Logique 2021
Devoir à la Maison #1

David Baelde

Ceci est la V3 de l'énoncé ; les corrections sont signalées dans la marge.
Le devoir est à rendre avant le 10 mars à midi, sous la forme d'un PDF composé en LaTeX, par email à David Baelde. Pour rappel, les devoirs maison seront notés et remplaceront au moins en partie les épreuves sur table cette année.
Vous pouvez travailler le DM en groupe, mais j'attends des rendus rédigés individuellement.
Dans l'énoncé, la substitution de x par t dans A est notée $A\{x \mapsto t\}$ mais j'accepte toute notation usuelle dans vos copies. Tâchez de concentrer votre effort de rédaction sur les points intéressants ; à titre indicatif, aucune question ne justifie de réponse faisant plus d'une page.

1 Axiomes et calculs pour l'arithmétique

La *déduction naturelle modulo* s'obtient en ajoutant aux règles de la déduction naturelle classique la règle de déduction modulo

$$\frac{\Gamma \vdash B \quad A \equiv B}{\Gamma \vdash A}$$

où $\equiv$ est une *congruence* sur les termes et les formules du langage. Une congruence est une relation d'équivalence qui passe au contexte. Concrètement, on demande donc que :

- pour tout symbole de fonction n-aire, $f(t_1, \ldots, t_n) \equiv f(t'_1, \ldots, t'_n)$ quand $t_i \equiv t'_i$ pour tout $i \in [1; n]$;
- pour tout connecteur propositionnel binaire $\star$, on a $A \star B \equiv A' \star B'$ quand $A \equiv A'$ et $B \equiv B'$;
- pour tout quantificateur $\mathcal{Q}$, on a $\mathcal{Q}x.A \equiv \mathcal{Q}x.A'$ quand $A \equiv A'$.

Axiomes de réflexivité et schéma de Leibniz :

$$\forall x.\ x = x \qquad \forall x, y.\ x = y \Rightarrow A\{z \mapsto x\} \Rightarrow A\{z \mapsto y\}$$

Schéma d'induction :

$$A\{z \mapsto 0\} \Rightarrow (\forall x.\, A\{z \mapsto x\} \Rightarrow A\{z \mapsto s(x)\}) \Rightarrow \forall x.\ A\{z \mapsto x\}$$

Axiomes 3 et 4 de Peano :

$$\forall x.\ 0 \neq s(x) \qquad \forall x, y.\ s(x) = s(y) \Rightarrow x = y$$

Axiomes sur l'addition et la multiplication :

$$\begin{array}{ll} \forall y.\ 0 + y = y & \forall x, y.\ s(x) + y = s(x + y) \\ \forall y.\ 0 \times y = 0 & \forall x, y.\ s(x) \times y = (x \times y) + y \end{array}$$

FIGURE 1 – Les axiomes de Peano

On supposera de plus que $\equiv$ est préservée par l'application d'une substitution, et donc en particulier par renommage des variables.

Dans cette exercice nous considérerons des dérivations en déduction naturelle usuelle utilisant l'axiomatique de Peano PA, qu'on rappelle en Figure 1. Plutôt que d'expliciter l'utilisation des axiomes via la composante Γ des séquents, on pourra considérer qu'on a une seconde règle d'axiome qui permet de dériver $\Gamma \vdash A$ quand A est un axiome de la théorie considérée. On explicitera la théorie en annotant les séquents, en écrivant par exemple $\Gamma \vdash_{PA} A$.

On considèrera d'autre part la *théorie calculatoire* C donnée en Figure 2, qui spécifie un ensemble d'axiomes et une congruence $\equiv$. On écrira $\Gamma \vdash_C A$ quand le séquent est dérivable en déduction modulo en utilisant ces axiomes (via la règle axiome étendue comme ci-dessus) et la règle de déduction modulo la congruence donnée par C.

Question 1

Montrer que la relation $\equiv$ définie en Figure 2 coincide avec la relation $\sim$ définie inductivement par les règles suivantes, où f, $\star$ et $\mathcal{Q}$ sont des symboles quelconques comme plus haut :

V2 : ajouté la symétrie. Merci RP !

$$\frac{}{u \sim u} \qquad \frac{v \sim u}{u \sim v} \qquad \frac{u \sim u' \quad u' \sim u''}{u \sim u''}$$

La théorie calculatoire C est donnée par le schéma d'induction (comme dans PA) et la relation $\equiv$ définie comme la plus petite congruence satisfaisant, pour tous termes u et v :

$$\begin{array}{rcl@{\qquad\qquad}rcl} 0 = 0 & \equiv & \top & 0 + u & \equiv & u \\ s(u) = s(v) & \equiv & u = v & 0 \times u & \equiv & 0 \\ 0 = s(v) & \equiv & \bot & s(u) + v & \equiv & s(u + v) \\ s(u) = 0 & \equiv & \bot & s(u) \times v & \equiv & (u \times v) + v \end{array}$$

FIGURE 2 – Théorie calculatoire de l'arithmétique

$$\frac{t_1 \sim t'_1 \quad \dots \quad t_n \sim t'_n}{f(t_1, \dots, t_n) \sim f(t'_1, \dots, t'_n)} \qquad \frac{A \star A' \quad B \star B'}{A \star B \sim A' \star B'} \qquad \frac{A \sim A'}{\mathcal{Q}x.A \sim \mathcal{Q}x.A'}$$

$\overline{0 = 0 \sim \top}$ et de même pour les autres conditions sur $\equiv$ de la Figure 2.

Question 2

Montrer que, si $\Gamma \vdash_C A$ est dérivable en déduction modulo, alors $\Gamma \vdash_{PA} A$ est dérivable en déduction naturelle. On privilégiera une approche sémantique, en montrant d'abord que tout ce qui est démontrable dans $\vdash_C$ est correct dans les modèles égalitaires de PA. V3 : simplification.

Question 3

Montrer que les formules suivantes sont dérivables en déduction modulo avec la théorie calculatoire de l'arithmétique :

- $\forall x.\ x = 0 \vee \exists y.\ x = s(y)$
- $\forall x.\ x = x$
- $\forall x, y.\ x = y \Rightarrow y = x$
- $\forall x, y, z.\ x = y \Rightarrow y = z \Rightarrow x = z$

On veillera à préciser quels axiomes et congruences sont utilisés, et à donner les grandes étapes de la construction d'une dérivation, mais il n'est pas nécessaire de dessiner ne serait-ce qu'un morceau d'arbre de preuve.

Question 4

Montrer que, pour tout terme t, la formule suivante est dérivable en déduction modulo avec la théorie calculatoire de l'arithmétique :

$$\forall x, y.\ x = y \Rightarrow t\{z \mapsto x\} = t\{z \mapsto y\}$$

Question 5

Montrer que, pour toute formule A, la formule suivante est dérivable en déduction modulo avec la théorie calculatoire de l'arithmétique :

$$\forall x, y.\ x = y \Rightarrow A\{z \mapsto x\} \Rightarrow A\{z \mapsto y\}$$

Question 6
Conclure que toutes les conséquences de l'arithmétique de Peano sont prouvables dans la théorie calculatoire de l'arithmétique.

2 Calculs monadiques des prédicats

Dans cet exercice on suppose que le langage ne comporte qu'une sorte. Pour les preuves d'indécidabilité, il faudra réduire des problèmes indécidables connus ; veillez à mentionner les étapes clé de l'argument, et à précisément décrire l'encodage utilisé. Pour la preuve de décidabilité, vous pourrez vous inspirerer du dernier TD de février ; ici encore, j'attends la description précise de la technique de preuve utilisée (e.g. quel énoncé intermédiaire est prouvé par induction sur quoi) mais la rédaction détaillée des cas évidents est inutile.

Question 7
Montrer l'indécidabilité de la validité dans le calcul des prédicats équipé d'un unique symbole de prédicat, d'arité 2, quand tous les symboles de fonction sont unaires. (Indice : on peut restreindre le symbole de prédicat à être l'égalité.)

Question 8
Montrer l'indécidabilité de la validité dans le calcul des prédicats quand tous les symboles de prédicats sont unaires, à l'exception d'un unique symbole de relation binaire. (Lire la question suivante : on ne peut pas restreindre le symbole de prédicat binaire à être l'égalité.)

Question 9
Montrer la décidabilité de la validité dans le calcul des prédicats avec égalité, sans symboles de fonction, et uniquement des symboles de prédicats unaires. (Indice : montrer que si une formule de ce langage a un modèle, elle en a un avec un domaine de cardinal au plus $n2^k$ où k est le nombre de prédicats unaires utilisé et n le nombre de variables utilisées.)