

# Déduction modulo théorie et variantes

David Delahaye

Faculté des Sciences  
[David.Delahaye@lirmm.fr](mailto:David.Delahaye@lirmm.fr)

Master M2 2018-2019

# Déduction modulo théorie

## Une preuve c'est quoi ?

- Comment démontrer  $2 + 2 = 4$  ?
- Point de vue des Babyloniens : c'est du calcul !
- Point de vue des Grecs : c'est de la déduction !

## Une preuve

- C'est un peu des deux ;
- Les systèmes de preuve n'incluent pas la notion de calcul.

## Déduction modulo théorie

- Faire la part du calcul et de la déduction (dichotomie) ;
- Raisonner modulo une congruence sur les propositions.

# Axiomes ou pas axiomes ?

## Place des axiomes ?

- Les laisser parmi la liste des hypothèses ?
- Explosion combinatoire dans l'espace de recherche de preuve ;
- Pas d'indications pour outils de déduction automatique.

## Une solution : les solveurs SMT

- SMT = « Satisfiability Modulo Theories » ;
- Combinaison d'un solveur SAT (DPLL) et de plugins de théories ;
- Mais :
  - ▶ Procédures de décision spécifiques pour chaque théorie donnée ;
  - ▶ Contrainte de décidabilité des théories ;
  - ▶ Manque d'automatisabilité et de généralité.

# Axiomes ou pas axiomes ?

## Déduction modulo théorie

- Transformer les axiomes en règles de réécriture ;
- Changer la recherche de preuves avec axiomes en calculs ;
- Éviter l'explosion combinatoire dans la recherche de preuve ;
- Réduire la taille des preuves (on ne garde que les étapes significatives).

# Déduction modulo théorie

## Inclusion

$$\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Preuve en calcul des séquents

$$\frac{\frac{\frac{\dots, x \in A \vdash A \subseteq A, x \in A}{\dots \vdash A \subseteq A, x \in A \Rightarrow x \in A} \Rightarrow R}{\dots \vdash A \subseteq A, \forall x. x \in A \Rightarrow x \in A} \forall R}{\dots, (\forall x. x \in A \Rightarrow x \in A) \Rightarrow A \subseteq A \vdash A \subseteq A} \Rightarrow L}{\frac{A \subseteq A \Leftrightarrow \forall x. x \in A \Rightarrow x \in A \vdash A \subseteq A}{\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b \vdash A \subseteq A} \wedge L}{\forall L \times 2}$$

# Déduction modulo théorie

## Inclusion

$$\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Règle de réécriture

$$a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Preuve en déduction modulo théorie

$$\frac{\frac{\frac{}{x \in A \vdash x \in A} \text{Ax}}{\vdash x \in A \Rightarrow x \in A} \Rightarrow R}{\vdash A \subseteq A} \forall R \quad (A \subseteq A \longrightarrow \forall x. x \in A \Rightarrow x \in A)}$$

# Dédution modulo théorie

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Règle de réécriture

$$a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Preuve en déduction modulo théorie

$$\frac{\frac{\frac{}{x \in A \vdash x \in A} \text{Ax}}{\vdash x \in A \Rightarrow x \in A} \Rightarrow R}{\vdash A \subseteq A} \forall R \quad (A \subseteq A \longrightarrow \forall x. x \in A \Rightarrow x \in A)}$$

# Déduction modulo théorie

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Règle de réécriture

$$a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Preuve en déduction modulo théorie

$$\frac{\frac{\frac{}{x \in A \vdash x \in A} \text{Ax}}{\vdash x \in A \Rightarrow x \in A} \Rightarrow R}{\vdash A \subseteq A} \forall R \quad (A \subseteq A \longrightarrow \forall x. x \in A \Rightarrow x \in A)}$$



# Déduction modulo théorie

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Règle de réécriture

$$a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Preuve en déduction modulo théorie

$$\frac{\frac{\overline{x \in A \vdash x \in A} \text{ Ax}}{\vdash x \in A \Rightarrow x \in A} \Rightarrow R}{\vdash A \subseteq A} \forall R (A \subseteq A \longrightarrow \forall x. x \in A \Rightarrow x \in A)$$

# Superdédution (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Preuve en calcul des séquents

$$\frac{\frac{\frac{\dots, x \in A \vdash A \subseteq A, x \in A}{\dots \vdash A \subseteq A, x \in A \Rightarrow x \in A} \Rightarrow R}{\dots \vdash A \subseteq A, \forall x. x \in A \Rightarrow x \in A} \forall R}{\dots, (\forall x. x \in A \Rightarrow x \in A) \Rightarrow A \subseteq A \vdash A \subseteq A} \Rightarrow L}{\frac{A \subseteq A \Leftrightarrow \forall x. x \in A \Rightarrow x \in A \vdash A \subseteq A}{\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b \vdash A \subseteq A} \wedge L}{\forall L \times 2}$$

# Superdéduction (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Calcul de la règle de superdéduction

## Preuve en superdéduction

$$\frac{x \in A \vdash x \in A}{\vdash A \subseteq A} \begin{array}{l} Ax \\ \text{IncR} \end{array}$$

# Superdéduction (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Calcul de la règle de superdéduction

## Preuve en superdéduction

$$\frac{x \in A \vdash x \in A}{\vdash A \subseteq A} \begin{array}{l} Ax \\ \text{IncR} \end{array}$$

# Superdédution (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Calcul de la règle de superdédution

$$\frac{\Gamma \vdash \forall x (x \in a \Rightarrow x \in b), \Delta}{\Gamma \vdash a \subseteq b, \Delta}$$

## Preuve en superdédution

$$\frac{\frac{x \in A \vdash x \in A}{\vdash A \subseteq A}}{\text{Ax}} \text{IncR}$$

# Superdédution (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Calcul de la règle de superdédution

$$\frac{\frac{\Gamma, x \in a \vdash x \in b, \Delta}{\Gamma \vdash x \in a \Rightarrow x \in b, \Delta} \Rightarrow R}{\Gamma \vdash \forall x (x \in a \Rightarrow x \in b), \Delta} \forall R, x \notin \Gamma, \Delta} \Gamma \vdash a \subseteq b, \Delta$$

## Preuve en superdédution

$$\frac{x \in A \vdash x \in A}{\vdash A \subseteq A} \begin{array}{l} Ax \\ IncR \end{array}$$

# Superdédution (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Calcul de la règle de superdédution

$$\frac{\Gamma, x \in a \vdash x \in b, \Delta}{\Gamma \vdash a \subseteq b, \Delta} \text{IncR}, x \notin \Gamma, \Delta$$

## Preuve en superdédution

$$\frac{\frac{x \in A \vdash x \in A}{\vdash A \subseteq A}}{\text{Ax}} \text{IncR}$$

# Superdédution (variante)

## Inclusion

$$\forall a. \forall b. a \subseteq b \longrightarrow \forall x. x \in a \Rightarrow x \in b$$

## Calcul de la règle de superdédution

$$\frac{\Gamma, x \in a \vdash x \in b, \Delta}{\Gamma \vdash a \subseteq b, \Delta} \text{IncR}, x \notin \Gamma, \Delta$$

## Preuve en superdédution

$$\frac{\overline{x \in A \vdash x \in A}}{\vdash A \subseteq A} \begin{array}{l} \text{Ax} \\ \text{IncR} \end{array}$$



## Théorie des ensembles (déduction modulo théorie)

- Axiomes :
  - ▶  $\forall s, t. s = t \Leftrightarrow \forall x. x \in s \Leftrightarrow x \in t$ ;
  - ▶  $\forall s, t, x. x \in s \cap t \Leftrightarrow x \in s \wedge x \in t$ ;
  - ▶  $\forall s, t, x. x \in s \cup t \Leftrightarrow x \in s \vee x \in t$ .
- Transformer ces axiomes en règles de réécriture ;
- Démontrer dans cette théorie avec règles de réécriture :
  - ▶  $\forall a, b, c. a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$  ;
  - ▶  $\forall a, b, c. a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$ .

## Théorie des ensembles (superdédution)

- Axiomes :
  - ▶  $\forall s, t. s = t \Leftrightarrow \forall x. x \in s \Leftrightarrow x \in t$ ;
  - ▶  $\forall s, t, x. x \in s \cap t \Leftrightarrow x \in s \wedge x \in t$ ;
  - ▶  $\forall s, t, x. x \in s \cup t \Leftrightarrow x \in s \vee x \in t$ .
- Transformer ces axiomes en règles de superdédution (deux règles par axiome, une règle gauche et une règle droite) ;
- Démontrer dans cette théorie avec superdédution :
  - ▶  $\forall a, b, c. a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$  ;
  - ▶  $\forall a, b, c. a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$ .

# Tableaux et superdédution

## Règles de clôture et règles analytiques

$$\frac{\perp}{\odot} \odot_{\perp}$$

$$\frac{\neg\top}{\odot} \odot_{\neg\top}$$

$$\frac{P \quad \neg P}{\odot} \odot$$

$$\frac{\neg\neg P}{P} \alpha_{\neg\neg}$$

$$\frac{P \Leftrightarrow Q}{\neg P, \neg Q \mid P, Q} \beta_{\Leftrightarrow}$$

$$\frac{\neg(P \Leftrightarrow Q)}{\neg P, Q \mid P, \neg Q} \beta_{\neg\Leftrightarrow}$$

$$\frac{P \wedge Q}{P, Q} \alpha_{\wedge}$$

$$\frac{\neg(P \vee Q)}{\neg P, \neg Q} \alpha_{\neg\vee}$$

$$\frac{\neg(P \Rightarrow Q)}{P, \neg Q} \alpha_{\neg\Rightarrow}$$

$$\frac{P \vee Q}{P \mid Q} \beta_{\vee}$$

$$\frac{\neg(P \wedge Q)}{\neg P \mid \neg Q} \beta_{\neg\wedge}$$

$$\frac{P \Rightarrow Q}{\neg P \mid Q} \beta_{\Rightarrow}$$

# Tableaux et superdédution

## $\delta/\gamma$ -règles

$$\frac{\exists x.P(x)}{P(\epsilon(x).P(x))} \delta_{\exists}$$

$$\frac{\neg \forall x.P(x)}{\neg P(\epsilon(x).\neg P(x))} \delta_{\neg \forall}$$

$$\frac{\forall x.P(x)}{P(X)} \gamma_{\forall M}$$

$$\frac{\neg \exists x.P(x)}{\neg P(X)} \gamma_{\neg \exists M}$$

$$\frac{\forall x.P(x)}{P(t)} \gamma_{\forall inst}$$

$$\frac{\neg \exists x.P(x)}{\neg P(t)} \gamma_{\neg \exists inst}$$

## Calcul des règles de superdédution

- $\mathcal{S} \equiv$  règles de clôture, règles analytiques, règles  $\delta$ ,  $\gamma_{\forall M}$  et  $\gamma_{\neg\exists M}$  ;
- Axiome :  $R : P \longrightarrow \varphi$  ;
- Une règle de superdédution positive  $R$  (et une négative  $\neg R$ ) :
  - ▶ Initialiser la procédure avec la formule  $\varphi$  ;
  - ▶ Appliquer les règles de  $\mathcal{S}$  jusqu'à ce que plus aucune ne s'applique ;
  - ▶ Collecter les prémisses et la conclusion, et remplacer  $\varphi$  par  $P$ .
- S'il y a des métavariabes, ajouter une règle d'instanciation  $R_{\text{inst}}$  (ou  $\neg R_{\text{inst}}$ ).

# Tableaux et superdédution

## Exemple (inclusion)

$$\frac{\frac{\forall x (x \in a \Rightarrow x \in b)}{X \in a \Rightarrow X \in b} \gamma_{\forall M}}{X \notin a \mid X \in b} \beta \Rightarrow$$

$$\frac{a \subseteq b}{X \notin a \mid X \in b} \text{Inc}$$

$$\frac{a \subseteq b}{t \notin a \mid t \in b} \text{Inc}_{\text{inst}}$$

$$\frac{\frac{\neg \forall x (x \in a \Rightarrow x \in b)}{\neg (\epsilon_x \in a \Rightarrow \epsilon_x \in b)} \delta_{\neg \forall}}{\epsilon_x \in a, \epsilon_x \notin b} \alpha_{\neg \Rightarrow}$$

avec  $\epsilon_x = \epsilon(x). \neg(x \in a \Rightarrow x \in b)$

$$\frac{a \not\subseteq b}{\epsilon_x \in a, \epsilon_x \notin b} \neg \text{Inc}$$

avec  $\epsilon_x = \epsilon(x). \neg(x \in a \Rightarrow x \in b)$

# Tableaux et superdédution

## Exemple de recherche de preuve

- Avec les règles classiques des tableaux :

$$\frac{\frac{\frac{\frac{\forall a \forall b ((a \subseteq b) \Leftrightarrow (\forall x (x \in a \Rightarrow x \in b))) , A \not\subseteq A}{(X \subseteq Y) \Leftrightarrow (\forall x (x \in X \Rightarrow x \in Y))} \gamma_{\forall M} \times 2}{X \subseteq Y, \forall x (x \in X \Rightarrow x \in Y)} \Pi'}{\frac{(A \subseteq A) \Leftrightarrow (\forall x (x \in A \Rightarrow x \in A))}{A \subseteq A, \forall x (x \in A \Rightarrow x \in A)} \beta_{\Leftrightarrow}} \beta_{\Leftrightarrow} \Pi \quad \odot$$

Où  $\Pi$  est :

$$\frac{\frac{\frac{A \not\subseteq A, \neg \forall x (x \in A \Rightarrow x \in A)}{\neg (\epsilon_x \in A \Rightarrow \epsilon_x \in A)} \delta_{\neg \forall}}{\epsilon_x \in A, \epsilon_x \notin A} \alpha_{\neg \Rightarrow}}{\odot} \odot$$

avec  $\epsilon_x = \epsilon(x). \neg(x \in A \Rightarrow x \in A)$

# Tableaux et superdédution

## Exemple de recherche de preuve

- Avec les règles classiques des tableaux :

$$\frac{\frac{\frac{\forall a \forall b ((a \subseteq b) \Leftrightarrow (\forall x (x \in a \Rightarrow x \in b))) , A \not\subseteq A}{(A \subseteq A) \Leftrightarrow (\forall x (x \in A \Rightarrow x \in A))} \gamma_{\forall \text{inst}} \times 2}{\frac{A \subseteq A, \forall x (x \in A \Rightarrow x \in A)}{\quad} \Pi \quad \beta_{\Leftrightarrow}}{\quad} \odot$$

Où  $\Pi$  est :

$$\frac{\frac{\frac{A \not\subseteq A, \neg \forall x (x \in A \Rightarrow x \in A)}{\neg(\epsilon_x \in A \Rightarrow \epsilon_x \in A)} \delta_{\neg \forall}}{\frac{\epsilon_x \in A, \epsilon_x \notin A}{\quad} \alpha_{\neg \Rightarrow}}{\quad} \odot$$

avec  $\epsilon_x = \epsilon(x) . \neg(x \in A \Rightarrow x \in A)$



# Tableaux et superdédution

## Exemple de recherche de preuve

- Avec les règles de superdédution :

$$\frac{\frac{A \not\subseteq A}{\epsilon_x \in A, \epsilon_x \notin A} \neg\text{Inc}}{\odot} \odot$$

avec  $\epsilon_x = \epsilon(x). \neg(x \in A \Rightarrow x \in A)$

## Théorie des ensembles (tableaux et superdédution)

- Axiomes :
  - ▶  $\forall s, t. s = t \Leftrightarrow \forall x. x \in s \Leftrightarrow x \in t$ ;
  - ▶  $\forall s, t, x. x \in s \cap t \Leftrightarrow x \in s \wedge x \in t$ ;
  - ▶  $\forall s, t, x. x \in s \cup t \Leftrightarrow x \in s \vee x \in t$ .
- Transformer ces axiomes en règles de superdédution pour les tableaux selon la méthode vue précédemment ;
- Démontrer en utilisant les tableaux et ces nouvelles règles :
  - ▶  $\forall a, b, c. a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ ;
  - ▶  $\forall a, b, c. a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$ .

## Algorithme d'unification de Robinson

- $G\{s_1 = t_1, \dots, s_n = t_n\} \leftrightarrow \{x_1 = u_1, \dots, x_m = u_m\}$   
où  $x_i$  sont des variables distinctes et  $x_i \notin u_j$ ;
- Règles :
  - ▶  $G \cup \{t = t\} \leftrightarrow G$  (delete);
  - ▶  $G \cup \{f(s_1, \dots, s_n) = f(t_1, \dots, t_n)\} \leftrightarrow G \cup \{s_1 = t_1, \dots, s_n = t_n\}$   
(decompose);
  - ▶  $G \cup \{f(s_1, \dots, s_n) = g(t_1, \dots, t_m)\} \leftrightarrow \perp$ , si  $f \neq g$  ou  $n \neq m$   
(conflict);
  - ▶  $G \cup \{f(s_1, \dots, s_n) = x\} \leftrightarrow G \cup \{x = f(s_1, \dots, s_n)\}$  (swap);
  - ▶  $G \cup \{x = t\} \leftrightarrow G[t/x] \cup \{x = t\}$ , si  $x \notin t$  et  $x \in G$  (eliminate);
  - ▶  $G \cup \{x = f(s_1, \dots, s_n)\} \leftrightarrow \perp$ , si  $x \in f(s_1, \dots, s_n)$  (check).