

Preuves assistées par ordinateur – TD n 3

Preuves dans l'arithmétique de Peano

L'arithmétique d Peano (PA) st la théorie classiqu construit sur la signatur formé par un symbol d constant 0 (« zéro »), un symbol d fonction s (« succ ss ur ») d'arité 1, d ux symbol s d fonction $+$ (« plus ») t (« fois ») d'arité 2, t un symbol d prédicat $=$ (« égalité ») d'arité 2, t dont l s axiom s sont l s suivants :

Axiomes d'égalité et de compatibilité

- | | |
|---|---|
| 1: $\forall x (x = x)$ | 5: $\forall x \forall x' \forall y (x = x' \rightarrow x + y = x' + y)$ |
| 2: $\forall x \forall y (x = y \rightarrow y = x)$ | 6: $\forall x \forall y \forall y' (y = y' \rightarrow x + y = x + y')$ |
| 3: $\forall x \forall y \forall z (x = y \wedge y = z \rightarrow x = z)$ | 7: $\forall x \forall x' \forall y (x = x' \rightarrow x \cdot y = x' \cdot y)$ |
| 4: $\forall x \forall x' (x = x' \rightarrow s(x) = s(x'))$ | 8: $\forall x \forall y \forall y' (y = y' \rightarrow x \cdot y = x \cdot y')$ |

Axiomes d'addition

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

Axiomes de multiplication

- 11: $\forall y (0 \cdot y = 0)$
 12: $\forall x \forall y (s(x) \cdot y = (x \cdot y) + y)$

Axiomes de Peano

- 13 $\forall x \forall x' (s(x) = s(x') \rightarrow x = x')$
 14 $\forall x : (s(x) = 0)$
 15 $\forall x_1 \dots \forall x_n (Afx := 0g \wedge \forall x (A \rightarrow Afx := s(x)g) \rightarrow \forall x A)$
 pour tout formul A où $FV(A) = \{x_1; \dots; x_n\}$

La théorie intuitionnist formé sur la mêm signatur t l s mêm s axiom s st noté HA. Dans c qui suit, on utilis l s abréviations $1 = s(0)$, $2 = s(1)$, $3 = s(2)$, tc.

Exercice 1 – Principe de Leibniz

1. À l'aïd d s axiom s d'égalité, montr r qu (la clôture univ rs ll d) la formul

$$x = y \rightarrow x \cdot x + 2 \cdot (x \cdot z) + z \cdot z = y \cdot y + 2 \cdot (y \cdot z) + z \cdot z$$

st un théorèm d HA. Qu ll st sa signification ?

2. Montr r qu pour tout t rm t d l'arithmétique on a

$$\vdash_{\text{HA}} (x = y \rightarrow tfz := xg = tfz := yg)$$

3. Montr r qu pour tout formul A d l'arithmétique on a

$$\vdash_{\text{HA}} (x = y \rightarrow (Afx := xg, Afx := yg))$$

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

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

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. C'est seulement 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 qu' : $\forall x \forall y (x = 2 \cdot y \rightarrow x = 2 \cdot y + 1)$

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

(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 :

$$\forall x (A(x) \rightarrow \exists x_0 [A(x_0) \wedge \forall x (A(x) \rightarrow x_0 \leq x)])$$

(où $x_0 \leq x$ 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

$$\forall x \forall y (x \leq y \rightarrow \text{prime}(y))$$

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

$$\text{prime}(x) \equiv x \neq 1 \wedge \forall y \forall z (x = y \cdot z \rightarrow y = 1 \wedge z = 1) :$$

Expliquer comment la preuve usuelle de ce théorème (qu'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, +, ·, variables, connecteurs et quantificateurs) une formule $P(x; y; z)$ à trois variables libres x, y, z exacte ment, telle qu'elle exprime que « $z = x^y$ ». Vérifier qu'on a :

1. $\forall x \forall z (P(x; 0; z) \rightarrow z = 1)$
2. $\forall x \forall y \forall z [P(x; y; z) \rightarrow \forall z' (P(x; s(y); z') \rightarrow z' = z \cdot x)]$