Logique
Devoir à la Maison

David Baelde et Gilles Dowek

1 Axiomes et règles de calcul pour l'arithmétique

Soit $\mathcal{L}$ un langage, une *congruence* sur $\mathcal{L}$ est une relation d'équivalence $\sim$, définie sur les termes et les propositions de $\mathcal{L}$, telle que

- pour tout symbole de fonction f d'arité n et tous t_1, ..., t_n, t'_1, ..., t'_n, si, pour tout $i \in [1, n]$, $t_i \sim t'_i$, alors $f(t_1, \ldots, t_n) \sim f(t'_1, \ldots, t'_n)$,
- pour tout symbole de prédicat f d'arité n et tous t_1, ..., t_n, t'_1, ..., t'_n, si, pour tout $i \in [1, n]$, $t_i \sim t'_i$, alors $P(t_1, \ldots, t_n) \sim P(t'_1, \ldots, t'_n)$,
- si $A \sim A'$, alors $\neg A \sim \neg A'$,
- pour tout connecteur binaire $\star$, si $A \sim A'$ et $B \sim B'$, alors $A \star B \sim A' \star B'$,
- pour tout quantificateur $\mathcal{Q}$, si $A \sim A'$, alors $\mathcal{Q}x\ A \sim \mathcal{Q}x\ A'$.

Question 1
Soit $\equiv$ la relation définie inductivement, sur les termes et les propositions de l'arithmétique, par les règles (dans les trois premières, t, t' et t'' sont des termes ou des propositions)

$$\frac{}{t \equiv t} \qquad \frac{t \equiv t'}{t' \equiv t} \qquad \frac{t \equiv t' \quad t' \equiv t''}{t \equiv t''}$$

$$\frac{t_1 \equiv t'_1 \quad \ldots \quad t_n \equiv t'_n}{f(t_1, \ldots, t_n) \equiv f(t'_1, \ldots, t'_n)} \qquad \frac{t_1 \equiv t'_1 \quad \ldots \quad t_n \equiv t'_n}{P(t_1, \ldots, t_n) \equiv P(t'_1, \ldots, t'_n)}$$

$$\frac{A \equiv A'}{\neg A \equiv \neg A'} \qquad \frac{A \equiv A' \quad B \equiv B'}{A \star B \equiv A' \star B'} \qquad \frac{A \equiv A'}{\mathcal{Q}x\ A \equiv \mathcal{Q}x\ A'}$$

$$\frac{}{0 = 0 \equiv \top} \qquad \frac{}{S(t) = S(u) \equiv t = u} \qquad \frac{}{0 = S(u) \equiv \bot} \qquad \frac{}{S(t) = 0 \equiv \bot}$$

$$\frac{}{0 + u \equiv u} \qquad \frac{}{0 \times u \equiv 0} \qquad \frac{}{S(t) + u \equiv S(t + u)} \qquad \frac{}{S(t) \times u \equiv (t \times u) + u}$$

Montrer que $\equiv$ est la plus petite congruence $\sim$ vérifiant les propriétés

$$\begin{array}{rcl@{\qquad}rcl}
0 = 0 & \sim & \top & 0 + u & \sim & u \\
S(t) = S(u) & \sim & t = u & 0 \times u & \sim & 0 \\
0 = S(u) & \sim & \bot & S(t) + u & \sim & S(t + u) \\
S(t) = 0 & \sim & \bot & S(t) \times u & \sim & (t \times u) + u
\end{array}$$

Axiomes de réflexivité et schéma de Leibniz :

$$\forall x\ (x = x) \qquad \forall x \forall y\ (x = y \Rightarrow (x/z)A \Rightarrow (y/z)A)$$

Schéma de récurrence :

$$(0/z)A \Rightarrow \forall x\ ((x/z)A \Rightarrow (S(x)/z)A) \Rightarrow \forall y\ (y/z)A$$

Axiomes 3 et 4 de Peano :

$$\forall x \forall y\ (S(x) = S(y) \Rightarrow x = y) \qquad \forall x\ \neg(0 = S(x))$$

Axiomes de l'addition et la multiplication :

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

FIGURE 1 – Les axiomes de Peano

Question 2
Montrer que si t et t' sont deux termes ou deux propositions tels que $t \equiv t'$ et σ est une substitution, alors $\sigma t \equiv \sigma t'$.

La *déduction naturelle modulo théorie* est un système logique obtenu en ajoutant aux règles de la déduction naturelle classique la règle

$$\frac{\Gamma \vdash A}{\Gamma \vdash B}\ \textit{conv} \text{ si } A \equiv B$$

où $\equiv$ est une congruence définie sur les termes et les propositions du langage. Une théorie est donc définie d'une part par un ensemble d'axiomes et d'autres part par une congruence $\equiv$.

Dans cet exercice, nous considérerons des démonstrations en déduction naturelle usuelle utilisant les axiomes de Peano PA, rappelés Figure 1. Nous disons que $\Gamma \vdash_{PA} A$ est démontrable si le séquent $\Gamma \vdash A$ est démontrable dans PA.

Nous considérons d'autre part la théorie C, en déduction modulo théorie, formée par la congruence définie Question 1 et le schéma d'axiome de récurrence. Nous disons que $\Gamma \vdash_C A$ est démontrable quand le séquent $\Gamma \vdash A$ est démontrable en déduction modulo théorie, dans la théorie C.

Question 3

Donner une démonstration dans C de la proposition A

$$S(S(S(S(0)))) \times S(S(S(S(0)))) = S(S(S(S(S(S(S(S(S(S(S(S(S(S(S(S(0))))))))))))))))$$

Question 4
Montrer que, si $\Gamma \vdash_C A$ est démontrable, alors $\Gamma \vdash_{PA} A$ est démontrable. On privilégiera une approche sémantique, en montrant d'abord que tout ce qui est démontrable dans $\vdash_C$ est valide dans tous les modèles bivalués et égalitaires de PA.

Question 5
Montrer que les propositions

- $\forall x\ (x = x)$
- $\forall x \forall y\ (x = y \Rightarrow y = x)$
- $\forall x \forall y \forall z\ (x = y \Rightarrow y = z \Rightarrow x = z)$

sont démontrables dans la théorie C.

On veillera à préciser quels axiomes et congruences sont utilisés, et à donner les grandes étapes de la construction d'une démonstration, mais il n'est pas nécessaire de dessiner l'arbre.

Question 6
Montrer que les propositions

$$\forall x \forall x' \forall y \forall y'\ (x = x' \Rightarrow y = y' \Rightarrow x + y = x' + y')$$

$$\forall x \forall x' \forall y \forall y'\ (x = x' \Rightarrow y = y' \Rightarrow x \times y = x' \times y')$$

sont démontrables dans la théorie C.

Question 7
Montrer que, pour tout terme t, la proposition

$$\forall x \forall y\ (x = y \Rightarrow (x/z)t = (y/z)t)$$

est démontrable dans la théorie C.

Question 8
Montrer que, pour toute proposition A, la proposition

$$\forall x \forall y\ (x = y \Rightarrow (x/z)A \Rightarrow (y/z)A)$$

est démontrable dans C.

Question 9
Montrer que les axiomes de PA sont démontrables dans la théorie C.

Question 10
Conclure que toutes les propositions démontrables dans l'arithmétique de Peano sont démontrables dans la théorie C.

2 Une équation polynomiale dont l'absence de solutions entières n'est pas démontrable dans l'arithmétique

Toutes les démonstrations, dans cet exercice, sont dans l'arithmétique de Peano. Nous notons $\mathbb{N}$ le modèle standard de cette théorie. Nous notons $\underline{n}$ le terme $S(S(...S(0)...))$, avec n occurrences du symbole S. Et nous admettons le théorème de Matiyasevich, selon lequel l'ensemble des propositions closes de la forme

$$\exists x_1 ... \exists x_m \ (t = u)$$

valides dans le modèle $\mathbb{N}$ est indécidable.

Question 11
Montrer que si t est un terme clos de l'arithmétique, alors il existe un entier n tel que la proposition $t = \underline{n}$ soit démontrable.

Monter que si n et p sont deux entiers, alors ou bien la proposition $\underline{n} = \underline{p}$ est démontrable ou bien la proposition $\neg(\underline{n} = \underline{p})$ est démontrable.

Montrer que si t et u sont deux termes clos de l'arithmétique, alors la proposition $t = u$ est démontrable ou la proposition $\neg(t = u)$ est démontrable.

Question 12
Soit t et u deux termes de l'arithmétique dont les variables sont parmi $x_1, ..., x_m$.

Montrer que si la proposition $\exists x_1 \ldots \exists x_m \ (t = u)$ n'est pas démontrable, alors pour tout $p_1, ..., p_m$, la proposition $(\underline{p_1}/x_1, ..., \underline{p_m}/x_m)(t = u)$ n'est pas démontrable.

Montrer que si la proposition $\exists x_1 \ldots \exists x_m \ (t = u)$ n'est pas démontrable, alors pour tout $p_1, ..., p_m$, la proposition $(\underline{p_1}/x_1, ..., \underline{p_m}/x_m)\neg(t = u)$ est démontrable.

Question 13
Montrer qu'il existe une proposition close A de la forme $\exists x_1 ... \exists x_m \ (t = u)$ telle que ni A ni $\neg A$ ne soit démontrable dans l'arithmétique.

Question 14
Nous reprenons la proposition de la question 13. Montrer que

- pour tous $p_1, ..., p_m$ la proposition $(\underline{p_1}/x_1, ..., \underline{p_m}/x_m)\neg(t = u)$ est démontrable
- la proposition $\forall x_1 \ ... \ \forall x_m \neg(t = u)$ n'est pas démontrable.