Université Bordeaux 1
Master d'Informatique 1, 2011/2012

LOGIQUE

TD 2 : Élimination des coupures

Exercice 2.1 Harrop
1- On considère les théories (i.e. ensembles de formules) : $\mathrm{EG}, \mathrm{P}_0, \mathrm{PA}, \mathrm{MO}, \mathrm{GR}$. Lesquelles sont des théories de Harrop ? Quelles conséquences peut-on en tirer ?

Exercice 2.2 PA versus P_0
1-Notons P_0' (resp. PA') l'ensemble des formules de P_0 (resp. PA) sauf l'axiome A2. PA' est-il une théorie de Harrop ?
2- Donner une preuve dans LK de $\mathrm{PA}' \models A2$.
3- Pouvez-vous donner une preuve dans LJ de $\mathrm{PA}' \models A2$? existe-t-il un terme t, et une preuve dans LK de $\mathrm{PA}' \models \quad x = 0 \vee x = S(t)$?

Exercice 2.3 Un modèle non-standard de P_0'.
Soit $\mathcal{M} =_{\text{déf.}} \langle \mathcal{N}, 0_{\mathcal{N}}, \mathrm{S}_{\mathcal{N}}, +_{\mathcal{N}}, \times_{\mathcal{N}} \rangle$ la structure « arithmétique » suivante :

$$\begin{aligned}
\mathcal{N} &=_{\text{déf.}} (\mathbb{N} \times \{\bullet\}) \cup (\mathbb{N} \times \{\circ\}) \text{ où } \bullet \neq \circ \\
0_{\mathcal{N}} &=_{\text{déf.}} \langle 0, \bullet \rangle \\
\mathrm{S}_{\mathcal{N}}\langle p, \alpha \rangle &=_{\text{déf.}} \langle \mathrm{S}p, \alpha \rangle \text{ où } \alpha \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle +_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p + q, \alpha \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle \times_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p \times q, \beta \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\}
\end{aligned}$$

Le domaine $\mathcal{N}$ est constitué de deux copies de $\mathbb{N}$, les entiers « noirs » $\langle p, \bullet \rangle$ et les entiers « blancs » $\langle p, \circ \rangle$.La constante zéro est interprétée par le zéro noir $\langle 0, \bullet \rangle$; les opérations successeur, addition et multiplication sont interprétées de telle sorte que :

- le successeur conserve la couleur de son argument,
- l'addition prend la couleur de son *premier* argument,
- la multiplication prend la couleur de son *second* argument.

1. Montrer que $\mathcal{M}$ est un modèle de P_0'. Est-ce un modèle de P_0 ?
2. Montrer qu'aucune des propriétés suivantes n'est conséquence de P_0' :

$$\forall x\ (0 + x = x) \tag{1}$$
$$\forall x, y\ (x + y = y + x) \tag{2}$$
$$\forall x, y, z\ (x + y = x + z \to y = z) \tag{3}$$
$$\forall x\ (x \times \mathrm{S}0 = x) \tag{4}$$
$$\forall x, y\ (x \times y = y \times x) \tag{5}$$

Exercice 2.4 Arithmétique de Heyting

Soit Φ une formule du premier ordre sur la signature de l'arithmétique.

1- Montrer que , si $\mathrm{P}'_0 \vdash\ \forall x \Phi$ est prouvable dans LJ, alors $\mathrm{P}'_0 \vdash\ \Phi$ est prouvable dans LJ.

2- La propriété de la question 1 est-elle vraie en prenant comme membre gauche PA ? ou en prenant comme système logique LK ?

3- Montrer que, si $\mathrm{P}'_0 \vdash \forall x, \exists y \Phi(x, y)$ est prouvable dans LJ, alors, il existe un terme t tel que $\mathrm{P}'_0 \vdash \Phi(x, t)$ est prouvable dans LJ.

4- La propriété de la question 3 est-elle vraie en prenant comme membre gauche PA ? ou en prenant comme système logique LK ?

5- Supposons que $\mathrm{PA}' \vdash \forall x, \exists y \Phi(x, y)$ est prouvable dans LJ, en " n'utilisant qu'une seule récurrence" i.e.

$$\mathrm{P}'_0 \vdash_{\mathrm{LJ}} \exists y \ \ \Phi(0, y); \quad \mathrm{P}'_0 \vdash_{\mathrm{LJ}} (\exists y \Phi(x, y)) \rightarrow (\exists y \Phi(S(x), y))$$

5.1- Vérifer que, sous ces hypothèses, il existe bien dans LJ une preuve de $\mathrm{PA}' \vdash \forall x, \exists y \Phi(x, y)$.

Pour tout $n \in \mathbb{N}$, on note $\underline{n}$ le terme $S(S(\ldots(S(0))\ldots))$ qui reprénte l'entier n dans le langage de l' arithmétique de Peano.

5.2- Montrer que, pour tout entier $n \in \mathbb{N}$, il existe un terme t_n tel que $\mathrm{P}'_0 \vdash_{\mathrm{LJ}} \Phi(\underline{n}, t_n)$.

5.3- Donner un algorithme de calcul de la fonction $n \mapsto t_n$ fondé sur l'algorithme d'élimination des coupures.

On admet maintenant que la propriété démontré dans l'exercice 4, question 5, est vraie pour toute formule de la forme $\forall x, \exists y \Phi(x, y)$ (même si la preuve utilise plus qu'une récurrence).

Exercice 2.5 Fonctions récursives

On se demande si une réciproque de l'énoncé admis ci-dessus est vraie. Nous faisons la supposition (**SUPP**) :

pour toute fonction totale, calculable, $f : \mathbb{N} \rightarrow \mathbb{N}$, il existe une formule $\Phi(x, y)$ telle que

(P1) $\mathrm{PA} \vdash \forall x, \exists_1 y \Phi(x, y)$ est prouvable dans LJ

où $\exists_1 x \ \ F(x)$ est une abbréviation de $\exists x \ \ F(x) \wedge (\forall y, z \ \ F(y) \wedge F(z) \rightarrow y = z)$

(P2) pour tous entiers naturels n, m, $\mathbb{N} \models \ \Phi(\underline{n}, \underline{m})$ si et seulement si $f(n) = m$.

1- Peut-on en déduire une énumération effective des fonctions totales calculables ?

2- Par un argument de diagonalisation, montrer que **SUPP** est fausse.

Admettons le théorème [Matiyasevich, 1971] : une partie $M \subseteq \mathbb{N}$ est récursivement énumérable ssi, il existe un entier $q \in \mathbb{N}$ et un polynôme $P \in \mathbb{Z}[X, Y_1, \ldots, Y_q]$ tels que, pour tout $x \in \mathbb{N}$,

$$x \in M \Leftrightarrow \exists \vec{y} \in \mathbb{N}^q, P(x, \vec{y}) = 0.$$

Exercice 2.6 Indécidabilité de PA
Soit q un entier naturel, P un polynome de $\mathbb{Z}[X, Y_1, \ldots, Y_q]$.
1- Montrer que, si $\mathbb{N} \models \exists \vec{y} P(\underline{n}, \vec{y}) = 0$.
alors il existe un vecteur d'entiers naturels $\vec{m}$ tel que $\mathrm{PA} \vdash_{\mathrm{LK}} P(\underline{n}, \underline{\vec{m}}) = 0$.
2- Montrer que, si $\mathrm{PA} \vdash_{\mathrm{LK}} \exists \vec{y}\ \ P(\underline{n}, \vec{y}) = 0$, alors $\mathbb{N} \models \exists \vec{y} P(\underline{n}, \vec{y}) = 0$.
3- Montrer qu' il existe un polynôme P tel que le problème
Donnée : $n \in \mathbb{N}$; Question : existe-t-il un vecteur $\vec{m} \in \mathbb{N}^q$ tel que $P(n, \vec{m}) = 0$?
est indécidable.
4- En déduire que le problème suivant est indécidable :
Donnée : une formule Φ ; Question : $\mathrm{PA} \vdash_{\mathrm{LK}} \Phi$?

Exercice 2.7 Signature
Pour tout multi-ensemble de formules Γ, on note $\mathcal{S}(\Gamma)$ la signature composée des symboles de relation et des symboles de fonctions apparaissant dans Γ.
1- Montrer que, si le séquent $\Gamma \vdash \Delta$ est prouvable dans LK, alors il admet une preuve qui n'utilise que des symboles de $\mathcal{S}(\Gamma, \Delta)$.
2- Soit $S = \Gamma \vdash \Delta$ un séquent n'utilisant aucun symbole de fonction. Montrer qu'il existe un ensemble fini de formules $\mathcal{F}$, calculable à partir de S, tel que S est prouvable dans LK ssi il admet une preuve dont tous les séquents sont des paires $\Gamma' \vdash \Delta'$ où Γ', Δ' sont des multi-ensembles de formules de l'ensemble $\{F[x_1 := y_1, \ldots, x_q := y_q] \mid y_j \in \mathcal{V}, F \in \mathcal{F}\}$.
3- Peut-on en conclure que le problème suivant est décidable :
Donnée : un séquent $S = \Gamma \vdash \Delta$, sans symbole de fonction ; Question : S est-il dérivable dans LK ?

Exercice 2.8 Équations dans les groupes

1- Esquisser une preuve π_1 dans LJ de

$$\mathrm{GR} \vdash \exists x \ \ x * a * a * b = b * a * a * x$$

2- Esquisser une preuve π_2 dans LJ de

$$\mathrm{GR}, x * a * a * b = b * a * a * x \vdash \exists y \ \ b * a * a * x * I(b) * I(a) * I(a) * x * x = y * y * I(x)$$

3- En déduire, en utilisant une coupure, une preuve dans LJ de

$$\mathrm{GR} \vdash \exists x \exists y \ \ b * a * a * x * I(b) * I(a) * I(a) * x * x = y * y * I(x)$$

4- Quels sont les termes t_1, t_2 fournis par π_1, π_2, tels que

$$\mathrm{GR} \vdash \ \ t_1 * a * a * b = b * a * a * t_1$$

et

$$\mathrm{GR}, x * a * a * b = b * a * a * x \vdash \ \ b * a * a * x * I(b) * I(a) * I(a) * x * x = t_2 * t_2 * I(x)$$

5- Pouvez-vous en déduire des termes t_3, t_4 tels que

$$\mathrm{GR} \vdash \ \ b * a * a * t_3 * I(b) * I(a) * I(a) * t_3 * t_3 = t_4 * t_4 * I(t_3)$$

6- Comment obtenir de tels termes t_3, t_4 par élimination de coupures ?