Corrigé (?) du TD 10

Commençons par rappeler l'énoncé. Je tenterai ensuite de répondre aux questions de l'exercice et aux problèmes qui s'étaient posés lors de la dernière séance de TD de la manière la plus claire possible.

On considère l'arithmétique de Peano, notée PA, qui est une théorie d'un langage $\mathcal{L}$.
On dit qu'un ensemble $A \subseteq \mathbb{N}$ est *exprimable* s'il existe un prédicat arithmétique $H(n)$ tel que

$$\forall n \in \mathbb{N} \qquad H(\overline{n}) \iff n \in A$$

On parlera également, par une généralisation évidente, de prédicats ou de fonctions n-aires *exprimables*.
On se donne une fonction bijective g, de l'ensemble des mots (qu'ils soient des formules bien formées ou non) de $\mathcal{L}$ dans $\mathbb{N}$; $g(\psi)$ est appelé le *numéro de Gödel* de ψ. On note ψ_n la formule vérifiant $g(\psi_n) = n$. On définit une fonction injective d de $\mathbb{N}$ dans $\mathbb{N}$, qui à n associe le numéro de Gödel de $\psi_n(\bar{n})$, si ψ_n est une formule à une variable libre.
Pour A une partie de $\mathbb{N}$, on note $\tilde{A}$ son complémentaire et A^* l'image réciproque de A par d.

1. Montrer que si A est exprimable, alors $\tilde{A}$ l'est aussi.

Pas de problème : si A est exprimable par $H(n)$, alors $\tilde{A}$ est exprimable par $\neg H(n)$.

2. Montrer que les fonctions récursives sont exprimables.

Commençons par préciser ce que l'on entend pas « fonction exprimable ». Une fonction $f : \mathbb{N}^k \to \mathbb{N}$ est exprimable s'il existe une formule du langage de l'arithmétique $H(x_1, x_2, \ldots, x_k, y)$ telle que

$$\forall x_1, \ldots, x_k, y \in \mathbb{N} \qquad H(\overline{x_1}, \ldots, \overline{x_k}, \overline{y}) \iff f(x_1, \ldots, x_k) = y$$

Prouver que les fonctions récursives sont exprimables se fait bien entendu par induction. Commençons par les fonctions de base : les constantes, les projections et la fonction successeur.

- Si l'on note $\tilde{a} : \begin{pmatrix} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & a \end{pmatrix}$, on a

$$\forall x, y \in \mathbb{N} \qquad y = \overline{a} \iff \tilde{a}(x) = y$$

-

$$\forall x, y \in \mathbb{N} \qquad \overline{y} = S\overline{x} \iff y = \text{succ}(x)$$

- Si l'on note $p_k^n : \begin{pmatrix} \mathbb{N}^n & \to & \mathbb{N} \\ (x_1, \ldots, x_n) & \mapsto & x_k \end{pmatrix}$, on a

$$\forall x_1, \ldots, x_n, y \in \mathbb{N} \qquad \overline{y} = \overline{x_k} \iff p_k^n(x_1, \ldots, x_n) = y$$

Maintenant pour la composition. Supposons que $f : \mathbb{N}^n \to \mathbb{N}$ et $g_1, \ldots, g_n : \mathbb{N}^k \to \mathbb{N}$ soient toutes exprimables, repectivement par les formules $F, G_1, \ldots, G_n$. Alors $f \circ (g_1, \ldots, g_n)$ est exprimable par la formule

$$H(x_1, \ldots, x_k, y) \equiv \exists z_1 G_1\left(x_1, \ldots, x_k\right) \wedge \ldots \wedge \exists z_n G_n\left(x_1, \ldots, x_k\right) \wedge F\left(z_1, \ldots, z_n, y\right)$$

Passons ensuite à la minimisation. Supposons $f : \mathbb{N}^{n+1} \to \mathbb{N}$ exprimable. Rappelons que le schéma de minimisation nous assure que la fonction μf, qui à $(x_1, \ldots, x_n)$ associe, s'il existe, le plus petit t tel que $f(x_1, \ldots, x_n, t) = 0$ et pour tout $s < t$, f est définie en $(x_1, \ldots, x_n, s)$. Soit F une formule exprimant f ; alors la formule suivante exprime μf :

$$G(x_1, \ldots, x_n, t) \equiv F(x_1, \ldots, x_n, t, 0) \wedge \forall s \ (s < t \Rightarrow \exists z \ F(x_1, \ldots, x_n, s, z))$$

Enfin le plat de résistance : la récurrence. Commençons par résoudre une question qui s'était posée lors du TD : non, on ne peut pas définir la multiplication dans le langage de l'arithmétique réduit à (S,+). En effet, si l'on ôte de l'arithmétique de Peano le symbole de multiplication, on obtient ce que l'on appelle l'arithmétique de Presburger, qui est connue pour être complète (mais peu puissante, bien entendue), ce qui, modulo le théorème d'incomplétude de Gödel, montre que l'on ne peut pas définir la multiplication dans cette théorie.
Il nous manquait, la dernière fois, la possibilité de parler de suite d'entiers... c'est pour ça que Dieu, je veux dire Gödel, a inventé la fonction β, ainsi définie :

$$\beta(x, y, i) = x \mod (y(i+1)+1)$$

Je vous laisse vérifier que β est exprimable, mettons par F_β. Cette fonction possède la remarquable propriété suivante : pour toute suite finie d'entiers $(s_1, \ldots, s_n)$, il existe x et y tels que $\beta(x, y, 0) = n$ et pour tout $i \in \{1, \ldots, n\}$, $\beta(x, y, i) = s_i$. Je vous laisse également prouver cette assertion, si vous piochez jetez donc un œil du côté du lemme des restes chinois.
Bien, en quoi cette fonction va-t-elle nous aider ? Eh bien, maintenant, on va pouvoir en quelque sorte quantifier sur les suites, donc quantifier sur un nombre non fixé de variables. Allons-y pour le schéma de récurrence : soit $g : \mathbb{N}^n \to \mathbb{N}$ et $h : \mathbb{N}^{n+2} \to \mathbb{N}$ récursives et supposées exprimables, respectivement par G et H. Le schéma de récurrence nous dit que la fonction $f : \mathbb{N}^{n+1} \to \mathbb{N}$ définie par

$$\begin{cases} f(x_1, \ldots, x_n, 0) & = & g(x_1, \ldots, x_n) \\ f(x_1, \ldots, x_n, y+1) & = & h\left(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)\right) \end{cases}$$

est récursive.
La formule suivante montre que f est exprimable :

$$\begin{aligned} F(x_1, \ldots, x_n, y, z) \equiv \exists a, b \, [\beta(a, b, 0) = y+1 \wedge G\left(x_1, \ldots, x_n, \beta(a, b, 1)\right) \\ \wedge (\forall i 0 < i \leq y \Rightarrow \beta(a, b, i+1) = H\left(x_1, \ldots, x_n, i, w, \beta(a, b, i)\right)) \\ \wedge \beta(a, b, y+1) = z] \end{aligned}$$

Je pense que cette formule ne nécessite pas de commentaire particulier, si ce n'est que les expressions du type $H\left(x_1, \ldots, x_n, i, w, \beta(a, b, i)\right)$ sont en réalité des raccourcis bien commodes pour $\exists t \ F_\beta(a, b, i, t) \wedge H\left(x_1, \ldots, x_n, i, w, t\right)$; pour ceux qui ont l'habitude de la théorie des modèles ça doit paraître évident, et je conseillerai aux autres de ne pas se prendre la tête avec ça, du moins pas dans le contexte du cours de décidabilité...

3. Montrer que l'on peut choisir g (et d) de telle manière que, si A est exprimable, A^* le soit aussi.

Je vous laisse vous en convaincre. Ce n'est pas le passage le plus amusant de la preuve, ce n'est pas compliqué non plus, c'est juste un peu pénible à formaliser.

4. Montrer que l'ensemble des numéros de Gödel des énoncés prouvables de PA est exprimable.

On a même mieux, puisque cet ensemble est récursivement énumérable.[1] En effet, pour

[1] Je vous laisse en exercice la preuve que tout ensemble récursivement énumérable est exprimable.

parler informellement, on peut énumérer toutes les preuves dérivables dans PA ; pour chaque preuve on peut bien entendu regarder ce qu'elle prouve au juste, puis en donner le numéro de Gödel.

5. En déduire que PA est une théorie incomplète.

Soit P l'ensemble des numéros de Gödel des énoncés prouvable dans PA. P est exprimable, d'après la question précédente, donc $\left(\tilde{P}\right)^*$ aussi, d'après les questions 1 et 3. Soit $\psi(n)$ une formule exprimant $\left(\tilde{P}\right)^*$. Par définition, pour tout entier n, $\psi(\overline{n})$ est vraie si et seulement si $d(n)$ n'est pas le numéro de Gödel d'un énoncé prouvable dans PA. Considérons $\psi\left(\overline{g(\psi)}\right)$. Cet énoncé est vrai si et seulement si $d(g(\psi))$ n'est pas le numéro de Gödel d'un énoncé prouvable dans PA ; or $d(g(\psi))$ est par définition le numéro de Gödel de $\psi\left(\overline{g(\psi)}\right)$. On a ainsi trouvé un énoncé G tel que G est équivalent à « G n'est pas prouvable ». Comme PA est cohérente, on en déduit que G est vraie... mais non prouvable dans PA.