Stage M2 recherche
Formalisation de concepts mathématiques dans le système Coq

Vincent Demange

paul verlaine
université - metz
ufr mathématique informatique
mécanique et automatique

2 juillet 2008

Sommaire

Sommaire

Motivations / Objectifs

Motivations

- complexification des preuves mathématiques
- complexification des domaines mathématiques

$\Longrightarrow$ vérification mécanique des preuves

Motivations / Objectifs

Motivations

- complexification des preuves mathématiques
- complexification des domaines mathématiques

$\Longrightarrow$ vérification mécanique des preuves

Objectifs du stage

- se familiariser avec un système interactif de preuves
- pour démontrer des théorèmes mathématiques (non triviaux)

$\Longrightarrow$ théorèmes de points fixes dans les treillis avec Coq

Sommaire

Curry, Howard et Coq

Déduction naturelle minimale

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ hyp \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$$

Curry, Howard et Coq

Déduction naturelle minimale

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ hyp \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$$

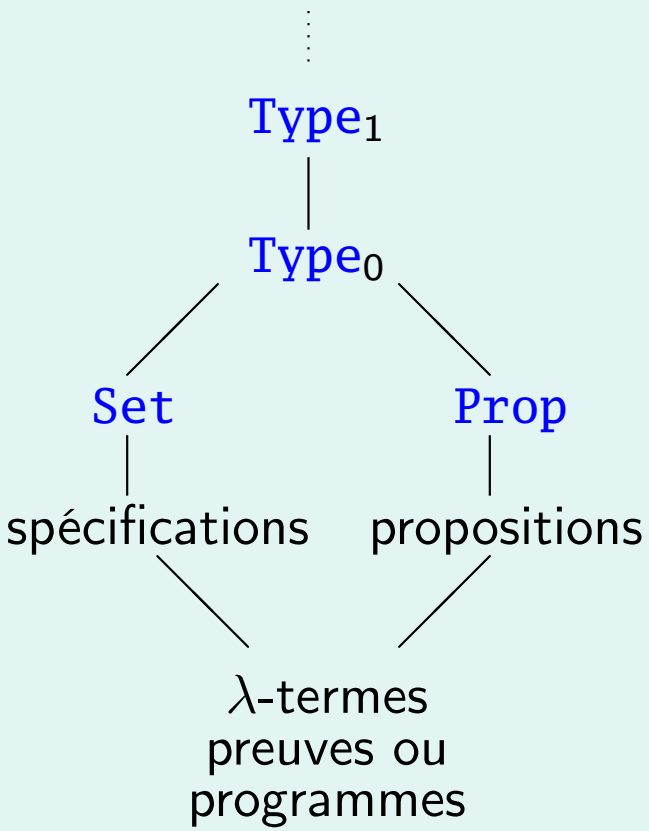
λ-calcul typé minimal

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ var \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \to B}\ \lambda \qquad \frac{\Gamma \vdash f : A \to B \quad \Gamma \vdash x : A}{\Gamma \vdash (f\ x) : B}\ app$$

Curry, Howard et Coq

λ-calcul typé minimal

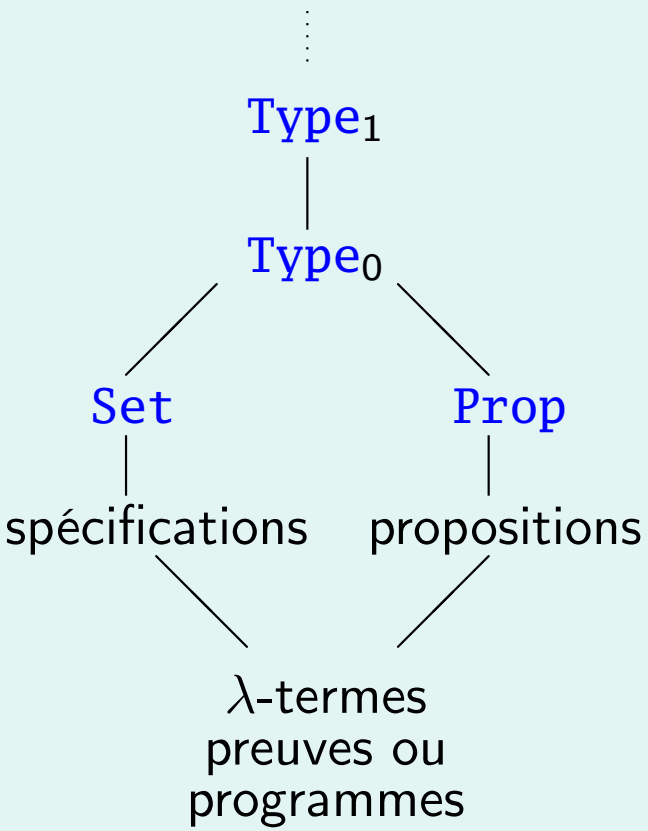
$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ var \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \to B}\ \lambda \qquad \frac{\Gamma \vdash f : A \to B \quad \Gamma \vdash x : A}{\Gamma \vdash (f\ x) : B}\ app$$



Curry, Howard et Coq

λ-calcul typé minimal

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ var \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \to B}\ \lambda \qquad \frac{\Gamma \vdash f : A \to B \quad \Gamma \vdash x : A}{\Gamma \vdash (f\ x) : B}\ app$$



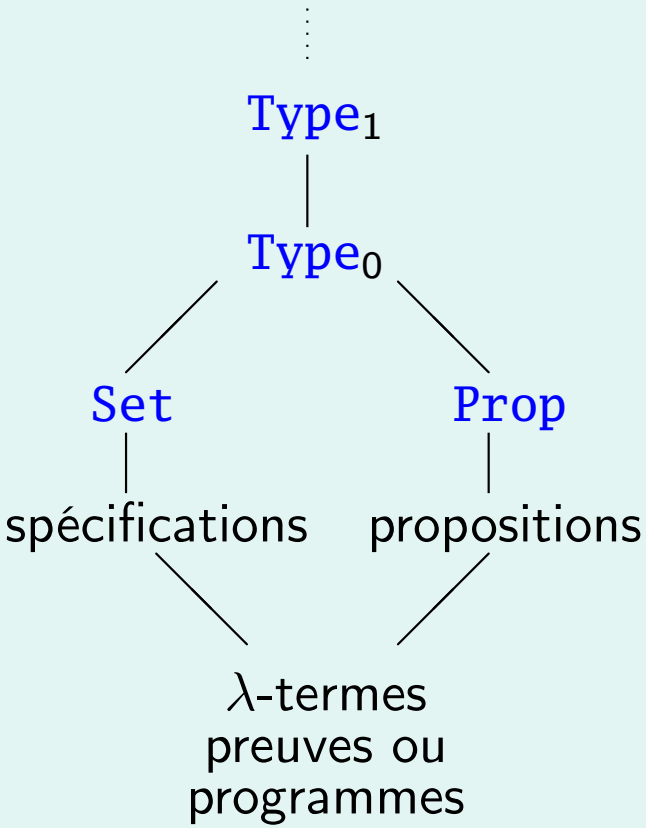
Types dépendants

$$\frac{\Gamma \vdash A : s \qquad \Gamma, a : A \vdash B : s'}{\Gamma \vdash \forall a : A, B : s''}\ Prod(s, s', s'')$$

Curry, Howard et Coq

Abstraction généralisée

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ var \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : \forall x : A, B}\ \lambda \qquad \frac{\Gamma \vdash t : \forall v : A, B \qquad \Gamma \vdash x : A}{\Gamma \vdash t\ x : B[v \leftarrow x]}\ app$$



Types dépendants

$$\frac{\Gamma \vdash A : s \qquad \Gamma, a : A \vdash B : s'}{\Gamma \vdash \forall a : A, B : s''}\ Prod(s, s', s'')$$

Curry, Howard et Coq

Abstraction généralisée

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ var \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : \forall x : A, B}\ \lambda \qquad \frac{\Gamma \vdash t : \forall v : A, B \qquad \Gamma \vdash x : A}{\Gamma \vdash t\ x : B[v \leftarrow x]}\ app$$

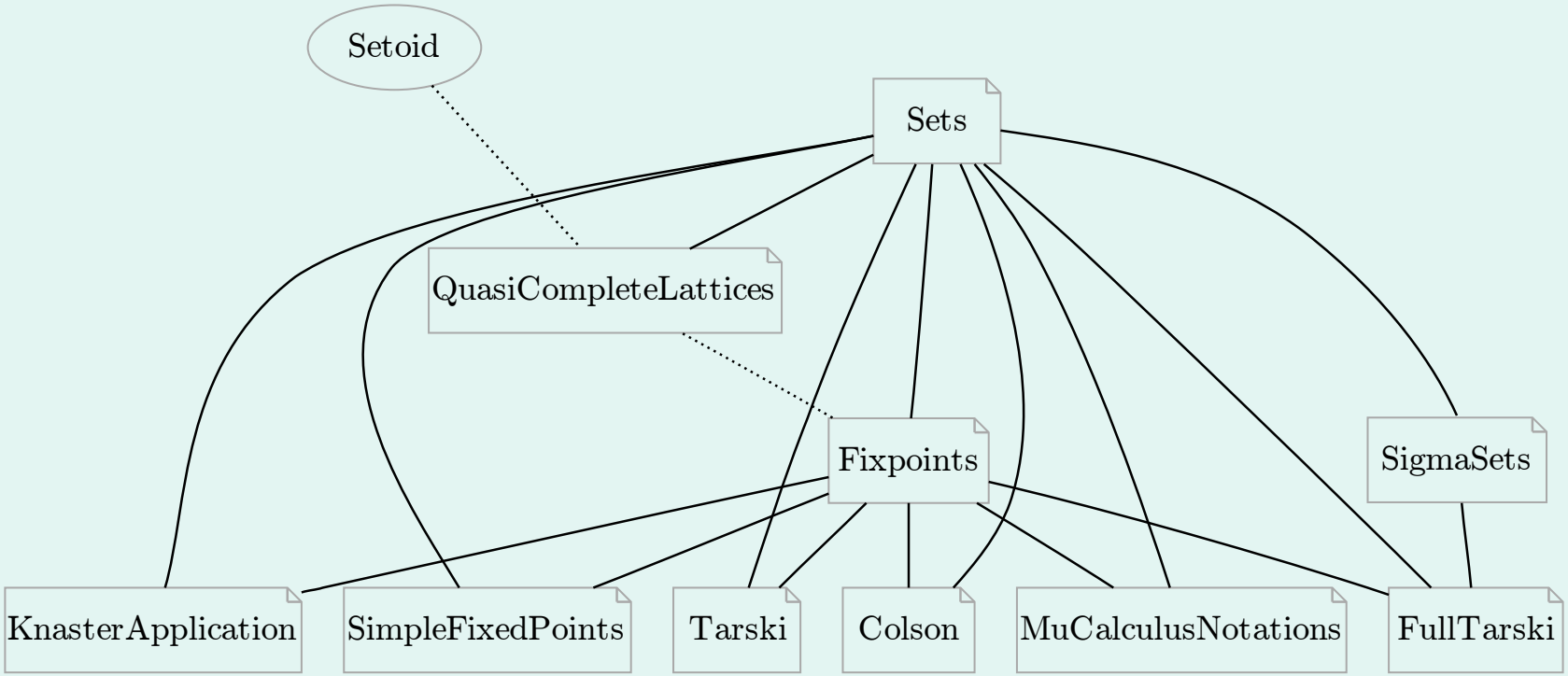
Types dépendants

$$\frac{\Gamma \vdash A : s \qquad \Gamma, a : A \vdash B : s'}{\Gamma \vdash \forall a : A, B : s''}\ Prod(s, s', s'')$$

(Set,Set,Set)	∀ x : Z, nat	Z → nat
(Set,Type,Type)	nat → Prop	prédicat
(Type,Prop,Prop)	∀ P : Prop, P → P	imprédicativité

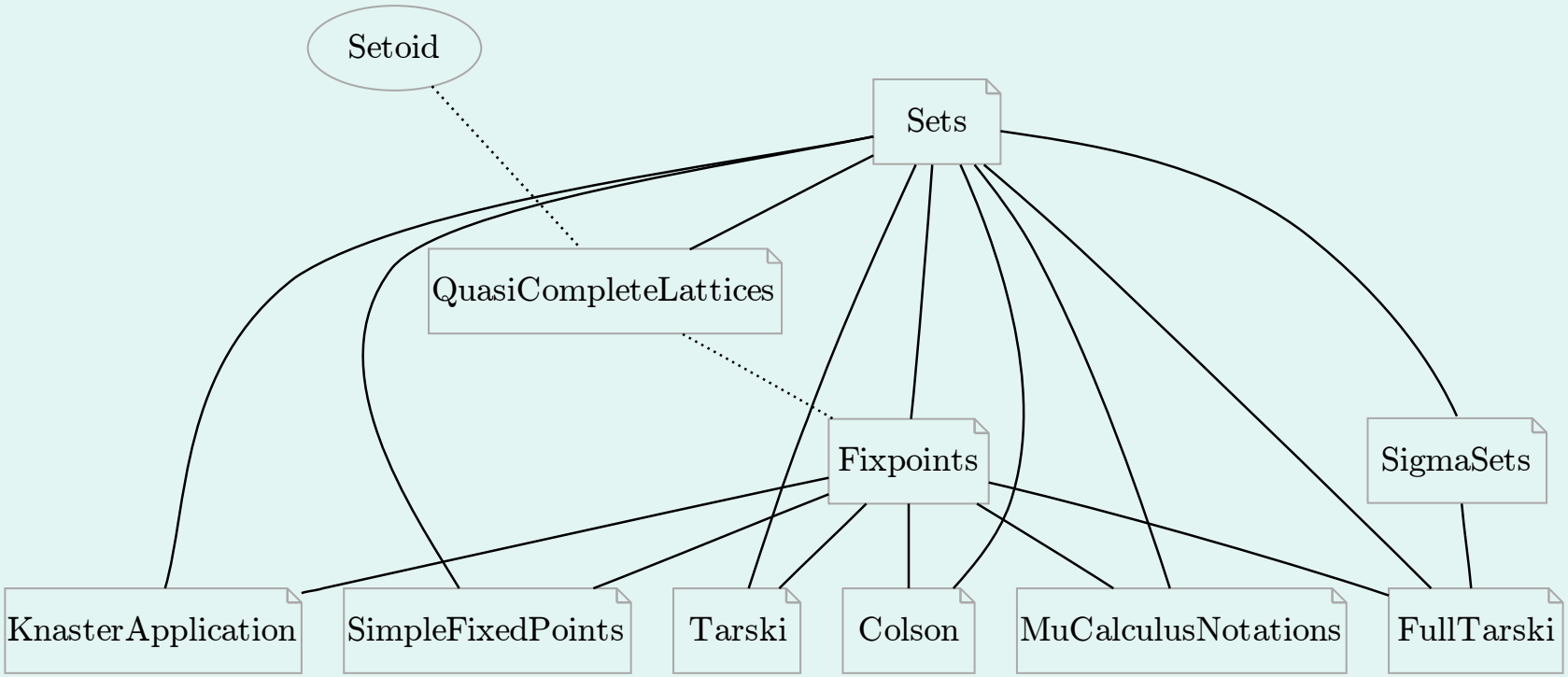
Sommaire

Organisation



2924 lignes de code

Organisation



5 jours (de 8h) pour formaliser une page (Barendregt)

Démonstration

Les notations

symbole	niveau	associativité	portée(s)
F ↔ G	95	no	type_scope
F ∨ G	85	right	type_scope
F ∧ G	80	right	type_scope
¬ F	75	right	type_scope
a = b	70	no	type_scope
m < n	70	no	nat_scope
m > n	70	no	nat_scope
m ≤ n	70	no	nat_scope
m ≥ n	70	no	nat_scope
m + n	50	left	nat_scope
m - n	50	left	nat_scope
m * n	40	left	nat_scope
m / n	40	left	nat_scope
m ^ n	30	right	nat_scope

La dualité

Si $(\Omega, \leq, \bigwedge, \bigvee)$ est un treillis complet, alors $(\Omega, \geq, \bigvee, \bigwedge)$ est un treillis complet.

Conséquences

Si $\forall L, P(L)$, alors $\forall L, P^{\partial}(L)$

où L treillis complet, et
P^{∂} obtenue de P en remplaçant $\leq$ par $\geq$, $\bigwedge$ par $\bigvee$, $\bigvee$ par $\bigwedge$ et réciproquement.

La dualité

Si $(\Omega, \leq, \bigwedge, \bigvee)$ est un treillis complet, alors $(\Omega, \geq, \bigvee, \bigwedge)$ est un treillis complet.

Conséquences

Si $\forall L, P(L)$, alors $\forall L, P^{\partial}(L)$

où L treillis complet, et
P^{∂} obtenue de P en remplaçant $\leq$ par $\geq$, $\bigwedge$ par $\bigvee$, $\bigvee$ par $\bigwedge$ et réciproquement.

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

Remarque préliminaire :

$$x \simeq^d y$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

Remarque préliminaire :

$$x \simeq^d y \quad \rhd_{\delta\beta^*} x \leq^d y \wedge y \leq^d x$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

Remarque préliminaire :

$$x \simeq^d y \quad \begin{array}{l} \rhd_{\delta\beta^*} x \leq^d y \wedge y \leq^d x \\ \rhd^*_{\delta\beta} x \geq y \wedge y \geq x \end{array}$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

Remarque préliminaire :

$$x \simeq^d y \quad \begin{array}{l} \triangleright_{\delta\beta^*} x \leq^d y \wedge y \leq^d x \\ \triangleright^*_{\delta\beta} x \geq y \wedge y \geq x \\ \triangleright^*_{\delta\beta} y \leq x \wedge x \leq y \end{array}$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

Remarque préliminaire :

$$
\begin{aligned}
x \simeq^d y \quad & \rhd_{\delta\beta^*} x \leq^d y \wedge y \leq^d x \\
& \rhd^*_{\delta\beta} x \geq y \wedge y \geq x \\
& \rhd^*_{\delta\beta} y \leq x \wedge x \leq y \\
& \equiv_{\beta\delta} y \simeq x
\end{aligned}
$$

Problème d'unification

Résumé du problème

$\bigwedge^d\{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee\{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

$$\left(\bigwedge\{x; \delta(x) \simeq x\} \simeq fixp_x, \delta(x)\right)^d$$

$$= \bigwedge^d\{x; \delta(x) \simeq^d x\} \simeq^d \bigwedge^d\{x; \delta(x) \leq^d x\}$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

$$\left(\bigwedge \{x; \delta(x) \simeq x\} \simeq fixp_x, \delta(x)\right)^d$$

$$= \bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d \bigwedge^d \{x; \delta(x) \leq^d x\}$$
$$\triangleright \bigwedge^d \{x; \delta(x) \leq^d x\} \simeq \bigwedge^d \{x; \delta(x) \simeq^d x\}$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

$$\left(\bigwedge \{x; \delta(x) \simeq x\} \simeq fixp_x, \delta(x)\right)^d$$

$$= \bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d \bigwedge^d \{x; \delta(x) \leq^d x\}$$
$$\triangleright \bigwedge^d \{x; \delta(x) \leq^d x\} \simeq \bigwedge^d \{x; \delta(x) \simeq^d x\}$$
$$\triangleright \bigvee \{x; x \leq \delta(x)\} \simeq \bigvee \{x; x \simeq \delta(x)\}$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

$$\left(\bigwedge \{x; \delta(x) \simeq x\} \simeq fixp_x, \delta(x)\right)^d$$

$$= \bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d \bigwedge^d \{x; \delta(x) \leq^d x\}$$
$$\triangleright \bigwedge^d \{x; \delta(x) \leq^d x\} \simeq \bigwedge^d \{x; \delta(x) \simeq^d x\}$$
$$\triangleright \bigvee \{x; x \leq \delta(x)\} \simeq \bigvee \{x; x \simeq \delta(x)\}$$
$$\equiv Fixp_x \delta(x) \simeq \bigvee \{x; x \simeq \delta(x)\}$$

Problème d'unification

Résumé du problème

$\bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d fixp_x, \delta(x)$ et
$\bigvee \{x; \delta(x) \simeq x\} \simeq Fixp_x, \delta(x)$ ne *correspondent* pas.

$$\left(\bigwedge \{x; \delta(x) \simeq x\} \simeq fixp_x, \delta(x)\right)^d$$

$$= \bigwedge^d \{x; \delta(x) \simeq^d x\} \simeq^d \bigwedge^d \{x; \delta(x) \leq^d x\}$$
$$\triangleright \bigwedge^d \{x; \delta(x) \leq^d x\} \simeq \bigwedge^d \{x; \delta(x) \simeq^d x\}$$
$$\triangleright \bigvee \{x; x \leq \delta(x)\} \simeq \bigvee \{x; x \simeq \delta(x)\}$$
$$\equiv Fixp_x \delta(x) \simeq \bigvee \{x; x \simeq \delta(x)\}$$

Solution : introduire un lemme technique

$$\bigvee \{x; \delta(x) \simeq x\} \simeq \bigvee \{x; x \simeq \delta(x)\}$$

Sommaire

Conclusion sur le travail

- formaliser de façon détaillée,
- proche du langage naturel,
- de façon réutilisable
- des théorèmes non triviaux

c'est possible !

Conclusion sur le travail

- formaliser de façon détaillée,
- proche du langage naturel,
- de façon réutilisable
- des théorèmes non triviaux

c'est possible !

$\Longrightarrow$ compétences pluridisciplinaires

Travaux futurs

- formaliser toujours plus
- de façon encore plus naturelle
- et ajouter plus de procédures d'automatisation

Exemple de Buchberger

- formaliser tous les articles d'un journal
- organisés dans des bases de données actives
- pour faciliter l'accès intelligent aux connaissances

$\Longrightarrow$ modification du processus de publication

Travaux futurs

- formaliser toujours plus
- de façon encore plus naturelle
- et ajouter plus de procédures d'automatisation

Exemple de Buchberger

- formaliser tous les articles d'un journal
- organisés dans des bases de données actives
- pour faciliter l'accès intelligent aux connaissances

$\Longrightarrow$ modification du processus de publication

Travaux futurs

- formaliser toujours plus
- de façon encore plus naturelle
- et ajouter plus de procédures d'automatisation

Exemple de Buchberger

- formaliser tous les articles d'un journal
- organisés dans des bases de données actives
- pour faciliter l'accès intelligent aux connaissances

$\Longrightarrow$ modification du processus de publication

Merci de votre attention, des questions ?