Preuves assistées par ordinateur – TD n° 2

Preuves dans l'arithmétique de Peano

L'arithmétique de Peano (PA) est la théorie classique construite sur la signature formée par un symbole de constante 0 (« zéro »), un symbole de fonction s (« successeur ») d'arité 1, deux symboles de fonction $+$ (« plus ») et $\times$ (« fois ») d'arité 2, et un symbole de prédicat $=$ (« égalité ») d'arité 2, et dont les axiomes sont les suivants :

Axiomes d'égalité et de compatibilité

1. $\forall x\ (x = x)$
2. $\forall x\ \forall y\ (x = y \Rightarrow y = x)$
3. $\forall x\ \forall y\ \forall z\ (x = y \wedge y = z \Rightarrow x = z)$
4. $\forall x\ \forall x'\ (x = x' \Rightarrow s(x) = s(x'))$
5. $\forall x\ \forall x'\ \forall y\ (x = x' \Rightarrow x + y = x' + y)$
6. $\forall x\ \forall y\ \forall y'\ (y = y' \Rightarrow x + y = x + y')$
7. $\forall x\ \forall x'\ \forall y\ (x = x' \Rightarrow x \times y = x' \times y)$
8. $\forall x\ \forall y\ \forall y'\ (y = y' \Rightarrow x \times y = x \times y')$

Axiomes d'addition

9. $\forall y\ (0 + y = y)$
10. $\forall x\ \forall y\ (s(x) + y = s(x + y))$

Axiomes de multiplication

11. $\forall y\ (0 \times y = 0)$
12. $\forall x\ \forall y\ (s(x) \times y = (x \times y) + y)$

Axiomes de Peano

13 $\forall x\ \forall x'\ (s(x) = s(x') \Rightarrow x = x')$
14 $\forall x\ \neg(s(x) = 0)$
15 $\forall x_1 \cdots \forall x_n\ (A\{x := 0\}\ \wedge\ \forall x\ (A \Rightarrow A\{x := s(x)\})\ \Rightarrow\ \forall x\ A)$
pour tout formule A où $FV(A) \subset \{x_1; \ldots; x_n; x\}$

La théorie intuitionniste formée sur la même signature et les mêmes axiomes est notée HA. Dans ce qui suit, on utilise les abréviations $1 = s(0)$, $2 = s(1)$, $3 = s(2)$, etc.

Exercice 1 – Principe de Leibniz

1. À l'aide des axiomes d'égalité, montrer que (la clôture universelle de) la formule

$$x = y \quad \Rightarrow \quad x \times x + 2 \times (x \times z) + z \times z \ = \ y \times y + 2 \times (y \times z) + z \times z$$

est un théorème de HA. Quelle est sa signification ?

2. Montrer que pour tout terme t de l'arithmétique on a

$$\vdash_{\mathrm{HA}} \quad x = y \ \Rightarrow \ t\{z := x\} = t\{z := y\}$$

3. Montrer que pour toute formule A de l'arithmétique on a

$$\vdash_{\mathrm{HA}} \quad x = y \ \Rightarrow \ (A\{z := x\} \Leftrightarrow A\{z := y\})$$

Exercice 2 (Associativité de l'addition) Construire dans HA une dérivation de :

$$\vdash_{\mathrm{HA}} \quad \forall x\ \forall y\ \forall z\ ((x+y)+z = x+(y+z))$$

Indication : On effectuera dans un premier temps la preuve *informellement*, en explicitant à chaque étape de raisonnement la règle ou l'axiome invoqué, éventuellement l'hypothèse de récurrence. Ce n'est que dans un deuxième temps qu'on traduira chaque étape de raisonnement en un fragment de dérivation, avant de procéder à l'assemblage des fragments ainsi obtenus.

Exercice 3 (Commutativité de l'addition) Montrer dans HA les théorèmes :

1. $\forall x\ (x+0=x)$
2. $\forall x\ \forall y\ (x+s(y)=s(x+y))$
3. $\forall x\ \forall y\ (x+y=y+x)$

(Même méthodologie qu'à l'exercice 2.)

Exercice 4 (Parité) Montrer dans HA que : $\forall x\ \exists y\ (x = 2\times y\ \vee\ x = 2\times y+1)$
Dans cet exercice, on s'attachera surtout à préciser les étapes de raisonnement sans entrer dans les détails de la dérivation. *Indication :* Ne pas hésiter à introduire des lemmes intermédiaires !

Exercice 5 (Multiplication) Montrer dans HA les théorèmes :

1. $\forall x\ \forall y\ \forall z\ ((x\times y)\times z\ =\ x\times(y\times z))$
2. $\forall x\ \forall y\ (x\times y\ =\ y\times x)$
3. $\forall x\ \forall y\ \forall\ z((x+y)\times z\ =\ x\times z+y\times z)$

(Même méthodologie qu'à l'exercice 4.)

Exercice 6 (Principe du minimum (**)) Étant donné une formule $A(x)$, démontrer dans l'arithmétique de Peano le théorème suivant :

$$\exists x\ A(x) \quad\Rightarrow\quad \exists x_0\ [A(x_0)\ \wedge\ \forall x\ (A(x)\ \Rightarrow\ x_0\le x)]$$

(où $x_0 \le x$ est une abréviation pour $\exists z\ (x_0+z=x)$). La preuve est-elle intuitionniste ?

Exercice 7 (Le théorème d'Euclide (***)) On s'intéresse à la démonstration, dans l'arithmétique de Peano, du théorème d'Euclide

$$\forall x\ \exists y\ (x\le y\wedge \mathrm{prime}(y))$$

exprimant l'infinité des nombres premiers, où $\mathrm{prime}(x)$ désigne l'abréviation

$$\mathrm{prime}(x)\ \equiv\ x\neq 1\ \wedge\ \forall y\ \forall z\ (x=y\times z\Rightarrow y=1\vee z=1)\,.$$

Expliquer comment la preuve usuelle de ce théorème (que l'on trouvera dans les bons ouvrages de mathématiques) peut se formaliser dans PA. Quelles sont les difficultés rencontrées ?

Exercice 8 (Fonction puissance (****)) Construire dans le langage de l'arithmétique de Peano (i.e. 0, s, $+$, $\times$, variables, connecteurs et quantificateurs) une formule $P(x,y,z)$ à trois variables libres x, y, z exactement, et qui exprime que « $z = x^y$ ». Vérifier qu'on a :

1. $\forall x\ \forall z\ (P(x,0,z)\Leftrightarrow z=1)$
2. $\forall x\ \forall y\ \forall z\ [P(x,y,z)\ \Rightarrow\ \forall z'\ (P(x,s(y),z')\Leftrightarrow z'=z\times x)]$