse : χ_R est une fonction représentable.
  But : R est un prédicat représentable.
  Notons $\mathcal{P}(x, y)$ la formule issue de l'hypothèse et définissons $\mathcal{P}_1(x)$ par $\mathcal{P}(x, 1)$. Dans la formule issue de l'hypothèse « χ_R est une fonction représentable », on pose $y = 1$ et on obtient l'équivalence :
  $$\mathcal{PA} \vdash \left[\mathcal{P}(n, 1) \leftrightarrow 1 = \chi_R(n)\right]$$
  — Si $R(n)$ est vrai, alors $\chi_R(n) = 1$. Donc $1 = \chi_R(n)$ est vrai. Donc, par l'équivalence, $\mathcal{P}_1(n)$ est vrai aussi. Plus précisément, $\mathcal{PA} \vdash (\mathcal{P}_1(n) \leftrightarrow (1 = 1))$. Donc, par définition de l'implication, on obtient : $\mathcal{PA} \vdash \mathcal{P}_1(n)$.
  — Si $R(n)$ est faux, alors $\chi_R(n) = 0$, donc, par l'équivalence, c'est $\neg\mathcal{P}_1(n)$ qui est vrai.
  Ainsi, le prédicat R est bien représentable par la formule $\mathcal{P}_1$.
- $\Leftarrow$
  Hypothèse : R est un prédicat représentable.
  But : χ_R est une fonction représentable.
  L'hypothèse nous donne une formule $\mathcal{P}_0(x)$ associée au prédicat R. On construit alors la formule $\mathcal{P}(x, y)$ pour la fonction χ_R ainsi :
  $$\mathcal{P}(x, y) \ : \quad \big(\mathcal{P}_0(x) \wedge (y = 1)\big) \vee \big(\neg\mathcal{P}_0(x) \wedge (y = 0)\big)$$
  Nous devons vérifier que cette formule fait bien de χ_R une fonction représentable.
  Exactitude. Fixons un entier n et posons $m = \chi_R(n)$, qui vaut donc 0 ou 1.
  — Si $m = 1$, alors $R(n)$ est vrai, donc par hypothèse $\mathcal{PA} \vdash \mathcal{P}_0(n)$. Donc $\mathcal{PA} \vdash \mathcal{P}_0(n) \wedge (m = 1)$, c'est-à-dire $\mathcal{PA} \vdash \mathcal{P}(n, m)$.
  — Si $m = 0$, alors $R(n)$ est faux et on obtient de manière similaire $\mathcal{PA} \vdash \mathcal{P}(n, m)$.

Dans tous les cas, on a bien vérifié la condition d'exactitude.

Unicité. Pour l'unicité, on doit justifier que, quel que soit y : $\mathcal{PA} \vdash \mathcal{P}(n,y) \to y = m$.
— Cas $y \neq 0$ et $y \neq 1$. Alors $\mathcal{P}(n,y)$ est faux, donc l'implication est vérifiée.
— Cas $y = 1$.
  — Si $R(n)$ est vrai, alors $\mathcal{PA} \vdash \mathcal{P}_0(n)$. Donc $\mathcal{PA} \vdash \mathcal{P}_0(n) \wedge (y = 1)$. Ainsi $\mathcal{PA} \vdash \mathcal{P}_0(n) \wedge (y = 1) \wedge (y = \chi_R(n))$, donc $\mathcal{PA} \vdash (\mathcal{P}(n,1) \to y = m)$ (car les deux assertions de part et d'autre de l'implication sont vraies).
  — Si $R(n)$ est faux, alors $\mathcal{PA} \vdash \neg\mathcal{P}_0(n)$ donc $\mathcal{P}(x,y)$ est faux, donc l'implication est vraie.
— Cas $y = 0$. Similaire au cas précédent.

□

2.4. Exemples importants

Le but du chapitre est de prouver que toutes les fonctions récursives primitives sont représentables. La stratégie a déjà été rencontrée : il suffit de le démontrer pour les trois fonctions de base, puis de montrer que cette propriété est stable par les opérations de composition et de récurrence.

Proposition 2.
Les fonctions de base Z, S et les projections P_i^p sont des fonctions représentables.

Démonstration. Il n'y a pas vraiment grand-chose à prouver. Il s'agit juste de donner la formule $\mathcal{P}(\mathbf{x}, y)$ qui convient.

- Prenons l'exemple de la fonction successeur S, définie par $S(n) = n+1$. On pose $\mathcal{P}(x,y) \ : \ y = S(x)$ (qui est une formule de $\mathcal{L}_0$).
  Pour $n \in \mathbb{N}$ fixé, et en notant $m = S(n) = n+1$, on a bien :
  $$\mathcal{P}(\overline{n}, y) \quad \leftrightarrow \quad y = S(\overline{n}) \quad \leftrightarrow \quad y = \overline{S(n)} \quad \leftrightarrow \quad y = \overline{m}$$
  Ces équivalences sont vraies dans tout système logique, pas besoin des axiomes de Peano. Ainsi S est une fonction représentable.
- Pour la fonction zéro Z, la formule est $\mathcal{P}(x,y) \ : \ y = 0$.
- Pour la projection P_i^p, la formule est $\mathcal{P}(\mathbf{x}, y) \ : \ y = x_i$.

□

Proposition 3.
Soient $f_1, \dots, f_q : \mathbb{N}^p \to \mathbb{N}$ et $g : \mathbb{N}^q \to \mathbb{N}$ des fonctions représentables. Alors $h = g(f_1, \dots, f_q)$ est aussi représentable.

Ainsi l'opération de composition est stable pour la propriété de représentabilité. Si on prouve qu'il en est de même pour l'opération de récurrence, on aura le résultat souhaité. Cependant, cette dernière stabilité sera beaucoup plus difficile à obtenir et nous occupera le reste du chapitre.
Pour l'instant, on se concentre sur la preuve de la proposition ci-dessus. Comme on l'a déjà dit, on donnera la preuve dans un cadre minimaliste, mais il est intéressant de commenter la formule générale qui fait de h une fonction représentable :

$$\mathcal{P}(\mathbf{x}, y) \ : \ \exists w_1 \dots \exists w_q \quad \mathcal{P}_0(w_1, \dots, w_q, y) \wedge \mathcal{P}_1(\mathbf{x}, w_1) \wedge \dots \wedge \mathcal{P}_q(\mathbf{x}, w_q)$$

où $\mathcal{P}_0$ est la formule associée à la fonction représentable g et $\mathcal{P}_i$ la formule de f_i $(i = 1, \dots, q)$. Le rôle des variables w_i est très intéressant : il s'agit de mémoriser le résultat intermédiaire du calcul $w_i = f_i(\mathbf{n})$, afin de pouvoir l'injecter dans g pour calculer $h(\mathbf{n}) = g(w_1, \dots, w_q) = g(f_1(\mathbf{n}), \dots, f_q(\mathbf{n}))$.

Démonstration. On fait la preuve seulement dans le cas $p = 1$ et $q = 1$. Soit $f_1 : \mathbb{N} \to \mathbb{N}$ une fonction représentable, représentée par la formule $\mathcal{P}_1(x,w)$. Soit $g : \mathbb{N} \to \mathbb{N}$ une fonction représentable, représentée par la formule $\mathcal{P}_0(w,y)$. On veut montrer que la composition $h = g \circ f_1 : \mathbb{N} \to \mathbb{N}$ est représentable.

On définit la formule :

$$\mathcal{P}(x,y) \ : \quad \exists w \ \ \mathcal{P}_0(w,y) \wedge \mathcal{P}_1(x,w)$$

qui va représenter la fonction h. Pour $n \in \mathbb{N}$, posons $k = f_1(n)$ et $m = g(k) = g(f_1(n)) = h(n)$.

- **Exactitude.** Par hypothèse, on a $\mathcal{PA} \vdash \mathcal{P}_0(k,m)$ et $\mathcal{PA} \vdash \mathcal{P}_1(n,k)$. Donc $\mathcal{PA} \vdash \exists w \left(\mathcal{P}_0(w,m) \wedge \mathcal{P}_1(n,w)\right)$ (il suffit de prendre $w = k$). Donc $\mathcal{PA} \vdash \mathcal{P}(n,m)$.
- **Unicité.** $\mathcal{PA}$ prouve par hypothèse les deux implications suivantes :

$$\forall w \ \ \left(\mathcal{P}_1(n,w) \to w = k\right)$$

$$\text{et} \quad \forall y \ \left(\mathcal{P}_0(k,y) \to y = m\right)$$

Ainsi, supposons qu'on ait $\mathcal{P}(n,y)$. Donc il existe w tel que $\mathcal{P}_0(w,y)$ et $\mathcal{P}_1(n,w)$. Comme on a $\mathcal{P}_1(n,w)$, alors $w = k$. On a donc $\mathcal{P}_0(k,y)$, ce qui implique $y = m$. Ainsi on a bien vérifié la condition d'unicité : $\mathcal{P}(n,y) \to y = m$.

□

Proposition 4.
La fonction reste, qui à a et b associe le reste $\text{reste}(b,a)$ de la division euclidienne de b par a, est représentable.

Démonstration. La formule est :

$$\mathcal{P}(a,b,r) \ : \quad \left[a = 0 \wedge b = r\right] \vee \left[\exists q \leqslant b \quad (b = qa + r) \wedge (r < a)\right]$$

On prouve l'exactitude et l'unicité. En effet l'arithmétique de Peano prouve l'existence et l'unicité de la division euclidienne. En fait, ce serait aussi vrai dans l'arithmétique $\mathcal{Q}$ de Robinson, donc sans utiliser la récurrence.
Remarque : « $\exists q \leqslant b \ \ \mathcal{P}$ » signifie « $\exists q \ \ (q \leqslant b) \wedge \mathcal{P}$ ». □

3. La fonction β de Gödel

Le but de cette section est d'étudier la fonction β de Gödel. C'est une construction astucieuse qui permet de stocker une liste quelconque d'entiers $(n_1, \ldots, n_l)$ à l'aide de seulement deux entiers a et b.
Cette construction joue le rôle de mémoire. En effet, pour calculer une suite par récurrence, il faut calculer $u_1, u_2, \ldots, u_{l-1}$ avant de pouvoir calculer u_l.

3.1. Théorème

Théorème 2.
Il existe une fonction $\beta : \mathbb{N}^3 \to \mathbb{N}$ qui est récursive primitive, représentable et telle que, pour tout entier l et toute suite $(n_1, \ldots, n_l)$ d'entiers, il existe $a, b \in \mathbb{N}$ tels que :

$$\beta(a,b,i) = n_i \qquad \text{pour } i = 1, \ldots, l.$$

La fonction β est au final assez simple, car $\beta(a,b,i)$ sera le reste de la division euclidienne de b par $a \times i + 1$. Ce qui est délicat, c'est d'expliquer l'existence de ces a et b. Pour cela, on aura besoin d'un théorème bien connu d'arithmétique.

3.2. Théorème des restes chinois

Théorème 3 (Théorème des restes chinois)**.**
Soient $a_1, \ldots, a_l$ des entiers premiers entre eux deux à deux. Soient $n_1, \ldots, n_l$ des entiers quelconques. Il existe $x \in \mathbb{N}$ tel que pour tout $i = 1, \ldots, l$, on ait :

$$x \equiv n_i \pmod{a_i}$$

Pour deux entiers, cela s'énonce ainsi :

Théorème 4.
Soient a et b des entiers premiers entre eux. Pour tous $\alpha, \beta \in \mathbb{N}$, il existe $x \in \mathbb{N}$ tel que :

$$\begin{cases} x \equiv \alpha \pmod{a} \\ x \equiv \beta \pmod{b} \end{cases}$$

D'un point de vue algébrique, on a même un isomorphisme de groupes :

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Démonstration. On définit :

$$\phi : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

par $\phi(\overline{x}^{ab}) = (\overline{x}^{a}, \overline{x}^{b})$ où l'on note $\overline{x}^{m}$ la classe de l'entier x modulo m.

- ϕ est bien définie. En effet, si $\overline{x}^{ab} = \overline{y}^{ab}$ alors $x = y + kab$, donc $\overline{x}^{a} = \overline{y}^{a}$ et $\overline{x}^{b} = \overline{y}^{b}$. Donc $\phi(\overline{x}^{ab}) = \phi(\overline{y}^{ab})$.
- ϕ est un morphisme de groupes : $\phi(\overline{x}^{ab} + \overline{y}^{ab}) = \phi(\overline{x}^{ab}) + \phi(\overline{y}^{ab})$.
- ϕ est injective. Si $\phi(\overline{x}^{ab}) = (\overline{0}^{a}, \overline{0}^{b})$ alors $\overline{x}^{a} = \overline{0}^{a}$ donc $x = k_1 a$, et $\overline{x}^{b} = \overline{0}^{b}$ donc $x = k_2 b$. Ainsi $k_1 a = k_2 b$. En particulier, b divise $k_1 a$. Or, par hypothèse, a et b sont premiers entre eux, donc d'après le lemme de Gauss b divise k_1, donc $k_1 = k_3 b$. Ainsi $x = k_1 a = k_3 ba$. Donc x est un multiple de ab et la classe $\overline{x}^{ab}$ est $\overline{0}^{ab}$. Ainsi l'application ϕ est injective.
- Comme les cardinaux des ensembles de départ et d'arrivée sont égaux (à ab), l'application est bijective.
- Ainsi, pour (α, β) donné, il existe un antécédent x par ϕ, ce qui dit exactement que :

$$\begin{cases} x \equiv \alpha \pmod{a} \\ x \equiv \beta \pmod{b} \end{cases}$$

□

3.3. Preuve

Construction de a et b. On se donne $n_1, \ldots, n_l \in \mathbb{N}$. On choisit $m \in \mathbb{N}$ tel que $m \geqslant l$ et $m! \geqslant n_i$ $(i = 1, \ldots, l)$. On pose $a = m!$. L'autre entier b sera construit à l'aide du théorème des restes chinois.

- Les entiers $ai+1$ sont premiers entre eux deux à deux. En effet, si p est un nombre premier qui divise $ai+1$ et $aj+1$ (avec $i < j$), alors par différence $p|a(j-i)$. Donc $p|a$ ou $p|(j-i)$. Or $j - i < l \leqslant m$ et $a = m!$ donc dans tous les cas, $p \leqslant m$. Cela entraîne $p|m!$ (c'est-à-dire $p|a$), mais comme $p|ai+1$ alors $p|1$. Contradiction.
- On a $ai + 1 > n_i$ car $n_i \leqslant m! = a$ $(i = 1, \ldots, l)$.
- Par le théorème des restes chinois, il existe $b \in \mathbb{N}$ tel que :

$$b \equiv n_i \pmod{ai+1} \quad \text{quel que soit } i = 1, \ldots, l$$

Construction de β. Cela justifie la construction de β : $\beta(a, b, i)$ est le reste de la division euclidienne de b par $ai + 1$. En effet, ce reste est caractérisé par $b \equiv n_i \pmod{ai+1}$ et $n_i < ai + 1$ comme ci-dessus.

β est récursive primitive. La première partie nous assure que ce codage existe même s'il est un peu compliqué. Cependant, le décodage reste simple :

$$\beta(a, b, i) = \text{reste}(b, ai + 1)$$

Ce reste est bien donné par une fonction récursive primitive. En effet :

$$\text{reste}(b, a) = \min\{r \leqslant b \mid \exists q \leqslant b \quad b = qa + r\}$$

La condition « $\exists q \leqslant b \quad b = qa + r$ » est bien un prédicat récursif primitif car la quantification est bornée. Donc le reste l'est aussi car il est obtenu par minimisation bornée. La borne sur le minimum n'est pas

naturelle, car en général $r < a$ dans une division euclidienne, mais cette borne b permet d'englober le cas exceptionnel $a = 0$.

β est représentable. La formule à considérer est :

$$\mathcal{B}(a,b,i,r) \ : \quad \big(\exists q \leqslant b \quad b = q(ai+1)+r\big) \wedge \big(r < ai+1\big)$$

Autrement dit, r est défini comme le reste de la division euclidienne de b par $ai+1$. On a vu que la fonction reste est représentable.
Abus de notation : a, b, i, r ne sont pas des variables du langage $\mathcal{L}_0$, elles devraient être remplacées par $x_1, x_2, \ldots$, mais les formules deviendraient moins lisibles.

Note. L'intérêt du codage par la fonction β est de n'utiliser que des additions et des multiplications, qui sont les seules opérations autorisées par le langage $\mathcal{L}_0$.
Sinon, pour coder une suite d'entiers, on aurait pu choisir le codage $2^{n_1}3^{n_2}5^{n_3}\ldots$ avec les nombres premiers. Mais dans $\mathcal{L}_0$, on n'a pas encore le droit de calculer des puissances : par exemple, pour calculer x^n, on calcule successivement $x, x^2, x^3 \ldots$ jusqu'à x^n. On a donc besoin de l'opération de récurrence, autrement dit, il faut pouvoir mettre en mémoire les résultats intermédiaires. Mais on ne sait pas encore que l'opérateur de récurrence préserve la représentabilité, puisque c'est exactement ce que l'on souhaite démontrer.
Une fois qu'on aura la représentabilité des fonctions récursives primitives grâce à la fonction β, on pourra utiliser des listes (finies) de nombres pour le codage de Gödel dans le langage $\mathcal{L}_0$.

4. Les fonctions récursives primitives sont représentables

Attaquons-nous à l'objectif final du chapitre.

Théorème 5.
Toute fonction $f : \mathbb{N}^p \to \mathbb{N}$ qui est récursive primitive est représentable.

4.1. Opération de récurrence

Pour prouver que les fonctions récursives primitives sont représentables, il reste donc à démontrer la stabilité de la représentabilité par l'opération de récurrence.

Proposition 5.
Soient $g : \mathbb{N}^p \to \mathbb{N}$ et $h : \mathbb{N}^{p+2} \to \mathbb{N}$ deux fonctions représentables. La fonction $f : \mathbb{N}^{p+1} \to \mathbb{N}$ définie par l'initialisation g et la relation de récurrence h est une fonction représentable.

Cette proposition entraîne le théorème ci-dessus, car on a déjà montré que les trois fonctions de base Z, S, P_i^p étaient représentables et que la composition préservait la représentabilité.

4.2. La formule

On va faire la preuve dans le cas $p = 1$ afin d'avoir l'écriture la plus simple possible.

- $g : \mathbb{N} \to \mathbb{N}$ représentable par $\mathcal{P}_g(x,u)$.
- $h : \mathbb{N}^3 \to \mathbb{N}$ représentable par $\mathcal{P}_h(x,y,u,v)$.
- $f : \mathbb{N}^2 \to \mathbb{N}$ définie par $f(x,0) = g(x)$ et $f(x,y+1) = h(x,y,f(x,y))$.

Le but est de trouver une formule qui représente f. Cette formule $\mathcal{P}_f(x,y,z)$ est : « il existe une suite finie (encodée par des entiers a et b), dont le premier terme est $z_0 = g(x)$, chaque transition respecte la relation de récurrence $z_{i+1} = h(x,i,z_i)$ et dont le dernier terme est $z_y = z$ ».

Il faut transcrire cette phrase dans $\mathcal{L}_0$. Pour cela on utilise la fonction β de Gödel. On va faire une modification mineure afin d'avoir une bonne indexation : on suppose maintenant que $\beta(a,b,i)$ encode une suite $n_0, n_1, n_2, \ldots$ (les indices partent de 0). On a vu que la fonction β est représentable, on note $\mathcal{B}(a,b,i,r)$ la formule correspondante. On rappelle que la fonction β a pour rôle de mémoriser une liste de nombres qui seront ici les termes z_i de la suite.
Voici la formule $\mathcal{P}_f$ dans le langage $\mathcal{L}_0$:

$$\mathcal{P}_f(x,y,z) \ : \quad \exists a\ \exists b \quad \text{Init}(a,b,x) \wedge \text{Trans}(a,b,x,y) \wedge \mathcal{B}(a,b,y,z)$$

On fixe x (cette variable x ne sert en fait à rien), on pose $z_0 = g(x)$, $z_1 = h(x,0,z_0)$, $z_2 = h(x,1,z_1), \ldots$ et le but est de calculer z_y afin de vérifier que c'est bien la valeur $z = f(x,y)$.
Avec $\mathcal{B}$ la formule associée à la fonction β de Gödel, les trois parties de la formule $\mathcal{P}_f$ sont définies ainsi :

- $\text{Init}(a,b,x)$: $\quad \exists u \quad \mathcal{B}(a,b,0,u) \wedge \mathcal{P}_g(x,u)$
  Ainsi on a $u = \beta(a,b,0)$ (le premier terme dans la mémoire) et en même temps $u = g(x)$, donc on a $z_0 = g(x) = \beta(a,b,0)$.
- $\text{Trans}(a,b,x,y)$: $\quad \forall i < y \quad \exists u\ \exists v \quad \mathcal{B}(a,b,i,u) \wedge \mathcal{B}(a,b,i+1,v) \wedge \mathcal{P}_h(x,i,u,v)$
  Les conjonctions donnent : $u = \beta(a,b,i)$ et $v = \beta(a,b,i+1)$ et $v = h(x,i,u)$. Ainsi si $z_i = \beta(a,b,i) = u$ alors $z_{i+1} = h(x,i,z_i) = h(x,i,u) = v = \beta(a,b,i+1)$. Ainsi par le principe de récurrence on a $z_i = \beta(a,b,i)$ pour tout $i \leqslant y$.
- $\mathcal{B}(a,b,y,z)$ signifie que $z = \beta(a,b,y)$ c'est-à-dire $z = z_y$.

4.3. Exactitude

On considère n (pour la variable x), l (pour la variable y) et $m = f(n,l)$ (pour la variable z). L'exactitude signifie que $\mathcal{PA} \vdash \mathcal{P}_f(n,l,m)$.
Cette fois on note $z_0 = g(n)$ et $z_{i+1} = h(n,i,z_i)$ pour $i = 0, \ldots, l-1$. But final : montrer que $m = z_l$.
On sait qu'il existe a, b qui encodent la suite et vérifient $\beta(a,b,i) = z_i$ pour $i = 0, \ldots, l$.

- On a $\beta(a,b,0) = z_0$, on a donc $\mathcal{PA} \vdash \mathcal{B}(a,b,0,z_0) \wedge \mathcal{P}_g(n,z_0)$. Donc en posant $u = z_0$, on a $\mathcal{PA} \vdash \text{Init}(a,b,n)$.
- Ensuite pour z_{i+1}, on pose $u = z_i$ et $v = z_{i+1}$, on a :
  $$\mathcal{B}(a,b,i,z_i) \wedge \mathcal{B}(a,b,i+1,z_{i+1}) \wedge \mathcal{P}_h(n,i,z_i,z_{i+1})$$
  Ceci pour $i = 0, \ldots, l-1$, donc $\mathcal{PA} \vdash \text{Trans}(a,b,n,l)$.
- Enfin $z_l = h(n,l-1,z_{l-1})$ donc $z_l = \beta(a,b,l) = f(n,l) = m$ et ainsi on a $\mathcal{B}(a,b,l,m)$.

4.4. Unicité

Il s'agit de démontrer que :

$$\mathcal{PA} \quad \vdash \quad \forall z \ \ \mathcal{P}_f(n,l,z) \to z = m$$

c'est-à-dire $z = z_l$.
Par récurrence sur l :

- Au rang 0 : La formule $\mathcal{P}_f(n,0,z)$ (avec $m = f(n,0) = g(n) = z_0$) se réduit à :
  $$\exists a\ \exists b \quad \text{Init}(a,b,n) \wedge \mathcal{B}(a,b,0,z)$$
  (car la condition « $\forall i < 0$ » est vide, donc le prédicat Trans est vrai). Donc $z_0 = \beta(a,b,0) = z$, d'où $z = m$ comme voulu.
- Hérédité. Fixons i avec $0 \leqslant i < l$ et supposons :
  $$\forall z \quad \mathcal{P}_f(n,i,z) \to z = z_i$$
  Soit z quelconque. Supposons $\mathcal{P}_f(n,i+1,z)$ vraie. Dans la formule $\mathcal{P}_f(n,i+1,z)$ est incluse la sous-formule $\mathcal{P}_f(n,i,v)$ donc par hypothèse de récurrence $v = z_i$. Mais on a en plus :
  $$\mathcal{B}(a,b,i,u) \wedge \mathcal{B}(a,b,i+1,v) \wedge \mathcal{P}_h(n,i,u,v) \wedge \mathcal{B}(a,b,i+1,z)$$

ce qui prouve dans l'ordre : $u = \beta(a,b,i) = z_i$, $v = \beta(a,b,i+1)$, $v = h(n,i,u) = h(n,i,z_i) = z_{i+1}$ et $z = \beta(a,b,i+1)$. On en déduit donc que $z = z_{i+1}$.

- Par le principe de récurrence (dans $\mathcal{PA}$), l'assertion est vraie pour tous les $i \leqslant l$, donc l'unicité est démontrée.

Remarque. Il est possible de tout faire dans l'arithmétique $\mathcal{Q}$ de Robinson, car en fait notre récurrence se limite à un nombre fini d'étapes (car l est fixé).
Cela termine la preuve que, pour les fonctions récursives primitives, l'opération de récurrence préserve la propriété d'être une fonction représentable.

4.5. Application aux prédicats

On savait que les trois fonctions récursives primitives de base étaient représentables, et que l'opération de composition préservait la représentabilité. On vient de terminer la preuve difficile que pour l'opération de récurrence on a aussi la stabilité de la représentabilité. Par définition de ce qu'est une fonction récursive primitive, on en déduit le Théorème 5 « Toutes les fonctions récursives primitives sont représentables. »
En particulier, on sait qu'un prédicat est représentable ssi sa fonction caractéristique l'est. Donc on a le Théorème 1 annoncé au tout début « Tout prédicat récursif primitif est représentable. »