

# Arithmetic as a theory modulo

## Gilles Dowek et Benjamin Werner

Lisa Allali

Logical

September 5, 2006

## Definitions

Une **Théorie en déduction modulo** est un ensemble d'axiomes et de règles de réécriture.

## Definitions

Une **Théorie en déduction modulo** est un ensemble d'axiomes et de règles de réécriture.

Une **Théorie purement calculatoire** est un ensemble règles de réécriture sans axiome.

## Definitions

Une **Théorie en déduction modulo** est un ensemble d'axiomes et de règles de réécriture.

Une **Théorie purement calculatoire** est un ensemble règles de réécriture sans axiome.

## Question

Comment passer d'un système axiomatique à un système purement calculatoire ?

# Présentation axiomatique de l'Arithmétique de Heyting

## Les symboles

$0, S, +, \times$  et  $=$

# Présentation axiomatique de l'Arithmétique de Heyting

## Les symboles

0, S, +, × et =

## Les axiomes de l'égalité

$$\forall x \ x = x$$

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

# Présentation axiomatique de l'Arithmétique de Heyting

## Les symboles

$0, S, +, \times$  et  $=$

## Les axiomes de l'égalité

$$\forall x \ x = x$$

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Les propositions

$$\forall x \ \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

$$((0/x)P \Rightarrow \forall y \ ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n \ (n/x)P)$$

$$\forall y \ (0 + y = y)$$

$$\forall x \ \forall y \ (S(x) + y = S(x + y))$$

$$\forall y \ (0 \times y = 0)$$

$$\forall x \ \forall y \ (S(x) \times y = x \times y + y)$$

# Les “faciles”

$$\forall y (0 + y = y)$$

$$\forall x \forall y (S(x) + y = S(x + y))$$

$$\forall y (0 \times y = 0)$$

$$\forall x \forall y (S(x) \times y = x \times y + y)$$

# Les “faciles”

$$\forall y (0 + y = y) \quad \rightsquigarrow \quad 0 + y \longrightarrow y$$

$$\forall x \forall y (S(x) + y = S(x + y))$$

$$\forall y (0 \times y = 0)$$

$$\forall x \forall y (S(x) \times y = x \times y + y)$$

## Les “faciles”

$$\forall y (0 + y = y) \quad \rightsquigarrow \quad 0 + y \longrightarrow y$$

$$\forall x \forall y (S(x) + y = S(x + y)) \quad \rightsquigarrow \quad S(x) + y \longrightarrow S(x + y)$$

$$\forall y (0 \times y = 0)$$

$$\forall x \forall y (S(x) \times y = x \times y + y)$$

# Les “faciles”

$$\forall y (0 + y = y) \quad \rightsquigarrow \quad 0 + y \longrightarrow y$$

$$\forall x \forall y (S(x) + y = S(x + y)) \quad \rightsquigarrow \quad S(x) + y \longrightarrow S(x + y)$$

$$\forall y (0 \times y = 0) \quad \rightsquigarrow \quad 0 \times y \longrightarrow 0$$

$$\forall x \forall y (S(x) \times y = x \times y + y)$$

# Les “faciles”

$$\forall y (0 + y = y) \quad \rightsquigarrow \quad 0 + y \longrightarrow y$$

$$\forall x \forall y (S(x) + y = S(x + y)) \quad \rightsquigarrow \quad S(x) + y \longrightarrow S(x + y)$$

$$\forall y (0 \times y = 0) \quad \rightsquigarrow \quad 0 \times y \longrightarrow 0$$

$$\forall x \forall y (S(x) \times y = x \times y + y) \quad \rightsquigarrow \quad S(x) \times y \longrightarrow x \times y + y$$

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ?

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Approche naïve

$$x = y \longrightarrow P(x) = P(y)$$

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Approche naïve

$$x = y \longrightarrow P(x) = P(y)$$

## Exemple

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Approche naïve

$$x = y \longrightarrow P(x) = P(y)$$

## Exemple

On veut prouver  $6 = 8$

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Approche naïve

$$x = y \longrightarrow P(x) = P(y)$$

## Exemple

On veut prouver  $6 = 8$

on réécrit avec le prédicat être pair

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Approche naïve

$$x = y \longrightarrow P(x) = P(y)$$

## Exemple

On veut prouver  $6 = 8$

on réécrit avec le prédicat être pair

$$Pair(6) = Pair(8)$$

# Les axiomes de l'égalité

## La réflexivité

remplacer  $\forall x \ x = x$  par  $x \longrightarrow x$  ? **Non**

## Que faire du schéma d'axiome ?

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Approche naïve

$$x = y \longrightarrow P(x) = P(y)$$

## Exemple

On veut prouver  $6 = 8$

on réécrit avec le prédicat être pair

$$Pair(6) = Pair(8)$$

$$true = true$$

# Les axiomes de l'égalité

Nécessité de l'équivalence

# Les axiomes de l'égalité

Nécessité de l'équivalence

On passe du schéma d'axiome

$$\forall x \forall y x = y \Rightarrow P(x) = P(y)$$

# Les axiomes de l'égalité

Nécessité de l'équivalence

On passe du schéma d'axiome

$$\forall x \forall y x = y \Rightarrow P(x) = P(y)$$

A l'équivalence

$$\forall x \forall y x = y \Leftrightarrow \forall P P(x) = P(y)$$

# Les axiomes de l'égalité

Nécessité de l'équivalence

On passe du schéma d'axiome

$$\forall x \forall y x = y \Rightarrow P(x) = P(y)$$

A l'équivalence

$$\forall x \forall y x = y \Leftrightarrow \forall P P(x) = P(y)$$

Oh oh ... on vient de passer à l'ordre supérieur

# Comment revenir au premier ordre

Passage à une théorie multi-sortée

# Comment revenir au premier ordre

## Passage à une théorie multi-sortée

On ajoute 2 sortes  $\iota$  et  $\kappa$ , et un symbole  $\in$

# Comment revenir au premier ordre

## Passage à une théorie multi-sortée

On ajoute 2 sortes  $\iota$  et  $\kappa$ , et un symbole  $\in$

### Le langage

$0 : \iota$

$S : \langle \iota, \iota \rangle$

$+$  :  $\langle \iota, \iota, \iota \rangle$

$\times$  :  $\langle \iota, \iota, \iota \rangle$

$=$  :  $\langle \iota, \iota \rangle$

$\in$  :  $\langle \iota, \kappa \rangle$

# Comment revenir au premier ordre

## Passage à une théorie multi-sortée

On ajoute 2 sortes  $\iota$  et  $\kappa$ , et un symbole  $\in$

## Le langage

$0 : \iota$

$S : \langle \iota, \iota \rangle$

$+$  :  $\langle \iota, \iota, \iota \rangle$

$\times$  :  $\langle \iota, \iota, \iota \rangle$

$=$  :  $\langle \iota, \iota \rangle$

$\in$  :  $\langle \iota, \kappa \rangle$

## Question

C'est bien joli mais on s'en sert comment ?

Pour toute proposition

$$P(z, y_1, \dots, y_n)$$

du langage, on ajoute un nouveau symbole de fonction de rang  
 $\langle l, \dots, l, \kappa \rangle$

$$f_{z, y_1, \dots, y_n, P}$$

Pour toute proposition

$$P(z, y_1, \dots, y_n)$$

du langage, on ajoute un nouveau symbole de fonction de rang  
 $\langle l, \dots, l, \kappa \rangle$

$$f_{z, y_1, \dots, y_n, P}$$

Modélisation de l'appartenance

$$x \in f_{z, y_1, \dots, y_n, P}(y_1, \dots, y_n) \Leftrightarrow (x/z)P$$

Et comme on a une équivalence ...

## Retour à notre axiome de l'égalité

... on peut faire une règle de réécriture

$$x \in f_{z,y_1,\dots,y_n,P}(y_1,\dots,y_n) \longrightarrow (x/z)P$$

## Retour à notre axiome de l'égalité

... on peut faire une règle de réécriture

$$x \in f_{z,y_1,\dots,y_n,P}(y_1,\dots,y_n) \longrightarrow (x/z)P$$

Revenons à notre mouton

$$\forall x \forall y x = y \Leftrightarrow \forall P P(x) = P(y)$$

## Retour à notre axiome de l'égalité

... on peut faire une règle de réécriture

$$x \in f_{z,y_1,\dots,y_n,P}(y_1,\dots,y_n) \longrightarrow (x/z)P$$

Revenons à notre mouton

$$\begin{aligned} \forall x \forall y \ x = y &\Leftrightarrow \forall P \ P(x) = P(y) \\ \forall x \forall y \ (x = y &\Leftrightarrow \forall p \ (x \in p \Rightarrow y \in p)) \end{aligned}$$

## Retour à notre axiome de l'égalité

... on peut faire une règle de réécriture

$$x \in f_{z,y_1,\dots,y_n,P}(y_1,\dots,y_n) \longrightarrow (x/z)P$$

Revenons à notre mouton

$$\begin{aligned} \forall x \forall y \ x = y &\Leftrightarrow \forall P \ P(x) = P(y) \\ \forall x \forall y \ (x = y &\Leftrightarrow \forall p \ (x \in p \Rightarrow y \in p)) \\ &\rightsquigarrow \\ x = y &\longrightarrow \forall p \ (x \in p \Rightarrow y \in p) \end{aligned}$$

## Retour à notre axiome de l'égalité

... on peut faire une règle de réécriture

$$x \in f_{z,y_1,\dots,y_n,P}(y_1,\dots,y_n) \longrightarrow (x/z)P$$

Revenons à notre mouton

$$\begin{aligned} \forall x \forall y \ x = y &\Leftrightarrow \forall P \ P(x) = P(y) \\ \forall x \forall y \ (x = y &\Leftrightarrow \forall p \ (x \in p \Rightarrow y \in p)) \\ &\rightsquigarrow \\ x = y &\longrightarrow \forall p \ (x \in p \Rightarrow y \in p) \end{aligned}$$

On récupère gratuitement la réflexivité de l'égalité

# Récapitulatif

$$\forall x \ x = x$$

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

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

$$\forall x \ \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$((0/x)P \Rightarrow \forall y \ ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n \ (n/x)P)$$

$$\forall y \ (0 + y = y)$$

$$\forall x \ \forall y \ (S(x) + y = S(x + y))$$

$$\forall y \ (0 \times y = 0)$$

$$\forall x \ \forall y \ (S(x) \times y = x \times y + y)$$

# Récapitulatif

$$\forall x \ x = x$$

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

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

$$\forall x \ \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$((0/x)P \Rightarrow \forall y \ ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n \ (n/x)P)$$

$$\forall y \ (0 + y = y) \rightsquigarrow 0 + y \longrightarrow y$$

$$\forall x \ \forall y \ (S(x) + y = S(x + y)) \rightsquigarrow S(x) + y \longrightarrow S(x + y)$$

$$\forall y \ (0 \times y = 0) \rightsquigarrow 0 \times y \longrightarrow 0$$

$$\forall x \ \forall y \ (S(x) \times y = x \times y + y) \rightsquigarrow S(x) \times y \longrightarrow x \times y + y$$

# Récapitulatif

$$\forall x \ x = x$$

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

$$\begin{aligned} & \begin{array}{c} \curvearrowright \\ x \in f_{z, y_1, \dots, y_n, P}(y_1, \dots, y_n) \end{array} \longrightarrow (x/z)P \\ & x = y \longrightarrow \forall p \ (x \in p \Rightarrow y \in p) \end{aligned}$$

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

$$\forall x \ \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$((0/x)P \Rightarrow \forall y \ ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n \ (n/x)P)$$

$$\forall y \ (0 + y = y) \rightsquigarrow 0 + y \longrightarrow y$$

$$\forall x \ \forall y \ (S(x) + y = S(x + y)) \rightsquigarrow S(x) + y \longrightarrow S(x + y)$$

$$\forall y \ (0 \times y = 0) \rightsquigarrow 0 \times y \longrightarrow 0$$

$$\forall x \ \forall y \ (S(x) \times y = x \times y + y) \rightsquigarrow S(x) \times y \longrightarrow x \times y + y$$

# Récapitulatif

$$\forall x \ x = x$$

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

$$\begin{aligned} & \begin{array}{c} \curvearrowright \\ x \in f_{z, y_1, \dots, y_n, P}(y_1, \dots, y_n) \end{array} \longrightarrow (x/z)P \\ & x = y \longrightarrow \forall p \ (x \in p \Rightarrow y \in p) \end{aligned}$$

$$\forall x \ 0 = S(x) \Rightarrow \perp \rightsquigarrow ?$$

$$\forall x \ \forall y \ (S(x) = S(y) \Rightarrow x = y) \rightsquigarrow ?$$

$$((0/x)P \Rightarrow \forall y \ ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n \ (n/x)P) \rightsquigarrow ?$$

$$\forall y \ (0 + y = y) \rightsquigarrow 0 + y \longrightarrow y$$

$$\forall x \ \forall y \ (S(x) + y = S(x + y)) \rightsquigarrow S(x) + y \longrightarrow S(x + y)$$

$$\forall y \ (0 \times y = 0) \rightsquigarrow 0 \times y \longrightarrow 0$$

$$\forall x \ \forall y \ (S(x) \times y = x \times y + y) \rightsquigarrow S(x) \times y \longrightarrow x \times y + y$$

0 n'est pas successeur

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

0 n'est pas successeur

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

Approche naïve

$$0 = S(x) \longrightarrow \perp$$

0 n'est pas successeur

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

Approche naïve

$$0 = S(x) \longrightarrow \perp$$

Perte de la confluence

0 n'est pas successeur

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

Approche naïve

$$0 = S(x) \longrightarrow \perp$$

Perte de la confluence

$$0 = S(x) \longrightarrow \perp$$

0 n'est pas successeur

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

Approche naïve

$$0 = S(x) \longrightarrow \perp$$

Perte de la confluence

$$0 = S(x) \longrightarrow \perp$$

$$0 = S(x) \longrightarrow \forall p \ (0 \in p \Rightarrow S(x) \in p)$$

Un nouveau prédicat

*Null*

# Retrouver la confluence

Un nouveau prédicat

*Null*

2 nouvelles règles de réécriture

au lieu de  $0 = S(x) \longrightarrow \perp$  on choisit

$$Null(S(x)) \longrightarrow \perp$$

# Retrouver la confluence

Un nouveau prédicat

*Null*

2 nouvelles règles de réécriture

au lieu de  $0 = S(x) \longrightarrow \perp$  on choisit

$$Null(S(x)) \longrightarrow \perp$$

On ajoute

$$Null(0) \longrightarrow \top$$

## Injectivité du successeur

$$\forall x \forall y (S(x) = S(y) \Rightarrow x = y)$$

## Injectivité du successeur

$$\forall x \forall y (S(x) = S(y) \Rightarrow x = y)$$

## Approche naïve

$$S(x) = S(y) \longrightarrow x = y$$

## Injectivité du successeur

$$\forall x \forall y (S(x) = S(y) \Rightarrow x = y)$$

## Approche naïve

$$S(x) = S(y) \longrightarrow x = y$$

## Perte de la confluence

## Injectivité du successeur

$$\forall x \forall y (S(x) = S(y) \Rightarrow x = y)$$

## Approche naïve

$$S(x) = S(y) \longrightarrow x = y$$

## Perte de la confluence

$$S(x) = S(y) \longrightarrow x = y$$

## Injectivité du successeur

$$\forall x \forall y (S(x) = S(y) \Rightarrow x = y)$$

## Approche naïve

$$S(x) = S(y) \longrightarrow x = y$$

## Perte de la confluence

$$S(x) = S(y) \longrightarrow x = y$$

$$S(x) = S(y) \longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$$S(x) = S(y)$$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$$S(x) = S(y)$$

$$\longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$$S(x) = S(y)$$

$$\longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$$

On instancie  $p$  à  $f_{z,x,A}$  avec  $A : x = Pred(z)$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$Pred(0) \longrightarrow 0$

$Pred(S(x)) \longrightarrow x$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$S(x) = S(y)$

$\longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$

On instancie  $p$  à  $f_{z,x,A}$  avec  $A : x = Pred(z)$

$\longrightarrow S(x) \in f_{z,A}(x) \Rightarrow S(y) \in f_{z,A}(x)$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$Pred(0) \longrightarrow 0$

$Pred(S(x)) \longrightarrow x$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$S(x) = S(y)$

$\longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$

On instancie  $p$  à  $f_{z,x,A}$  avec  $A : x = Pred(z)$

$\longrightarrow S(x) \in f_{z,A}(x) \Rightarrow S(y) \in f_{z,A}(x)$

$\longrightarrow (S(x)/z)(x = Pred(z)) \Rightarrow (S(y)/z)(x = Pred(z))$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$Pred(0) \longrightarrow 0$

$Pred(S(x)) \longrightarrow x$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$S(x) = S(y)$

$\longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$

On instancie  $p$  à  $f_{z,x,A}$  avec  $A : x = Pred(z)$

$\longrightarrow S(x) \in f_{z,A}(x) \Rightarrow S(y) \in f_{z,A}(x)$

$\longrightarrow (S(x)/z)(x = Pred(z)) \Rightarrow (S(y)/z)(x = Pred(z))$

$\longrightarrow x = Pred(S(x)) \Rightarrow x = Pred(S(y))$

# Retrouver la confluence

Un nouveau symbole de fonction

*Pred*

2 nouvelles règles de réécriture

$Pred(0) \longrightarrow 0$

$Pred(S(x)) \longrightarrow x$

“Simulation” de  $S(x) = S(y) \Rightarrow x = y$

$S(x) = S(y)$

$\longrightarrow \forall p (S(x) \in p \Rightarrow S(y) \in p)$

On instancie  $p$  à  $f_{z,x,A}$  avec  $A : x = Pred(z)$

$\longrightarrow S(x) \in f_{z,A}(x) \Rightarrow S(y) \in f_{z,A}(x)$

$\longrightarrow (S(x)/z)(x = Pred(z)) \Rightarrow (S(y)/z)(x = Pred(z))$

$\longrightarrow x = Pred(S(x)) \Rightarrow x = Pred(S(y))$

$\longrightarrow x = x \Rightarrow x = y$

# L'ESSENTIEL !!!

## Le schéma de récurrence

$$((0/x)P \Rightarrow \forall y ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n (n/x)P)$$

# L'ESSENTIEL !!!

Le schéma de récurrence

$$((0/x)P \Rightarrow \forall y ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n (n/x)P)$$

Il n'y a même pas d'approche naïve !!

# L'ESSENTIEL !!!

Le schéma de récurrence

$$((0/x)P \Rightarrow \forall y ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n (n/x)P)$$

Il n'y a même pas d'approche naïve !!

Où va-t-on bien pouvoir mettre une flèche de réécriture ?...

# Ô Miracle ... On dirait bien les entiers

Un nouveau prédicat : être un entier

$N$

# Ô Miracle ... On dirait bien les entiers

Un nouveau prédicat : être un entier

$N$

On définit  $N$  comme suit

$$\forall n (N(n) \Leftrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p))$$

# Ô Miracle ... On dirait bien les entiers

Un nouveau prédicat : être un entier

$N$

On définit  $N$  comme suit

$$\forall n (N(n) \Leftrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p))$$

On voit mieux où mettre la flèche ;)

$$N(n) \longrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p)$$

# Présentation alternative de l'arithmétique : $HA_{\rightarrow}$

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

$$\begin{array}{l} y = z \longrightarrow \forall p (y \in p \Rightarrow z \in p) \\ x \in f_{z, y_1, \dots, y_n, P}(y_1, \dots, y_n) \longrightarrow (x/z)P \end{array}$$

$$\begin{array}{ll} Pred(0) \longrightarrow 0 & Pred(S(x)) \longrightarrow x \\ Null(0) \longrightarrow \top & Null(S(x)) \longrightarrow \perp \end{array}$$

$$N(n) \longrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p)$$

# Et maintenant ?

Pourquoi ça marche ?

# Et maintenant ?

Pourquoi ça marche ?

L'article propose une succession d'extensions conservatives de HA jusqu'à HA $\rightarrow$

# Et maintenant ?

Pourquoi ça marche ?

L'article propose une succession d'extensions conservatives de HA jusqu'à HA $\rightarrow$

- HA

# Et maintenant ?

Pourquoi ça marche ?

L'article propose une succession d'extensions conservatives de HA jusqu'à  $HA_{\rightarrow}$

- HA
- $HA_{Pred}$

# Et maintenant ?

Pourquoi ça marche ?

L'article propose une succession d'extensions conservatives de HA jusqu'à  $HA_{\rightarrow}$

- HA
- $HA_{Pred}$
- $HA_N$

# Et maintenant ?

Pourquoi ça marche ?

L'article propose une succession d'extensions conservatives de HA jusqu'à  $HA_{\rightarrow}$

- HA
- $HA_{Pred}$
- $HA_N$
- $HA_{Class}$

# Et maintenant ?

Pourquoi ça marche ?

L'article propose une succession d'extensions conservatives de HA jusqu'à  $HA_{\rightarrow}$

- HA
- $HA_{Pred}$
- $HA_N$
- $HA_{Class}$
- $HA_{\rightarrow}$

## Les symboles

0, S, +, × et =

## Les axiomes de l'égalité

$$\forall x \ x = x$$

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

## Les propositions

$$\forall x \ \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \ 0 = S(x) \Rightarrow \perp$$

$$((0/x)P \Rightarrow \forall y \ ((y/x)P \Rightarrow (S(y)/x)P) \Rightarrow \forall n \ (n/x)P)$$

$$\forall y \ (0 + y = y)$$

$$\forall x \ \forall y \ (S(x) + y = S(x + y))$$

$$\forall y \ (0 \times y = 0)$$

$$\forall x \ \forall y \ (S(x) \times y = x \times y + y)$$

## Extension

$$Pred(0) = 0$$

$$Pred(S(x)) = x$$

$$\forall x \forall y (x = y \Rightarrow Pred(x) = Pred(y))$$

## Extension

$$Pred(0) = 0$$

$$Pred(S(x)) = x$$

$$\forall x \forall y (x = y \Rightarrow Pred(x) = Pred(y))$$

## Preuve de la conservativité

Lemme de Skolem :

Si  $\Gamma \vdash \forall x_1 \dots \forall x_n \exists y A$  alors  $\Gamma, (f(x_1, \dots, x_n)/y)A$  est une extension conservative de  $\Gamma$

## Extension

$$Pred(0) = 0$$

$$Pred(S(x)) = x$$

$$\forall x \forall y (x = y \Rightarrow Pred(x) = Pred(y))$$

## Preuve de la conservativité

Lemme de Skolem :

Si  $\Gamma \vdash \forall x_1 \dots \forall x_n \exists y A$  alors  $\Gamma, (f(x_1, \dots, x_n)/y)A$  est une extension conservative de  $\Gamma$

## Application du lemme de Skolem

$$\forall x \exists y ((x = 0 \Rightarrow y = 0) \wedge \forall z (x = S(z) \Rightarrow y = z))$$

$$\forall x ((x = 0 \Rightarrow Pred(x) = 0) \wedge \forall z (x = S(z) \Rightarrow Pred(x) = z))$$

## 2 Nouveaux symboles de prédicat

Null

N

### Système

$$\forall x \ x = x$$

$$\forall x \ \forall y \ x = y \Rightarrow P(x) = P(y)$$

$$(0/x)P \Rightarrow \forall y (N(y) \Rightarrow (y/x)P) \Rightarrow (S(y)/x)P \Rightarrow \forall n (N(n) \Rightarrow (n/x)P)$$

$$Pred(0) = 0$$

$$\forall x (Pred(S(x)) = x)$$

$$N(0)$$

$$\forall x (N(x) \Rightarrow N(S(x)))$$

$$Null(0)$$

$$\forall x (Null(S(x)) \Rightarrow \perp)$$

$$\forall y (0 + y = y)$$

$$\forall x \ \forall y (S(x) + y = S(x + y))$$

$$\forall y (0 \times y = 0)$$

$$\forall x \ \forall y (S(x) \times y = x \times y + y)$$

## Traduction de $HA_{pred}$ à $HA_N$

- $|P| = P$ , if  $P$  is atomic,  $|\top| = \top, A$   $|\perp| = \perp$ ,  
 $|A \wedge B| = |A| \wedge |B|$ ,  $|A \vee B| = |A| \vee |B|$ ,  $|A \Rightarrow B| = |A| \Rightarrow |B|$ ,

## Traduction de $HA_{pred}$ à $HA_N$

- $|P| = P$ , if  $P$  is atomic,  $|\top| = \top, A$   $|\perp| = \perp$ ,  
 $|A \wedge B| = |A| \wedge |B|$ ,  $|A \vee B| = |A| \vee |B|$ ,  $|A \Rightarrow B| = |A| \Rightarrow |B|$ ,
- $|\forall x A| = \forall x (N(x) \Rightarrow |A|)$ ,  $|\exists x A| = \exists x (N(x) \wedge |A|)$ .

## Traduction de $HA_{Pred}$ à $HA_N$

- $|P| = P$ , if  $P$  is atomic,  $|\top| = \top, A$   $|\perp| = \perp$ ,  
 $|A \wedge B| = |A| \wedge |B|$ ,  $|A \vee B| = |A| \vee |B|$ ,  $|A \Rightarrow B| = |A| \Rightarrow |B|$ ,
- $|\forall x A| = \forall x (N(x) \Rightarrow |A|)$ ,  $|\exists x A| = \exists x (N(x) \wedge |A|)$ .

On peut prouver que pour tout axiome  $A$  de  $HA_{Pred}$ ,  $|A|$  est prouvable dans  $HA_N$

Ainsi  $HA_N$  est une **extension** de  $HA_{Pred}$

Preuve de la conservativité : Tous les modèles constructifs de  $HA_{Pred}$  s'étendent en des modèles de  $HA_N$

## Passage à une théorie multi-sortée

On ajoute 2 sortes  $\iota$  et  $\kappa$ , et un symbole  $\in$

### Le langage

$0$	$\iota$	$S$	$\langle \iota, \iota \rangle$
$+$	$\langle \iota, \iota, \iota \rangle$	$\times$	$\langle \iota, \iota, \iota \rangle$
$=$	$\langle \iota, \iota \rangle$	$Null$	$\langle \iota \rangle$
$N$	$\langle \iota \rangle$	$\in$	$\langle \iota, \kappa \rangle$

Pour toute proposition  $P(z, y_1, \dots, y_n)$  du langage, on ajoute un nouveau symbole de fonction de rang  $\langle \iota, \dots, \iota, \kappa \rangle$   $f_{z, y_1, \dots, y_n, P}$

### Modélisation de l'appartenance

$$x \in f_{z, y_1, \dots, y_n, P}(y_1, \dots, y_n) \Leftrightarrow (x/z)P$$

## Les axiomes de HA<sub>Class</sub>

$$\forall y \forall z (y = z \Leftrightarrow \forall p (y \in p \Rightarrow z \in p))$$

$$\forall z \forall y_1 \dots \forall y_n (x \in f_{z, y_1, \dots, y_n} P(y_1, \dots, y_n) \Leftrightarrow (x/z)P)$$

$$\forall n (N(n) \Leftrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p))$$

$$Pred(0) = 0$$

$$\forall x (Pred(S(x)) = x)$$

$$Null(0)$$

$$\forall x (Null(S(x)) \Rightarrow \perp)$$

$$\forall y (0 + y = y)$$

$$\forall x \forall y (S(x) + y = S(x + y))$$

$$\forall y (0 \times y = 0)$$

$$\forall y (S(x) \times y = x \times y + y)$$

## Les axiomes de HA<sub>Class</sub>

$$\forall y \forall z (y = z \Leftrightarrow \forall p (y \in p \Rightarrow z \in p))$$

$$\forall z \forall y_1 \dots \forall y_n (x \in f_{z, y_1, \dots, y_n} P(y_1, \dots, y_n) \Leftrightarrow (x/z)P)$$

$$\forall n (N(n) \Leftrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p))$$

$$Pred(0) = 0$$

$$\forall x (Pred(S(x)) = x)$$

$$Null(0)$$

$$\forall x (Null(S(x)) \Rightarrow \perp)$$

$$\forall y (0 + y = y)$$

$$\forall x \forall y (S(x) + y = S(x + y))$$

$$\forall y (0 \times y = 0)$$

$$\forall y (S(x) \times y = x \times y + y)$$

HA<sub>Class</sub> est une extension conservative de HA<sub>N</sub>

$$x = y \longrightarrow \forall p (x \in p \Rightarrow y \in p)$$

$$x \in f_{z,y_1,\dots,y_n,P}(y_1,\dots,y_n) \longrightarrow (x/z)P$$

$$N(n) \longrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p)$$

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

$$Null(0) \longrightarrow \top$$

$$Null(S(x)) \longrightarrow \perp$$

$$0 + y \longrightarrow y$$

$$S(x) + y \longrightarrow S(x + y)$$

$$0 \times y \longrightarrow 0$$

$$S(x) \times y \longrightarrow x \times y + y$$

# Conclusion

C'est gagné

Nous avons réussi à exprimer l'Arithmétique dans un système purement calculatoire

Le principe de substitutivité : avantages et inconvénients

$$x = y \longrightarrow \forall p (x \in p \Rightarrow y \in p)$$

Le principe de substitutivité : avantages et inconvénients

$$x = y \longrightarrow \forall p (x \in p \Rightarrow y \in p)$$

Objectif

$$S(x) = S(z) \longrightarrow x = y$$

$$0 = 0 \longrightarrow \top$$

$$0 = S(x) \longrightarrow \perp$$

$$S(x) = 0 \longrightarrow \perp$$

Le principe de substitutivité : avantages et inconvénients

$$x = y \longrightarrow \forall p (x \in p \Rightarrow y \in p)$$

Objectif

$$S(x) = S(z) \longrightarrow x = y$$

$$0 = 0 \longrightarrow \top$$

$$0 = S(x) \longrightarrow \perp$$

$$S(x) = 0 \longrightarrow \perp$$

Gains (à vérifier)

*Null* et *Pred*