Noé de Rancourt
Bureau T9A, toits du DMA
noe.de.rancourt@ens.fr
http://webusers.imj-prg.fr/~noe.de-rancourt/

TD de Logique 9 : Décidabilité, arithmétique

1er et 4 décembre 2017

Les exercices marqués du symbole ♦ sont importants, ce sont ceux que je prévois d'aborder en TD (je ne garantis pas qu'on aura le temps de tous les faire). Ceux d'entre eux qu'on aura eu le temps d'aborder sont à connaître. Les exercices sans symbole sont moins importants, on les abordera en TD si le temps le permet, et sinon je vous conseille de les faire chez vous pour approfondir. Les exercices marqués du symbole ♣ sont facultatifs, en général plus difficiles, et sont destinés à vous faire découvrir des notions en marge du cours ou des applications des notions vues en cours. N'hésitez pas à me demander des précisions à leur propos si ça vous intéresse.

Les exercices 1 et 2 sont à préparer avant le TD et seront corrigés tout au début de la séance.

I. Codage des formules, décidabilité

♦ **Exercice 1** (Codage des formules)**.**

Soit $\mathcal{L}$ un langage récursivement présenté. Montrer que l'ensemble des couples $(n, i) \in \mathbb{N}^2$ tels que n code une $\mathcal{L}$-formule dans laquelle la variable v_i ait au moins une occurence libre est primitif récursif. En déduire que l'ensemble des codes de $\mathcal{L}$-énoncés est primitif récursif.

♦ **Exercice 2.**

Montrer que la théorie vide sur le langage vide est décidable. (On pourra étudier les complétions de cette théorie.)

Exercice 3 (Complétions)**.**

Montrer qu'une théorie consistante et décidable possède une complétion décidable.

Exercice 4 (Nombre de complétions décidables)**.**

Soit $\mathcal{L}$ un langage récursivement présenté et T une $\mathcal{L}$-théorie consistante et décidable. On notera $C(T)$ l'ensemble des théories complètes et déductivement closes qui contiennent T, et $C_d(T)$ l'ensemble des éléments de $C(T)$ qui sont décidables.

1. Montrer que si $C(T)$ est fini, alors $C_d(T) = C(T)$.
2. Montrer que $|C_d(T)| = \min(|C(T|, \aleph_0)$. (On pourra utiliser le résultat de l'exercice 3.)
3. Montrer que pour tout cardinal κ avec $A \leqslant \kappa \leqslant \aleph_0$, il existe un langage $\mathcal{L}$ fini et une $\mathcal{L}$-théorie T consistante et décidable avec $|C_d(T)| = \kappa$.

II. Ensemble récursivement énumerables

Exercice 5 (Réduction *many-one*)**.**

Soient $A \subseteq \mathbb{N}^p$, $B \subseteq \mathbb{N}^q$ deux ensembles. On dit que A *se réduit* à B s'il existe $f : \mathbb{N}^p \to \mathbb{N}^q$ récursive totale telle que $A = f^{-1}(B)$. On notera ceci $A \leqslant_m B$.

1. Montrer que si $A \leqslant_m B$ et si B est récursif (resp. récursivement énumérable), alors A l'est également.

Soit Γ une classes de sous-ensembles de $\mathbb{N}^p$, pour $p \in \mathbb{N}^*$, qui est close par image réciproque récursive. On dit qu'un ensemble $A \in \Gamma$ est Γ-*complet* si tout ensemble de Γ s'y réduit.

2. Quels sont les ensembles récursif-complets ?
3. Montrer qu'un ensemble récursivement énumérable complet n'est pas récursif.
4. Montrer que l'ensemble $\{x \in \mathbb{N} \mid \phi^1(x, x) \downarrow\}$ est récursivement énumérable-complet.

III. Arithmétique

♦ **Exercice 6** (Modèles non-standards de l'arithmétique de Peano)**.**

Dans tout l'exercice, on travaille dans le langage $\mathcal{L}$ de l'arithmétique. Si $\mathcal{M}$ est un modèle de $\mathcal{PA}$, on rappelle qu'il existe un unique plongement :

$$\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathcal{M} \\ n & \longmapsto & \underline{n} = s^n(0) \end{array},$$

dont l'image est un segment initial de $\mathcal{M}$. On notera, dans cet exercice, son image $\mathbb{N}^{\mathcal{M}}$; un élément de $\mathbb{N}^{\mathcal{M}}$ sera dit *standard*, et un élément de $\mathcal{M} \backslash \mathbb{N}^{\mathcal{M}}$ sera dit *non-standard*. Un *modèle non-standard* de $\mathcal{PA}$ est un modèle possédant des éléments non-standards.

1. Montrer qu'il existe un modèle non-standard de $\mathcal{PA}$. Montrer qu'on peut même le choisir de sorte qu'il possède un élément divisible par tous les éléments standard. (On verra dans l'exercice 7 qu'un tel élément existe en fait dans tout modèle non-standard.)

On fixera, pour le reste de cet exercice, $\mathcal{M}$ un modèle non-standard de $\mathcal{PA}$.

2. Montrer que $(\mathcal{M} \backslash \mathbb{N}^{\mathcal{M}}, <)$ est isomorphe à $X \times \mathbb{Z}$ muni de l'ordre lexicographique, pour un certain ensemble totalement ordonné $(X, <)$.
3. Montrer que tout $A \subseteq M$ définissable et non-vide a un plus petit élement. En déduire que $\mathbb{N}^{\mathcal{M}}$ n'est pas définissable dans $\mathcal{M}$.
4. *(Overspill.)* Soit $\varphi(x)$ une formule à une variable libre et à paramètres dans $\mathcal{M}$ (c'est-à-dire une formule à une variable libre de $\mathcal{L}_{\mathcal{M}}$). On suppose que pour tout $n \in \mathcal{M}^{\mathbb{N}}$, $\mathcal{M} \models \varphi(n)$. Montrer qu'il existe $a \in \mathcal{M}$ non-standard tel que $\mathcal{M} \models \varphi(a)$.

Exercice 7 (Préliminaires pour le codage)**.**

Dans cet exercice, on démontre quelques résultats préliminaires et pas passionnants qui nous serviront à faire du codage dans les modèles de $\mathcal{PA}$. Au cours de cet exercice et des suivants, on notera $x \mid y$ la formule $\exists z\, xz = y$, et $r(x, y, z)$ la formule $z < y \wedge \exists t\, x = yt + z$ ("z est le reste de la division euclidienne de x par y") ; la formule $\forall z\, (z \mid x \wedge z \mid y \to z = 1)$ sera notée "x et y sont premiers entre eux".

1. Montrer que $\mathcal{PA} \models \forall x, y\,(x \leqslant y \to \exists! z\, x + z = y)$. La formule $x + z = y$ sera alors aussi notée $z = x - y$.

2. Montrer que la formule $r(x, y, z)$ est fonctionnelle en x et y dès lors que $y \neq 0$, autrement dit que $\mathcal{PA} \vdash \forall x, y\,(y \neq 0 \to \exists! z\, r(x, y, z))$. On notera donc plutôt par la suite cette formule $z = r(x, y)$.

3. Montrer, dans $\mathcal{PA}$, la forme suivante du théorème des restes chinois : "pour tous x, y, u, v, si u et v sont premiers entre eux et si $x < u$ et $y < v$, alors il existe z tel que $r(z, u) = x$ et $r(z, v) = y$".

♦ **Exercice 8** (Codage dans un modèle de $\mathcal{PA}$)**.**

Soit $\mathcal{M} \models \mathcal{PA}$. Soient $T \in \mathcal{M}$ et $(u_t)_{t \leqslant T}$ une suite d'éléments de $\mathcal{M}$. On dit qu'une paire $(a, b) \in \mathcal{M}^2$ *code* la suite $(u_t)_{t \leqslant T}$ si pour tout $t \leqslant T$, on a $\mathcal{M} \models u_t = r(a, (t + 1)b + 1)$, et on dit que la suite $(u_t)_{t \leqslant T}$ est *codable* s'il existe une paire qui la code.

1. Si $\mathcal{M} = \mathbb{N}$, montrer que toute suite est codable. (On pourra prendre $b = n!$ où $n = \max(1 + \max_{t \leqslant T} u_t, T)$ et utiliser le théorème des restes chinois.)

Ce résultat n'est pas exprimable dans $\mathcal{PA}$, par contre, on va maintenant montrer des résultats s'en approchant. On fixe, dans la suite, $\mathcal{M}$ un modèle de $\mathcal{PA}$.

2. Soit $f : \mathcal{M} \longrightarrow \mathcal{M}$ une fonction définissable avec paramètres (c'est-à-dire qu'il existe une formule $\varphi(x, y)$ a deux variables libre et à paramètres dans $\mathcal{M}$ telle que pour tout $a \in \mathcal{M}$, $\mathcal{M} \models \forall y\,(\varphi(a, y) \leftrightarrow y = f(a))$). Soit $T \in \mathcal{M}$; on suppose que pour tout $t \leqslant T$, $f(t) > 0$. Montrer qu'il existe $a \in \mathcal{M}$ non-nul divisible par tous les $f(t)$ pour $t \leqslant T$. En déduire que pour tout $T \in \mathcal{M}$, il existe $a \in \mathcal{M}$ non nul divisible par tous les $t \leqslant T$ non-nuls.

3. Soient $f : \mathcal{M} \longrightarrow \mathcal{M}$ une fonction définissable avec paramètres, et $T \in \mathcal{M}$. Montrer que la suite $(f(t))_{t \leqslant T}$ est codable.

4. Soient $T \in \mathcal{M}$ et $(u_t)_{t \leqslant T+1}$ une suite d'éléments de $\mathcal{M}$. On suppose que $(u_t)_{t \leqslant T}$ est codable. Montrer que $(u_t)_{t \leqslant T+1}$ l'est aussi.

♦ **Exercice 9** (Exponentiation en arithmétique de Peano)**.**

Le but de cet exercice est de définir l'exponentiation en arithmétique de Peano, et de montrer ses propriétés basiques ; plus précisément, on veut définir une formule $\exp(x, y, z)$ à trois variables libres satisfaisant les propriétés suivantes :

- $\mathcal{PA} \vdash \forall x, y\, \exists! z\, \exp(x, y, z)$ (exp est fonctionnelle) ;
- $\mathcal{PA} \vdash \forall x\, \exp(x, 0, 1)$;
- $\mathcal{PA} \vdash \forall x, y, z\,(\exp(x, y, z) \longrightarrow \exp(x, s(y), x \times z))$.

On notera alors abusivement cette formule $x^y = z$.

1. Montrer que si elle existe, exp est "unique" dans le sens où si une autre formule $\exp'$ satisfait les mêmes propriétés, alors on a $\mathcal{P} \vdash \forall x, y, z\,(\exp(x, y, z) \longrightarrow \exp'(x, y, z))$.

2. Soient $\mathcal{M} \models \mathcal{P}$ et $x, y, z \in \mathcal{M}$; on dira que $z = x^y$ s'il existe une suite $(u_t)_{t \leqslant y}$ d'éléments de $\mathcal{M}$ telle que $u_0 = 1$, pour tout $t < y$, $u_{t+1} = xu_t$, et $u_y = z$. Écrire une formule $\exp(x, y, z)$ qui corresponde à cette définition, en utilisant le codage défini à l'exercice 8.

3. Montrer que la formule exp définie à la question précédente satisfait les propriétés requises. On la notera désormais abusivement $z = x^y$.

4. Montrer successivement les propriétés suivantes de l'exponentiation :

   (a) $x^{y+z} = x^y x^z$;

   (b) Pour $x > 1$ fixé, $y \longrightarrow x^y$ est croissante ;

   (c) Pour tous $x > 1$ et y, $x^y > y$.