Déduction modulo théorie et variantes

David Delahaye

Faculté des Sciences
David.Delahaye@lirmm.fr

Master M2 2020-2021

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 généricité.

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, x \in A \vdash A \subseteq A, x \in A}\,\mathrm{ax}}{\ldots \vdash A \subseteq A, x \in A \Rightarrow x \in A}\,\Rightarrow_{\mathrm{right}}}{\ldots \vdash A \subseteq A, \forall x. x \in A \Rightarrow x \in A}\,\forall_{\mathrm{right}} \qquad \dfrac{}{\ldots, A \subseteq A \vdash A \subseteq A}\,\mathrm{ax}}{\dfrac{\ldots, (\forall x. x \in A \Rightarrow x \in A) \Rightarrow A \subseteq A \vdash A \subseteq A}{A \subseteq A \Leftrightarrow \forall x. x \in A \Rightarrow x \in A \vdash A \subseteq A}\,\wedge_{\mathrm{left}}}\,\Rightarrow_{\mathrm{left}}}{\forall a. \forall b. a \subseteq b \Leftrightarrow \forall x. x \in a \Rightarrow x \in b \vdash A \subseteq A}\,\forall_{\mathrm{left}} \times 2$$

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

$$\dfrac{\dfrac{\dfrac{}{x \in A \vdash x \in A}\ \text{ax}}{\vdash x \in A \Rightarrow x \in A}\ \Rightarrow_{\text{right}}}{\vdash A \subseteq A}\ \forall_{\text{right}}\ (A \subseteq A \longrightarrow \forall x.x \in A \Rightarrow x \in A)$$

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

$$\dfrac{\dfrac{\dfrac{}{x \in A \vdash x \in A}\text{ax}}{\vdash x \in A \Rightarrow x \in A}\Rightarrow_{\text{right}}}{\vdash A \subseteq A}\forall_{\text{right}}\ (A \subseteq A \longrightarrow \forall x.x \in A \Rightarrow x \in A)$$

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

$$\cfrac{\cfrac{\cfrac{}{x \in A \vdash x \in A}\text{ax}}{\vdash x \in A \Rightarrow x \in A}\Rightarrow_{\text{right}}}{\vdash A \subseteq A}\forall_{\text{right}}\ (A \subseteq A \longrightarrow \forall x.x \in A \Rightarrow x \in A)$$

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

$$\cfrac{\cfrac{\cfrac{}{x \in A \vdash x \in A}\ \text{ax}}{\vdash x \in A \Rightarrow x \in A}\ \Rightarrow_{\text{right}}}{\vdash A \subseteq A}\ \forall_{\text{right}}\ (A \subseteq A \longrightarrow \forall x.x \in A \Rightarrow x \in A)$$

Superdéduction (variante)

Inclusion

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

Preuve en calcul des séquents

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, x \in A \vdash A \subseteq A, x \in A}\;\mathrm{ax}}{\ldots \vdash A \subseteq A, x \in A \Rightarrow x \in A}\;\Rightarrow_{\mathrm{right}}}{\ldots \vdash A \subseteq A, \forall x.x \in A \Rightarrow x \in A}\;\forall_{\mathrm{right}} \qquad \dfrac{}{\ldots, A \subseteq A \vdash A \subseteq A}\;\mathrm{ax}}{\dfrac{\ldots, (\forall x.x \in A \Rightarrow x \in A) \Rightarrow A \subseteq A \vdash A \subseteq A}{A \subseteq A \Leftrightarrow \forall x.x \in A \Rightarrow x \in A \vdash A \subseteq A}\;\wedge_{\mathrm{left}}}\;\Rightarrow_{\mathrm{left}}}{\forall a.\forall b.a \subseteq b \Leftrightarrow \forall x.x \in a \Rightarrow x \in b \vdash A \subseteq A}\;\forall_{\mathrm{left}} \times 2$$

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

$$\dfrac{\dfrac{}{x \in A \vdash x \in A}\,\text{ax}}{\vdash A \subseteq A}\,\subseteq_{\text{right}}$$

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

$$\dfrac{\dfrac{}{x \in A \vdash x \in A}\,\text{ax}}{\vdash A \subseteq A}\,\subseteq_{\text{right}}$$

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

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

Preuve en superdéduction

$$\dfrac{\dfrac{}{x \in A \vdash x \in A}\,\text{ax}}{\vdash A \subseteq A}\,\subseteq_{\text{right}}$$

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

$$\dfrac{\dfrac{\dfrac{\Gamma, x \in a \vdash x \in b, \Delta}{\Gamma \vdash x \in a \Rightarrow x \in b, \Delta}\Rightarrow_{\text{right}}}{\Gamma \vdash \forall x\,(x \in a \Rightarrow x \in b), \Delta}\forall_{\text{right}},\ x \notin \Gamma, \Delta}{\Gamma \vdash a \subseteq b, \Delta}$$

Preuve en superdéduction

$$\dfrac{\dfrac{}{x \in A \vdash x \in A}\text{ax}}{\vdash A \subseteq A}\subseteq_{\text{right}}$$

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

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

Preuve en superdéduction

$$\dfrac{\dfrac{}{x \in A \vdash x \in A}\ \text{ax}}{\vdash A \subseteq A}\ \subseteq_{\text{right}}$$

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

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

Preuve en superdéduction

$$\cfrac{\cfrac{}{x \in A \vdash x \in A}\,\text{ax}}{\vdash A \subseteq A} \subseteq_{\text{right}}$$

Exercice

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 :
  - $\forall a, b, c. a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$;
  - $\forall a, b, c. a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

Exercice

Théorie des ensembles (superdéduction)

- 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 superdéduction (deux règles par axiome, une règle gauche et une règle droite) ;
- Démontrer dans cette théorie avec superdéduction :
  - $\forall a, b, c.a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$;
  - $\forall a, b, c.a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

Tableaux et superdéduction

Règles de clôture et règles analytiques

$$\frac{\bot}{\odot}\ \odot_{\bot} \qquad \frac{\neg\top}{\odot}\ \odot_{\neg\top} \qquad \frac{P \qquad \neg P}{\odot}\ \odot$$

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

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

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

Tableaux et superdéduction

δ/γ-règles

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

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

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

Tableaux et superdéduction

Calcul des règles de superdéduction

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

Tableaux et superdéduction

Exemple (inclusion)

$$\dfrac{\dfrac{\forall x. x \in a \Rightarrow x \in b}{X \in a \Rightarrow X \in b}\,\gamma_{\forall M}}{X \notin a \mid X \in b}\,\beta_{\Rightarrow}$$

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

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

$$\dfrac{a \subseteq b}{X \notin a \mid X \in b}\,\subseteq$$

$$\dfrac{a \not\subseteq b}{\epsilon_x \in a, \epsilon_x \notin b}\,\neg\subseteq$$

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

$$\dfrac{a \subseteq b}{t \notin a \mid t \in b}\,\subseteq_{\text{inst}}$$

Tableaux et superdéduction

Exemple de recherche de preuve

- Avec les règles classiques des tableaux :

$$
\dfrac{\dfrac{\forall a.\forall b.a \subseteq b \Leftrightarrow \forall x.x \in a \Rightarrow x \in b, A \not\subseteq A}{X \subseteq Y \Leftrightarrow \forall x.x \in X \Rightarrow x \in Y}\ \gamma_{\forall M} \times 2}{\dfrac{\dfrac{X \subseteq Y, \forall x.x \in X \Rightarrow x \in Y}{A \subseteq A \Leftrightarrow \forall x.x \in A \Rightarrow x \in A}\ \gamma_{\forall \mathrm{inst}} \times 2}{\dfrac{A \subseteq A, \forall x.x \in A \Rightarrow x \in A}{\odot}\ \odot \qquad \Pi}\ \beta_{\Leftrightarrow} \qquad \Pi'}\ \beta_{\Leftrightarrow}
$$

Où Π est :

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

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

Tableaux et superdéduction

Exemple de recherche de preuve

- Avec les règles classiques des tableaux :

$$\cfrac{\forall a.\forall b.a \subseteq b \Leftrightarrow \forall x.x \in a \Rightarrow x \in b, A \not\subseteq A}{\cfrac{A \subseteq A \Leftrightarrow \forall x.x \in A \Rightarrow x \in A}{\cfrac{A \subseteq A, \forall x.x \in A \Rightarrow x \in A}{\odot}\ \odot \qquad \Pi}\ \beta_{\Leftrightarrow}}\ \gamma_{\forall\text{inst}} \times 2$$

Où Π est :

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

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

Tableaux et superdéduction

Exemple de recherche de preuve

- Avec les règles de superdéduction :

$$\dfrac{\dfrac{A \not\subseteq A}{\epsilon_x \in A, \epsilon_x \notin A}\ \neg\subseteq}{\odot}\ \odot$$

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

Exercice

Théorie des ensembles (tableaux et superdéduction)

- 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 superdéduction pour les tableaux selon la méthode vue précédemment ;
- Démontrer en utilisant les tableaux et ces nouvelles règles :
  - $\forall a, b, c. a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$;
  - $\forall a, b, c. a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

Projet

Algorithme d'unification de Robinson

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