Systèmes Canoniques Abstraits : Application à la Complétion et à la Déduction Modulo

Séminaire PROTHEO

Guillaume Burel

LORIA – Équipe PROTHEO
Encadrant : Claude Kirchner

Jeudi 3 Novembre 2005

Première partie I

Soutenance de stage de mastère

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]
- résolution [ordonnée, avec sélection, ...]

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\rightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]
- résolution [ordonnée, avec sélection, ...]

Différentes représentations des preuves mais une notion commune : certaines preuves sont « meilleures » que d'autres :

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]
- résolution [ordonnée, avec sélection, ...]

Différentes représentations des preuves mais une notion commune : certaines preuves sont « meilleures » que d'autres : preuves sans coupures

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]
- résolution [ordonnée, avec sélection, ...]

Différentes représentations des preuves mais une notion commune : certaines preuves sont « meilleures » que d'autres : preuves sans coupures, preuves par réécriture (en « vallée »)

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]
- résolution [ordonnée, avec sélection, ...]

Différentes représentations des preuves mais une notion commune : certaines preuves sont « meilleures » que d'autres : preuves sans coupures, preuves par réécriture, preuves qui appliquent la résolution sur les grands atomes en premier.

Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques

- calcul des séquents $\longrightarrow$ calcul des constructions [inductives, algébriques, ...]
- complétion [close, standard, modulo, ...]
- résolution [ordonnée, avec sélection, ...]

Différentes représentations des preuves mais une notion commune : certaines preuves sont « meilleures » que d'autres : preuves sans coupures, preuves par réécriture, preuves qui appliquent la résolution sur les grands atomes en premier.

Cadre des systèmes canoniques abstraits (S.C.A.) introduit par [Dershowitz et Kirchner, 2004] : la notion de bonne preuve est traduite par un ordre sur les preuves.

Introduction

Cadre le plus général et formel possible $\longrightarrow$ nécessité de vérifier qu'il correspond bien à des cas concrets.

Introduction

Cadre le plus général et formel possible $\longrightarrow$ nécessité de vérifier qu'il correspond bien à des cas concrets.

Systèmes de séquents $\longrightarrow$ obligation de généraliser le cadre

Introduction

Cadre le plus général et formel possible $\longrightarrow$ nécessité de vérifier qu'il correspond bien à des cas concrets.

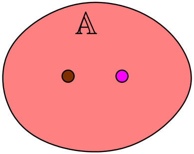
Systèmes de séquents $\longrightarrow$ obligation de généraliser le cadre

Complétion : formalisme autour duquel a été construit le cadre
Preuve non détaillée dans [Bonacina et Dershowitz, 2005] pour la complétion close
Preuve pour la complétion standard $\longrightarrow$ représentation des preuves

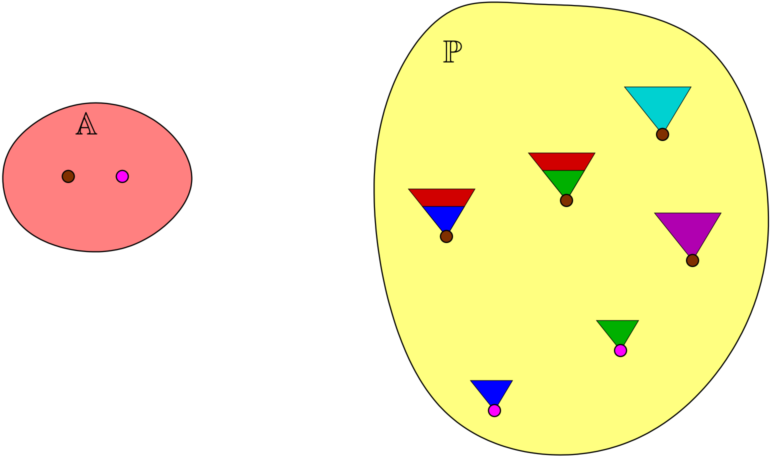
Plan

Plan

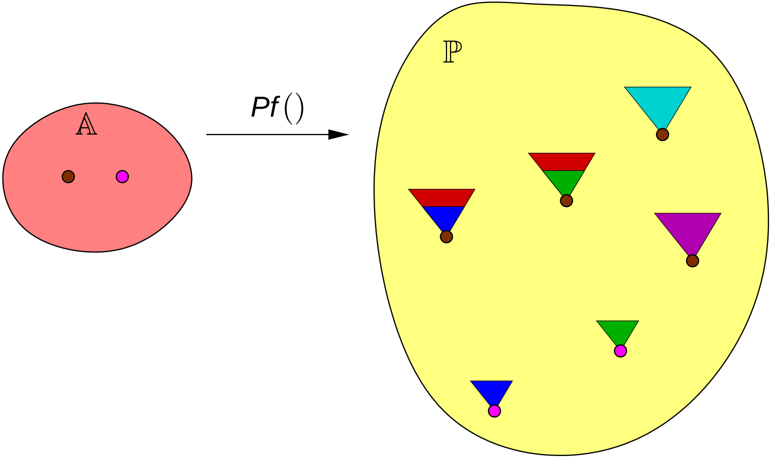
Définitions



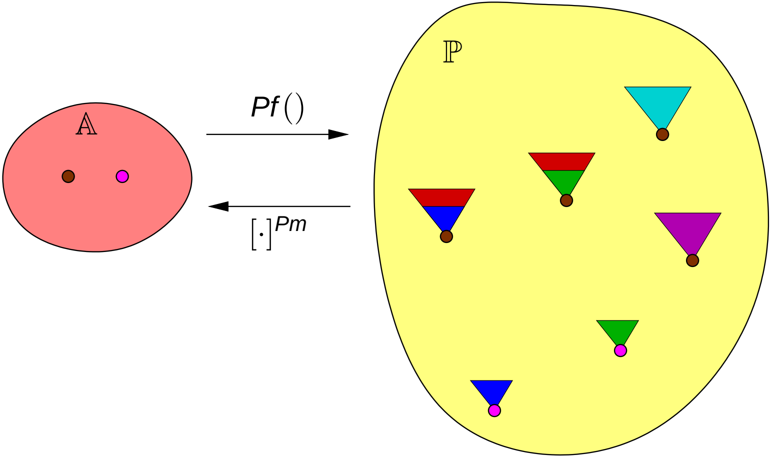
Définitions



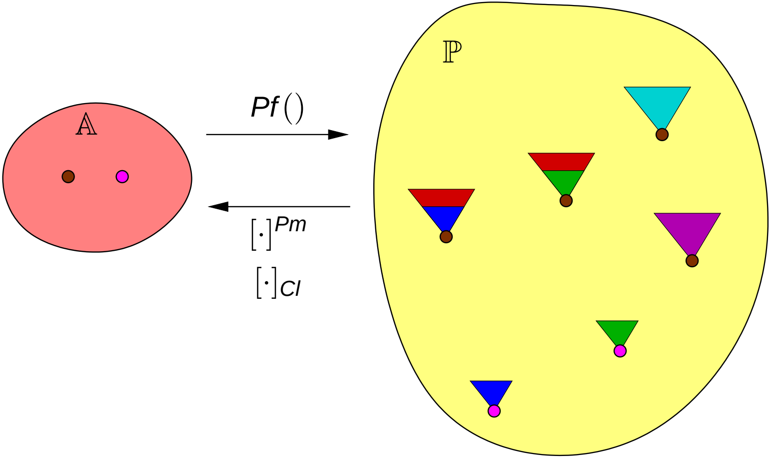
Définitions



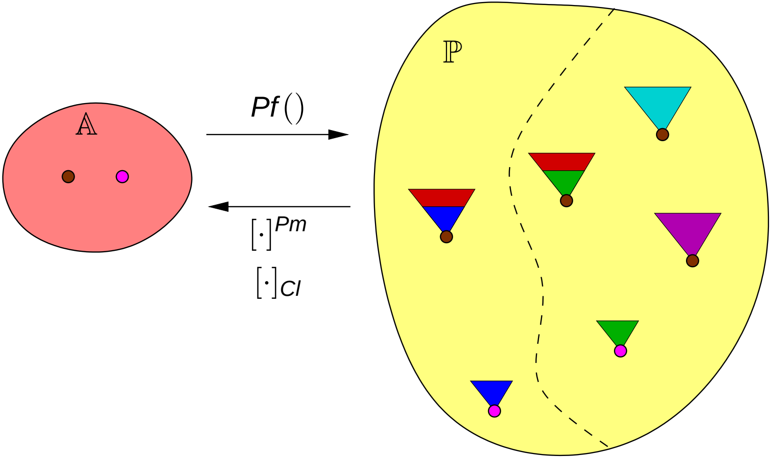
Définitions



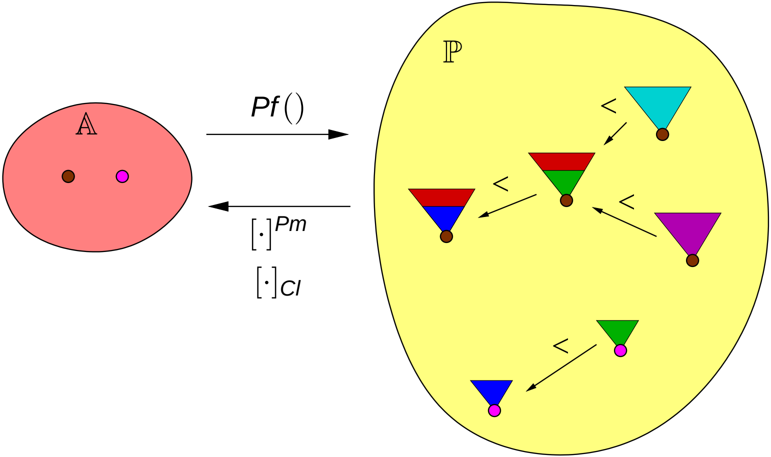
Définitions



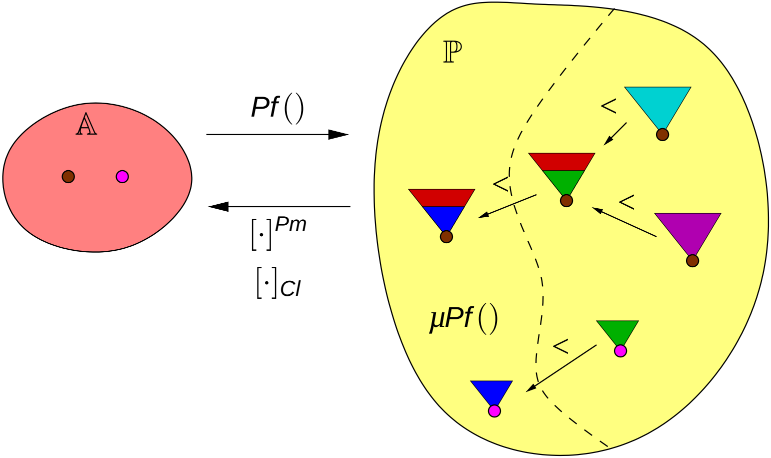
Définitions



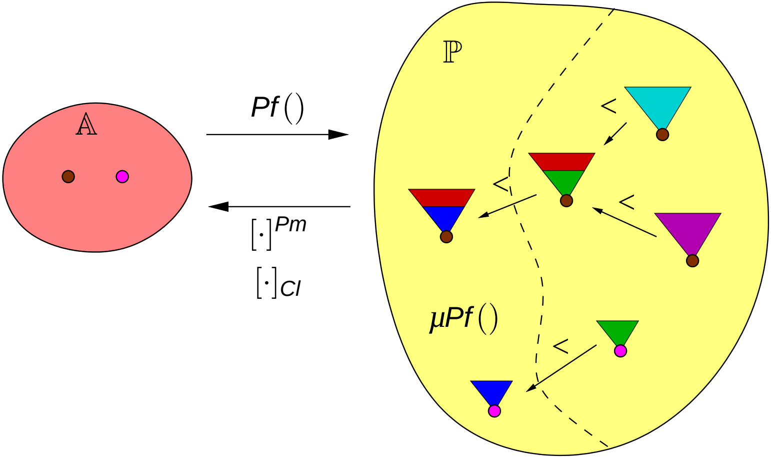
Définitions



Définitions



Définitions



Pour les *justifications* : $\sqsupseteq$

Pour les *présentations* : $\succsim$

Postulats

$$Th\,A \overset{!}{=} [Pf(A)]_{Cl}$$

Postulats

$$Th\,A \stackrel{!}{=} [Pf(A)]_{Cl}$$

POSTULAT A (RÉFLEXIVITÉ).

Pour toute présentation A :

$$A \subseteq Th\,A$$

Postulats

$$Th\,A \overset{!}{=} [Pf(A)]_{Cl}$$

POSTULAT A (RÉFLEXIVITÉ).

Pour toute présentation A :

$$A \subseteq Th\,A$$

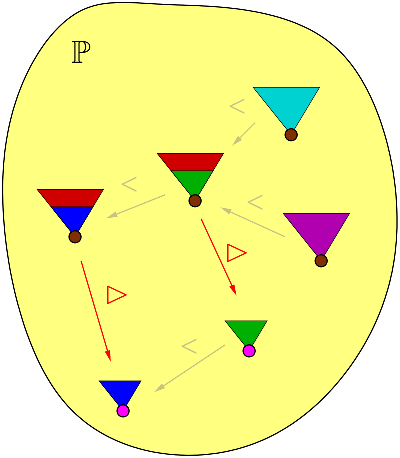
POSTULAT B (FERMETURE).

Pour toute présentation A :

$$Th\,Th\,A \subseteq Th\,A$$

Sous-preuves

On définit aussi une notion de sous-preuve sur $\mathbb{P}$ notée $\rhd$.



Preuve triviale $\widehat{a}$ telle que $[\widehat{a}]^{Pm} = \{[\widehat{a}]_{Cl}\} = \{a\}$ et $\forall q.\ \widehat{a} \not\rhd q$

POSTULAT C (TRIVIA).

Pour toute preuve p et toute formule a :

$$a \in [p]^{Pm} \Rightarrow p \trianglerighteq \widehat{a}$$

Postulats

POSTULAT C (TRIVIA).

Pour toute preuve p et toute formule a :

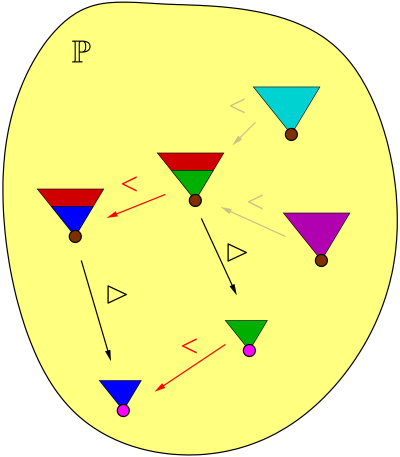
$$a \in [p]^{Pm} \Rightarrow p \trianglerighteq \widehat{a}$$

POSTULAT D (MONOTONIE DES HYPOTHÈSES DES SOUS-PREUVES).

Pour toutes preuves p et q :

$$p \trianglerighteq q \Rightarrow [p]^{Pm} \supseteq [q]^{Pm}$$

Postulat E



Postulats

POSTULAT C (TRIVIA).

Pour toute preuve p et toute formule a :

$$a \in [p]^{Pm} \Rightarrow p \trianglerighteq \widehat{a}$$

POSTULAT D (MONOTONIE DES HYPOTHÈSES DES SOUS-PREUVES).

Pour toutes preuves p et q :

$$p \trianglerighteq q \Rightarrow [p]^{Pm} \supseteq [q]^{Pm}$$

POSTULAT E (REMPLACEMENT).

Pour toutes preuves p, q et r :

$$p \triangleright q > r \Rightarrow \exists v \in Pf\left([p]^{Pm} \cup [r]^{Pm}\right).\ p > v \triangleright r$$

Présentation Canonique

$$A^\sharp \quad \stackrel{!}{=} \quad \left[\mu Pf\left(Th\,A\right)\right]^{Pm}$$

Présentation Canonique

$$A^\sharp \quad \stackrel{!}{=} \quad \left[\mu Pf\left(Th\, A\right)\right]^{Pm}$$

$\mu Pf\left(Th\, A^\sharp\right) \subseteq Pf\left(A^\sharp\right)$

Notion de *saturation*

Présentation Canonique

$$A^\sharp \quad \stackrel{!}{=} \quad [\mu Pf(Th\,A)]^{Pm}$$

$$\mu Pf(Th\,A^\sharp) \subseteq Pf(A^\sharp)$$

Notion de *saturation*

+

$$\forall r \in A^\sharp.\ A^\sharp \not\succsim A^\sharp \setminus \{r\}$$

Notion de *(non)-redondance*

Mécanismes de Déduction

Mécanisme de déduction : $\rightsquigarrow : 2^{\mathbb{A}} \longrightarrow 2^{\mathbb{A}}$

Limite : $A_\infty \stackrel{!}{=} \liminf_{j \to \infty} A_j = \bigcup_{j>0} \bigcap_{i>j} A_i$

Mécanismes de Déduction

Mécanisme de déduction : $\rightsquigarrow : 2^{\mathbb{A}} \longrightarrow 2^{\mathbb{A}}$

Limite : $A_\infty \stackrel{!}{=} \liminf_{j\rightarrow\infty} A_j = \bigcup_{j>0} \bigcap_{i>j} A_i$

Adéquat et sain : $A \rightsquigarrow B$ implique $Th\, A = Th\, B$

Mécanismes de Déduction

Mécanisme de déduction : $\rightsquigarrow: 2^{\mathbb{A}} \longrightarrow 2^{\mathbb{A}}$

Limite : $A_\infty \stackrel{!}{=} \liminf_{j\to\infty} A_j = \bigcup_{j>0} \bigcap_{i>j} A_i$

Adéquat et sain : $A \rightsquigarrow B$ implique $Th\,A = Th\,B$

Bon : $A \rightsquigarrow B$ implique $A \succsim B$

Mécanismes de Déduction

Mécanisme de déduction : $\rightsquigarrow : 2^{\mathbb{A}} \longrightarrow 2^{\mathbb{A}}$

Limite : $A_\infty \stackrel{!}{=} \liminf_{j\to\infty} A_j = \bigcup_{j>0} \bigcap_{i>j} A_i$

Adéquat et sain : $A \rightsquigarrow B$ implique $Th\,A = Th\,B$

Bon : $A \rightsquigarrow B$ implique $A \succsim B$

Canonique : $A_\infty = A_0^\sharp$

Plan

Déduction Naturelle et Postulat D

Déduction Naturelle

Axiom :

$$\frac{}{\Gamma, A \vdash A}\ \text{Ax}$$

Abstraction (→Introduction) :

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}\ \text{Abs}$$

Application (→Elimination) :

$$\frac{\Gamma \vdash A \rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \text{App}$$

Déduction Naturelle et Postulat D

Déduction Naturelle

Axiom :

$$\frac{}{\Gamma, A \vdash A}\ \text{Ax}$$

Abstraction ($\rightarrow$Introduction) :

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}\ \text{Abs}$$

Application ($\rightarrow$Elimination) :

$$\frac{\Gamma \vdash A \rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \text{App}$$

Nouveau Cadre

Plus de postulat D

Nouveau Cadre

Plus de postulat D

Postulat E modifié :

Postulat E_{gen} (Remplacement Généralisé).

Pour toute preuve p, q et r :

$$p \rhd q > r \Rightarrow \exists v \in Pf\left([p]^{Pm} \cup \left([r]^{Pm} \setminus [q]^{Pm}\right)\right).\ p > v \rhd r$$

Exemple

$$\dfrac{\dfrac{\overline{A, B \vdash A}\ \text{Ax}}{A \vdash B \rightarrow A}\ \text{Abs}}{\vdash A \rightarrow B \rightarrow A}\ \text{Abs}$$

Exemple

$$\dfrac{\dfrac{\overline{A, B \vdash A}\ \text{Ax}}{A \vdash B \to A}\ \text{Abs}}{\vdash A \to B \to A}\ \text{Abs}$$

Exemple

$$\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\text{Ax}}{A \vdash B \longrightarrow A}\text{Abs}}{\vdash A \longrightarrow B \longrightarrow A}\text{Abs} \quad \text{donne} \quad \dfrac{\color{red}{\dfrac{}{B \longrightarrow A, A \vdash B \longrightarrow A}\text{Ax}}}{\vdash A \longrightarrow B \longrightarrow A}\text{Abs}$$

Exemple

$$\dfrac{\dfrac{\overline{A, B \vdash A}\ \text{Ax}}{A \vdash B \to A}\ \text{Abs}}{\vdash A \to B \to A}\ \text{Abs} \quad \text{donne} \quad \dfrac{\overline{B \to A, A \vdash B \to A}\ \text{Ax}}{\color{red}{B \to A} \vdash A \to B \to A}\ \text{Abs}$$

Exemple

$$\cfrac{\cfrac{\overline{A, B \vdash A}\ \text{Ax}}{A \vdash B \to A}\ \text{Abs}}{\vdash A \to B \to A}\ \text{Abs} \quad \text{donne} \quad \cfrac{\overline{B \to A, A \vdash B \to A}\ \text{Ax}}{B \to A \vdash A \to B \to A}\ \text{Abs}$$

La preuve résultante est bien dans $Pf([p]^{Pm} \cup ([r]^{Pm} \setminus ([q]^{Pm} \setminus [p]^{Pm})))$.

Exemple

$$\dfrac{\dfrac{\overline{A, B \vdash A}\ \text{Ax}}{A \vdash B \rightarrow A}\ \text{Abs}}{\vdash A \rightarrow B \rightarrow A}\ \text{Abs} \quad \text{donne} \quad \dfrac{\overline{B \rightarrow A, A \vdash B \rightarrow A}\ \text{Ax}}{B \rightarrow A \vdash A \rightarrow B \rightarrow A}\ \text{Abs}$$

La preuve résultante est bien dans $Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}))$.

Exemple

$$\dfrac{\dfrac{\overline{A, B \vdash A}\ \text{Ax}}{A \vdash B \to A}\ \text{Abs}}{\vdash A \to B \to A}\ \text{Abs} \quad \text{donne} \quad \dfrac{\overline{B \to A, A \vdash B \to A}\ \text{Ax}}{B \to A \vdash A \to B \to A}\ \text{Abs}$$

La preuve résultante est bien dans $Pf(\emptyset \cup (\{B \to A, A\} \setminus \{A\}))$.

Exemple

$$\dfrac{\dfrac{\overline{A, B \vdash A}\;\text{Ax}}{A \vdash B \longrightarrow A}\;\text{Abs}}{\vdash A \longrightarrow B \longrightarrow A}\;\text{Abs} \quad \text{donne} \quad \dfrac{\overline{B \longrightarrow A, A \vdash B \longrightarrow A}\;\text{Ax}}{B \longrightarrow A \vdash A \longrightarrow B \longrightarrow A}\;\text{Abs}$$

La preuve résultante est bien dans $Pf(\{B \longrightarrow A\})$.

Plan

Application à la Complétion

Deux procédures de complétions ont été étudiées :

- complétion close ; preuve complète et détaillée, contrairement à celle de [Dershowitz, 2003, Bonacina et Dershowitz, 2005]
- complétion standard ; nécessité de comparer plusieurs représentations de preuves

Complétion Standard

La complétion standard a été introduite par [Knuth et Bendix, 1970]

Transforme un ensemble d'axiomes équationnels en un système de réécriture confluent et terminant

Complétude démontrée pour la première fois par [Huet, 1980]

Peut être représentée par des règles d'inférences, par exemple [Bachmair, 1987] Règles d'inférence

Termes de Preuve

Règles de Formation des Termes de Preuve [Meseguer, 1992]

Congruence :

$$\frac{\pi_1 : t_1 \longrightarrow t'_1 \quad \dots \quad \pi_n : t_n \longrightarrow t'_n}{f(\pi_1,\dots,\pi_n) : f(t_1,\dots,t_n) \longrightarrow f(t'_1,\dots,t'_n)}$$

Transitivité :

$$\frac{\pi_1 : t_1 \longrightarrow t_2 \quad \pi_2 : t_2 \longrightarrow t_3}{\pi_1;\pi_2 : t_1 \longrightarrow t_3}$$

Remplacement :

$\ell : (g(x_1,\dots,x_n), d(x_1,\dots,x_n)) \in E \cup R$

$$\frac{\pi_1 : t_1 \longrightarrow t'_1 \quad \dots \quad \pi_n : t_n \longrightarrow t'_n}{\ell(\pi_1,\dots,\pi_n) : g(t_1,\dots,t_n) \longrightarrow d(t'_1,\dots,t'_n)}$$

Symétrie :

$$\frac{\pi : t_1 \longrightarrow t_2}{\pi^{-1} : t_2 \longrightarrow t_1}$$

Preuves par Remplacement

Introduites par [Bachmair, 1987] pour montrer la complétude la complétion standard

Étape de preuve équationnelle : $s \xleftrightarrow[u=v]{p} t$

avec $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$

Preuves par Remplacement

Introduites par [Bachmair, 1987] pour montrer la complétude la complétion standard

Étape de preuve équationnelle : $s \underset{u=v}{\overset{p}{\longleftrightarrow}} t$

avec $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$

Étape de preuve par réécriture : $s \underset{u\to v}{\overset{p}{\longrightarrow}} t$ ou $t \underset{u\to v}{\overset{p}{\longleftarrow}} s$

avec $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$

Preuves par Remplacement

Introduites par [Bachmair, 1987] pour montrer la complétude la complétion standard

Étape de preuve équationnelle : $s \overset{p}{\underset{u=v}{\longleftrightarrow}} t$

avec $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$

Étape de preuve par réécriture : $s \overset{p}{\underset{u \to v}{\longrightarrow}} t$ ou $t \overset{p}{\underset{u \to v}{\longleftarrow}} s$

avec $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$

Preuve par remplacement :

$$s_0 \overset{p_0}{\underset{\ell_0}{\leftrightarrows_0}} s_1 \overset{p_1}{\underset{\ell_1}{\leftrightarrows_1}} s_2 \cdots s_n \overset{p_n}{\underset{\ell_n}{\leftrightarrows_n}} t_n$$

avec $\leftrightarrows_i \in \{\longleftrightarrow, \longrightarrow, \longleftarrow\}$

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2), (\ell_3; r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1}) \qquad \textbf{(Mouvements Parallèles)}$$

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1}) \qquad \textbf{(Mouvements Parallèles)}$$

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1}) \qquad \textbf{(Séquençage)}$$

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$
\begin{array}{lll}
\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1}) & & \textbf{(Mouvements Parallèles)} \\
\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1}) & & \textbf{(Séquençage)} \\
\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1}) & & \textbf{(Inversion de la Composition)}
\end{array}
$$

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$\pi \underset{\leadsto/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1})$$ **(Mouvements Parallèles)**

$$\underset{\leadsto/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1})$$ **(Séquençage)**

$$\underset{\leadsto/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1})$$ **(Inversion de la Composition)**

$$\underset{\leadsto/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1})$$

(Suppression des Inverses Inutiles)

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1})$$ **(Mouvements Parallèles)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1})$$ **(Séquençage)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1})$$ **(Inversion de la Composition)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1})$$

(Suppression des Inverses Inutiles)

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),\ell_3^{-1})$$

(Suppression des Identités Inutiles)

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1})$ **(Mouvements Parallèles)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1})$ **(Séquençage)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1})$ **(Inversion de la Composition)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1})$

(Suppression des Inverses Inutiles)

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),\ell_3^{-1})$

(Suppression des Identités Inutiles)

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3^{-1})$ **(Remontée de la Composition)**

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x)\longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l\longrightarrow r$, on a :

$\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1})$ **(Mouvements Parallèles)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1})$ **(Séquençage)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1})$ **(Inversion de la Composition)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1})$

(Suppression des Inverses Inutiles)

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),\ell_3^{-1})$

(Suppression des Identités Inutiles)

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3^{-1})$ **(Remontée de la Composition)**

$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3)^{-1}$ **(Inversion de la Congruence)**

Des Termes de Preuve aux Preuves par Remplacement

Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$\pi \underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1})$$ **(Mouvements Parallèles)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1})$$ **(Séquençage)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1})$$ **(Inversion de la Composition)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1})$$

(Suppression des Inverses Inutiles)

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),\ell_3^{-1})$$

(Suppression des Identités Inutiles)

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3^{-1})$$ **(Remontée de la Composition)**

$$\underset{\rightsquigarrow/\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3)^{-1}$$ **(Inversion de la Congruence)**

$$f(g(s),r) \xrightarrow[\ell_1]{1} f(d(s),r) \xleftrightarrow[\ell_2]{11} f(d(t),r) \xleftarrow[\ell_3]{2} f(d(t),l)$$

Ordre sur les preuves

Ordre sur les preuves par remplacement [Bachmair, 1987] :

Coût de $s \xleftrightarrow[u=v]{p} t$: $(\{\!\{s,t\}\!\},u,t)$

Coût de $s \xrightarrow[u\rightarrow v]{p} t$: $(\{\!\{s\}\!\},u,t)$

Coût d'une preuve par remplacement : multiensemble des coûts de ses étapes.

Ordre sur les preuves

Ordre sur les preuves par remplacement [Bachmair, 1987] :

Coût de $s \underset{u=v}{\overset{p}{\longleftrightarrow}} t$: $(\{\!\{s,t\}\!\},u,t)$

Coût de $s \underset{u\to v}{\overset{p}{\longrightarrow}} t$: $(\{\!\{s\}\!\},u,t)$

Coût d'une preuve par remplacement : multiensemble des coûts de ses étapes.

Ordre sur les termes de preuves :

Un terme de preuve p est supérieur à un autre q si le coût de la forme normale de p pour $\rightsquigarrow / \sim$ est supérieur à celui de la forme normale de q.

Vérification des Postulats

Postulats A B C D : pas de problèmes.

Postulat E :

Théorème 1 (Postulat E pour les Preuves Équationnelles).

Pour tous termes de preuves p, r, pour toute position $i \in \mathfrak{p}(p)$,

$$p_{|i} > r \text{ implique } p > p[r]_i$$

La Complétion Standard est Canonique

La complétion standard est saine et adéquate : [Bachmair, 1987, lemme 2.1]

La Complétion Standard est Canonique

La complétion standard est saine et adéquate : [Bachmair, 1987, lemme 2.1]

La complétion standard est bonne : [Bachmair, 1987, lemmes 2.5, 2.6]

La Complétion Standard est Canonique

La complétion standard est saine et adéquate : [Bachmair, 1987, lemme 2.1]

La complétion standard est bonne : [Bachmair, 1987, lemmes 2.5, 2.6]

La complétion standard est canonique :

THÉORÈME 2.

Pour toute dérivation $(E_i, R_i)_i$ de la complétion standard qui termine sans échec,

$$R_\infty = E_0^\sharp$$

Plan

Conclusion

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures
- aux complétions close et standard, pour lesquelles une preuve complète et détaillée est donnée.

Conclusion

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures
- aux complétions close et standard, pour lesquelles une preuve complète et détaillée est donnée.

Ces résultats sont probablement extensibles au calcul des séquents, à la logique linéaire

Conclusion

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures
- aux complétions close et standard, pour lesquelles une preuve complète et détaillée est donnée.

Ces résultats sont probablement extensibles au calcul des séquents, à la logique linéaire, à la complétion modulo, à l'algorithme de Buchberger.

Conclusion

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures
- aux complétions close et standard, pour lesquelles une preuve complète et détaillée est donnée.

Ces résultats sont probablement extensibles au calcul des séquents, à la logique linéaire, à la complétion modulo, à l'algorithme de Buchberger.

Calcul des constructions, calcul des séquents modulo, procédure de résolution ?

Conclusion

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures
- aux complétions close et standard, pour lesquelles une preuve complète et détaillée est donnée.

Ces résultats sont probablement extensibles au calcul des séquents, à la logique linéaire, à la complétion modulo, à l'algorithme de Buchberger.

Calcul des constructions, calcul des séquents modulo, procédure de résolution ?

Ordres différents sur les systèmes de séquent

Conclusion

On a pu appliquer les systèmes canoniques abstraits :

- à la déduction naturelle, grâce à une généralisation du cadre pour les systèmes de preuve ne préservant pas les hypothèses dans les sous-preuves ;
  preuves minimales = preuves sans coupures
- aux complétions close et standard, pour lesquelles une preuve complète et détaillée est donnée.

Ces résultats sont probablement extensibles au calcul des séquents, à la logique linéaire, à la complétion modulo, à l'algorithme de Buchberger.

Calcul des constructions, calcul des séquents modulo, procédure de résolution ?

Ordres différents sur les systèmes de séquent

Formalisation en Coq

Deuxième partie II

Déduction Modulo Asymétrique

Plan

6. Déduction Modulo et Réécriture
   - Introduction à la Déduction Modulo
   - Rappels de Réécriture
   - Confluence et Élimination des Coupures

7. Complétion Généralisée
   - Approche de G. Dowek
   - Notre Approche
   - Perspectives

Plan

6 Déduction Modulo et Réécriture
- Introduction à la Déduction Modulo
- Rappels de Réécriture
- Confluence et Élimination des Coupures

7 Complétion Généralisée
- Approche de G. Dowek
- Notre Approche
- Perspectives

La Déduction Modulo

Principe de Poincaré : différence entre démonstrations de

$2+2=4$	et	Axiome du choix $\Leftrightarrow$ Lemme de Zorn
calcul	$\neq$	raisonnement

En déduction modulo [Dowek et al., 2003], les étapes de calcul sont masquées pour faire apparaître le raisonnement.

Règles de conversion :

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{Conv-g} \qquad \text{si } A \equiv B \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A, \Delta}\ \text{Conv-d}$$

Calcul des Séquents Modulo

Règles de conversion :

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{Conv-g} \qquad \text{si } A \equiv B \quad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A, \Delta}\ \text{Conv-d}$$

Calcul des Séquents Modulo

$$\frac{}{\Gamma, A \vdash B, \Delta}\ \text{Axiom}\ \text{si } A \equiv B \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash \Delta}\ \text{Coup}\ \text{si } A \equiv B$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma \vdash A, \Delta}\ \neg\text{-d}\ \text{si } A \equiv \neg B \qquad \frac{\Gamma, B \vdash C, \Delta}{\Gamma \vdash A, \Delta}\ \Rightarrow\text{-d}\ \text{si } A \equiv B \Rightarrow C$$

$$\frac{\Gamma \vdash B, \Delta \quad \Gamma \vdash C, \Delta}{\Gamma \vdash A, \Delta}\ \wedge\text{-d}\ \text{si } A \equiv B \wedge C \qquad \frac{\Gamma \vdash B, C, \Delta}{\Gamma \vdash A, \Delta}\ \vee\text{-d}\ \text{si } A \equiv B \vee C$$

$$\frac{\Gamma \vdash \{t/x\}B, \Delta}{\Gamma \vdash A, \Delta}\ \exists\text{-d}\ \text{si } A \equiv \exists x.\ B \qquad \frac{\Gamma \vdash \{c/x\}B, \Delta}{\Gamma \vdash A, \Delta}\ \forall\text{-d}\ \text{si } A \equiv \forall x.\ B$$

et c constante fraîche

Déduction Modulo Asymétrique [Dowek, 2003]

Congruence $\equiv$ simulée par un système de réécriture $\longrightarrow$

Déduction Modulo Asymétrique [Dowek, 2003]

Congruence $\equiv$ simulée par un système de réécriture $\longrightarrow$

Analycité $\Rightarrow$ on ne réécrit que vers le haut

Règles de conversion :

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \vdash \Delta}\ \uparrow\text{-g} \quad \text{si } A \longrightarrow B \quad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A, \Delta}\ \uparrow\text{-d}$$

Calcul des Séquents Modulo Asymétrique

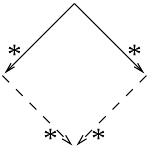
$$\frac{}{\Gamma, A \vdash B, \Delta}\ \text{Axiom} \quad \text{si } A \stackrel{*}{\longrightarrow} \stackrel{*}{\longleftarrow} B \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash \Delta}\ \text{Coup} \quad \text{si } A \stackrel{*}{\longleftarrow} \stackrel{*}{\longrightarrow} B$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma \vdash A, \Delta}\ \neg\text{-d} \quad \text{si } A \stackrel{*}{\longrightarrow} \neg B \qquad \frac{\Gamma \vdash B, C, \Delta}{\Gamma \vdash A, \Delta}\ \vee\text{-d} \quad \text{si } A \stackrel{*}{\longrightarrow} B \vee C$$

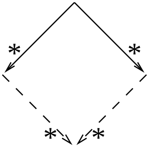
$$\frac{\Gamma \vdash B, \Delta \quad \Gamma \vdash C, \Delta}{\Gamma \vdash A, \Delta}\ \wedge\text{-d} \quad \text{si } A \stackrel{*}{\longrightarrow} B \wedge C \qquad \frac{\Gamma \vdash \{c/x\}B, \Delta}{\Gamma \vdash A, \Delta}\ \forall\text{-d} \quad \text{si } A \stackrel{*}{\longrightarrow} \forall x.\, B$$

et c constante fraîche

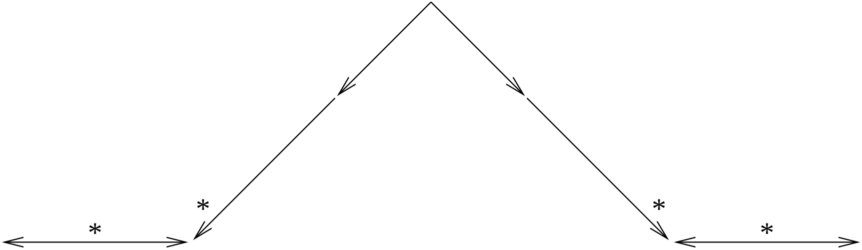
Réduction de Pics et Confluence

Confluence : 

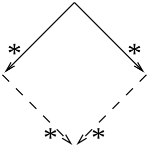
Réduction de Pics et Confluence

Confluence : 

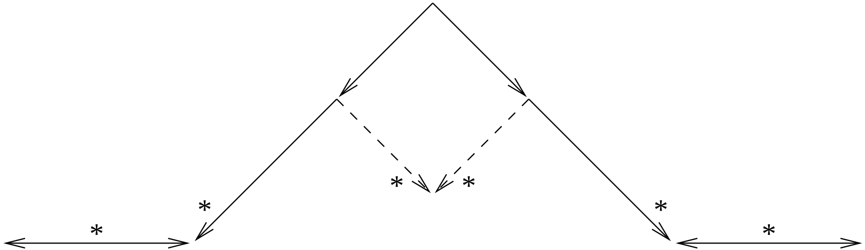
Algorithme de Newman de réduction de pics [Newman, 1942] :

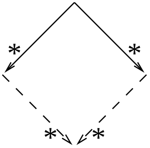


Réduction de Pics et Confluence

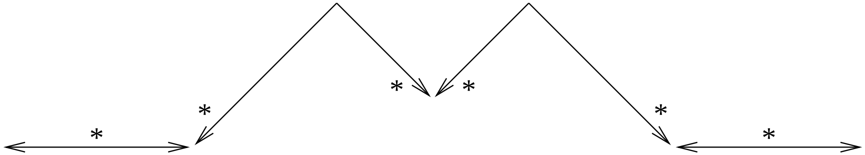
Confluence : 

Algorithme de Newman de réduction de pics [Newman, 1942] :



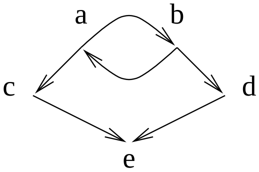
Confluence : 

Algorithme de Newman de réduction de pics [Newman, 1942] :



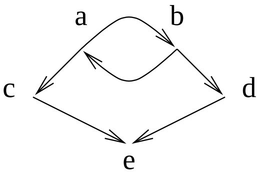
Confluence $\not\Rightarrow$ Réduction de Pics

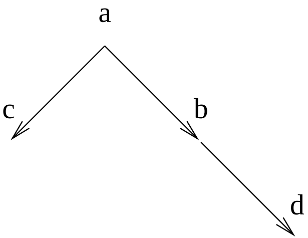
Contre-exemple :



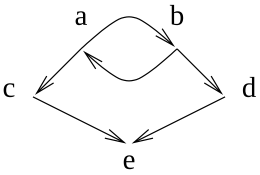
Confluence $\not\Rightarrow$ Réduction de Pics

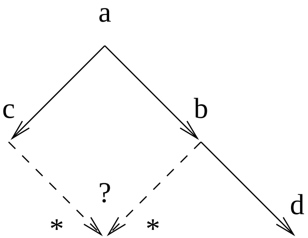
Contre-exemple :





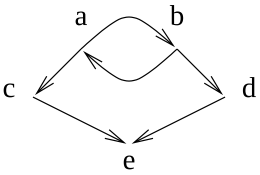
Contre-exemple :

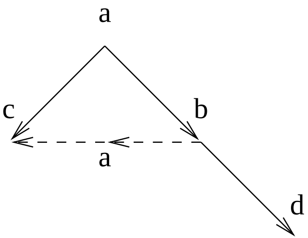




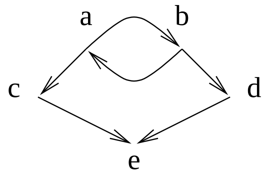
Confluence $\not\Rightarrow$ Réduction de Pics

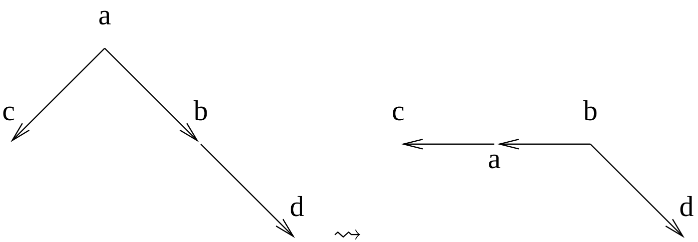
Contre-exemple :





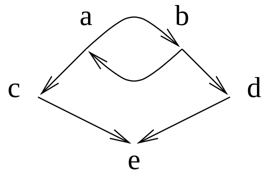
Contre-exemple :

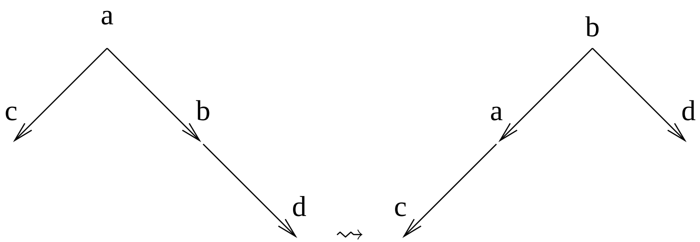




Confluence $\not\Rightarrow$ Réduction de Pics

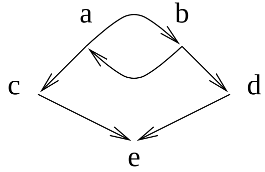
Contre-exemple :

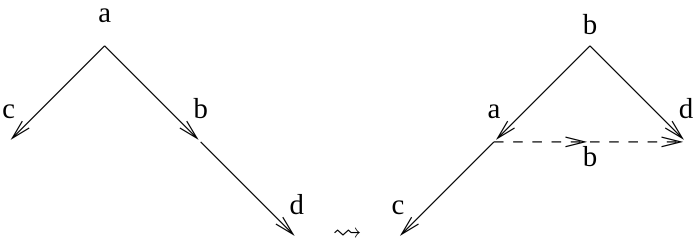




Confluence $\nRightarrow$ Réduction de Pics

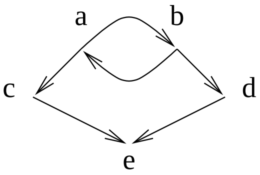
Contre-exemple :

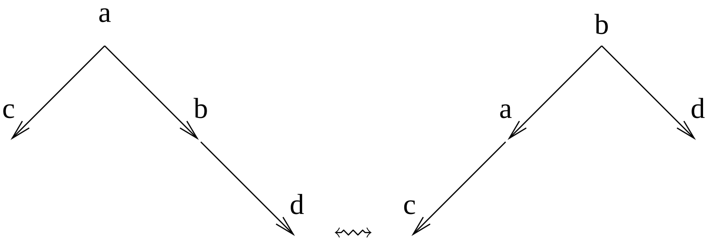




Confluence $\not\Rightarrow$ Réduction de Pics

Contre-exemple :





Réécriture sur les Termes Uniquement

THÉORÈME 3.

$\Gamma \vdash \Delta$ *ssi* $\exists A \in \Gamma, B \in \Delta$ *t.q.* $A \overset{*}{\leftrightarrow} B$

Démonstration.

$\Rightarrow$ par induction sur la preuve de $\Gamma \vdash \Delta$
$\Leftarrow$ par induction sur le nombre de pics sur la preuve par remplacement de $A \overset{*}{\leftrightarrow} B$, chaque pic est simulé par une règle de coupure

$\square$

Réécriture sur les Termes Uniquement

THÉORÈME 3.

$\Gamma \vdash \Delta$ *ssi* $\exists A \in \Gamma, B \in \Delta$ *t.q.* $A \overset{*}{\leftrightarrow} B$

THÉORÈME 4.

$\Gamma \vdash^{cf} \Delta$ *ssi* $\exists A \in \Gamma, B \in \Delta$ *t.q.* $A \overset{*}{\longrightarrow} \overset{*}{\longleftarrow} B$

Démonstration.

$\Rightarrow$ par induction sur la preuve de $\Gamma \vdash^{cf} \Delta$

$\Leftarrow$ on a $\dfrac{}{\Gamma, A \vdash B, \Delta}$ Axiom

$\square$

Réécriture sur les Termes Uniquement

Théorème 3.

$\Gamma \vdash \Delta$ *ssi* $\exists A \in \Gamma, B \in \Delta$ *t.q.* $A \overset{*}{\leftrightarrow} B$

Théorème 4.

$\Gamma \vdash^{cf} \Delta$ *ssi* $\exists A \in \Gamma, B \in \Delta$ *t.q.* $A \overset{*}{\rightarrow} \overset{*}{\leftarrow} B$

Corollaire 5.

confluence $\Leftrightarrow$ *élimination des coupures*

Réécriture sur les Propositions

Il est possible de réécrire des propositions atomiques :

$$x * y = 0 \longrightarrow x = 0 \vee y = 0$$

Réécriture sur les Propositions

Il est possible de réécrire des propositions atomiques :

$$x * y = 0 \longrightarrow x = 0 \vee y = 0$$

On a plus confluence $\Rightarrow$ élimination des coupures : contre-exemple de Crabbé

$$A \longrightarrow B \wedge \neg A$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{B,A\vdash A}\,\text{Axiome}}{B,A,\neg A\vdash}\,\neg\text{-g}}{B,A\vdash}\,\wedge\text{-g} \qquad \dfrac{\dfrac{}{B\vdash B}\,\text{Axiome} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{B,A\vdash A}\,\text{Axiome}}{B,A,\neg A\vdash}\,\neg\text{-g}}{B,A\vdash}\,\wedge\text{-g}}{B\vdash \neg A}\,\neg\text{-d}}{B\vdash A}\,\wedge\text{-d}}{B\vdash}\,\text{Coup}}{\vdash \neg B}\,\neg\text{-d}$$

(terme de preuve $\lambda y.(\lambda x.(\text{snd } x)x) < y, \lambda x.(\text{snd } x)x >$)

Résumé

Réécriture **Déduction Modulo**

Résumé

Réécriture | **Déduction Modulo**

Réduction de pics

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow$	Normalisation

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow$	Normalisation
$\Downarrow$		
Confluence		

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow$	Normalisation
$\Downarrow$		$\Downarrow$
Confluence	$\Leftarrow$	Propriété d'élimination des coupures

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow$	Normalisation
$\Downarrow$	$\cancel{\Nwarrow}$	$\Downarrow$
Confluence	$\Leftarrow$	Propriété d'élimination des coupures

Contre-exemple de Newman

Résumé

Réécriture		Déduction Modulo
Réduction de pics	$\Leftarrow$	Normalisation
$\Downarrow$	$\not\Nwarrow \; \not\Searrow$	$\Downarrow$
Confluence	$\Leftarrow$	Propriété d'élimination des coupures

Contre-exemple de Crabbé

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow\!\not\Rightarrow$	Normalisation
$\Downarrow\not\Uparrow$	$\not\nwarrow \; \not\searrow$	$\Downarrow\not\Uparrow$
Confluence	$\Leftarrow\!\not\Rightarrow$	Propriété d'élimination des coupures

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow\not\Rightarrow$	Normalisation
$\Downarrow\not\Uparrow$	$\not\nwarrow\ \not\searrow$	$\Downarrow\not\Uparrow$
Confluence	$\Leftarrow\not\Rightarrow$	Propriété d'élimination des coupures
$\Uparrow$		
Procédure de complétion		

Résumé

Réécriture		**Déduction Modulo**
Réduction de pics	$\Leftarrow\not\Rightarrow$	Normalisation
$\Downarrow\not\Uparrow$	$\not\Nwarrow\ \not\Searrow$	$\Downarrow\not\Uparrow$
Confluence	$\Leftarrow\not\Rightarrow$	Propriété d'élimination des coupures
$\Uparrow$		$\Uparrow$
Procédure de complétion		Complétion généralisée ?

Plan

6 Déduction Modulo et Réécriture
- Introduction à la Déduction Modulo
- Rappels de Réécriture
- Confluence et Élimination des Coupures

7 Complétion Généralisée
- Approche de G. Dowek
- Notre Approche
- Perspectives

Méthode de G. Dowek [Dowek, 2002]

Soit $\mathcal{T}$ une théorie sans quantificateur

Méthode de G. Dowek [Dowek, 2002]

Soit $\mathcal{T}$ une théorie sans quantificateur

On la met sous forme clausale $\rightsquigarrow \Gamma = \psi_1, \ldots, \psi_n$

Méthode de G. Dowek [Dowek, 2002]

Soit $\mathcal{T}$ une théorie sans quantificateur

On la met sous forme clausale $\rightsquigarrow \Gamma = \psi_1, \ldots, \psi_n$

Soit $\mathcal{M}$ un modèle de Γ

Il existe un litéral $\pm P \in \psi_1$ tel que $\mathcal{M} \models \pm P$

Méthode de G. Dowek [Dowek, 2002]

Soit $\mathcal{T}$ une théorie sans quantificateur

On la met sous forme clausale $\rightsquigarrow \Gamma = \psi_1, \ldots, \psi_n$

Soit $\mathcal{M}$ un modèle de Γ

Il existe un litéral $\pm P \in \psi_1$ tel que $\mathcal{M} \models \pm P$

- $\mathcal{M} \models P$: on considère les ψ_i tels que $\psi_i = P \vee A_i$

$$P \longrightarrow P \vee \neg A_1 \vee \cdots \vee \neg A_n$$

Méthode de G. Dowek [Dowek, 2002]

Soit $\mathcal{T}$ une théorie sans quantificateur

On la met sous forme clausale $\rightsquigarrow \Gamma = \psi_1, \ldots, \psi_n$

Soit $\mathcal{M}$ un modèle de Γ

Il existe un litéral $\pm P \in \psi_1$ tel que $\mathcal{M} \models \pm P$

- $\mathcal{M} \models P$: on considère les ψ_i tels que $\psi_i = P \vee A_i$

$$P \longrightarrow P \vee \neg A_1 \vee \cdots \vee \neg A_n$$

- $\mathcal{M} \not\models P$: on considère les ψ_i tels que $\psi_i = \neg P \vee A_i$

$$P \longrightarrow P \wedge A_1 \wedge \cdots \wedge A_n$$

Méthode de G. Dowek [Dowek, 2002]

Soit $\mathcal{T}$ une théorie sans quantificateur

On la met sous forme clausale $\rightsquigarrow \Gamma = \psi_1, \ldots, \psi_n$

Soit $\mathcal{M}$ un modèle de Γ

Il existe un litéral $\pm P \in \psi_1$ tel que $\mathcal{M} \models \pm P$

- $\mathcal{M} \models P$: on considère les ψ_i tels que $\psi_i = P \vee A_i$

$$P \longrightarrow P \vee \neg A_1 \vee \cdots \vee \neg A_n$$

- $\mathcal{M} \not\models P$: on considère les ψ_i tels que $\psi_i = \neg P \vee A_i$

$$P \longrightarrow P \wedge A_1 \wedge \cdots \wedge A_n$$

On supprime toutes les clauses utilisées, et on recommence jusqu'à ce qu'il n'y en ait plus

Exemple

Crabbé :

$$A \Leftrightarrow (B \wedge \neg A)$$

Exemple

Crabbé :

$$(A \Rightarrow (B \land \neg A)) \land ((B \land \neg A) \Rightarrow A)$$

Exemple

Crabbé :

$$(\neg A \vee (B \wedge \neg A)) \wedge (\neg(B \wedge \neg A) \vee A)$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M}$: $|A| \mapsto 0$, $|B| \mapsto 0$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M}$: $|A| \mapsto 0$, $|B| \mapsto 0$

- $P = A$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M}$: $|A| \mapsto 0$, $|B| \mapsto 0$

- $P = A$

$$A \longrightarrow A \wedge$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M}$: $|A| \mapsto 0$, $|B| \mapsto 0$

- $P = A$

$$A \longrightarrow A \wedge B \wedge$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A \vee \perp) \wedge (\neg B \vee A)$$

$\mathcal{M} : |A| \mapsto 0, |B| \mapsto 0$

- $P = A$

$$A \longrightarrow A \wedge B \wedge \perp$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M} : |A| \mapsto 0, |B| \mapsto 0$

- $P = A$

$$A \longrightarrow \perp$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M} : |A| \mapsto 0, |B| \mapsto 0$

- $P = A$

$$A \longrightarrow \perp$$

- $P = B$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M} : |A| \mapsto 0, |B| \mapsto 0$

- $P = A$

$$A \longrightarrow \bot$$

- $P = B$

$$B \longrightarrow B \wedge$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M} : |A| \mapsto 0, |B| \mapsto 0$

- $P = A$

$$A \longrightarrow \bot$$

- $P = B$

$$B \longrightarrow B \wedge A$$

Exemple

Crabbé :

$$(\neg A \vee B) \wedge (\neg A) \wedge (\neg B \vee A)$$

$\mathcal{M} : |A| \mapsto 0, |B| \mapsto 0$

- $P = A$

$$A \longrightarrow \perp$$

- $P = B$

$$B \longrightarrow B \wedge A$$

Possède la propriété d'élimination des coupures

Preuves Critiques

Définition 1 (Preuves Critiques).

$p \in \mu Pf(A)$ est dite critique si :

- $p \notin \mu Pf(ThA)$

Preuves Critiques

Définition 1 (Preuves Critiques).

$p \in \mu Pf(A)$ *est dite critique si :*

- $p \notin \mu Pf(ThA)$
- $\forall q \lhd p.\ q \in \mu Pf(Th\,A)$

Preuves Critiques

Définition 1 (Preuves Critiques).

$p \in \mu Pf(A)$ est dite critique si :

- $p \notin \mu Pf(ThA)$
- $\forall q \lhd p.\ q \in \mu Pf(Th\,A)$

THÉORÈME 6 (ÉQUITÉ DE LA COMPLÉTION).

Si une bonne dérivation $\{A_i\}_i$ est telle que

$$Crit(A_\infty) \sqsupset Pf(A_*)$$

alors elle est saturante

Idée : rajouter toutes les conclusions des preuves critiques

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$\dfrac{\dfrac{}{\vdash A}\uparrow\text{-d} \qquad \dfrac{}{A \vdash}\uparrow\text{-g}}{\vdash}\text{Coup}$$

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$\dfrac{\dfrac{\dfrac{\vdash B,A \qquad \dfrac{\dfrac{}{A\vdash A}\ \text{Axiome}}{\vdash \neg A, A}\ \neg\text{-d}}{\vdash B\wedge\neg A, A}\ \wedge\text{-d}}{\vdash A}\ \uparrow\text{-d} \qquad \dfrac{}{A\vdash}\ \uparrow\text{-g}}{\vdash}\ \text{Coup}$$

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$\dfrac{\dfrac{\dfrac{\vdash B, A \qquad \dfrac{\dfrac{}{A \vdash A}\,\text{Axiome}}{\vdash \neg A, A}\,\neg\text{-d}}{\vdash B \wedge \neg A, A}\,\wedge\text{-d}}{\vdash A}\,\uparrow\text{-d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\,\text{Axiome}}{A, B, \neg A \vdash}\,\neg\text{-g}}{A, B \wedge \neg A \vdash}\,\wedge\text{-g}}{A \vdash}\,\uparrow\text{-g}}{\vdash}\,\text{Coup}$$

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$\dfrac{\dfrac{\dfrac{{\color{red}B} \vdash B, A \qquad \dfrac{\dfrac{}{A \vdash A}\,\text{Axiome}}{\vdash \neg A, A}\,\neg\text{-d}}{\vdash B \wedge \neg A, A}\,\wedge\text{-d}}{\vdash A}\,\uparrow\text{-d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\,\text{Axiome}}{A, B, \neg A \vdash}\,\neg\text{-g}}{A, B \wedge \neg A \vdash}\,\wedge\text{-g}}{A \vdash}\,\uparrow\text{-g}}{\vdash}\,\text{Coup}$$

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$\dfrac{\dfrac{\dfrac{B \vdash B, A \qquad \dfrac{\dfrac{}{B, A \vdash A}\,\text{Axiome}}{B \vdash \neg A, A}\,\neg\text{-d}}{B \vdash B \wedge \neg A, A}\,\wedge\text{-d}}{B \vdash A}\,\uparrow\text{-d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{B, A, B \vdash A}\,\text{Axiome}}{B, A, B, \neg A \vdash}\,\neg\text{-g}}{B, A, B \wedge \neg A \vdash}\,\wedge\text{-g}}{B, A \vdash}\,\uparrow\text{-g}}{B \vdash}\,\text{Coup}$$

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$\dfrac{\dfrac{\dfrac{B \vdash B, A \qquad \dfrac{\dfrac{}{B, A \vdash A}\text{Axiome}}{B \vdash \neg A, A}\neg\text{-d}}{B \vdash B \wedge \neg A, A}\wedge\text{-d}}{B \vdash A}\uparrow\text{-d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{B, A, B \vdash A}\text{Axiome}}{B, A, B, \neg A \vdash}\neg\text{-g}}{B, A, B \wedge \neg A \vdash}\wedge\text{-g}}{B, A \vdash}\uparrow\text{-g}}{\color{red}{B \vdash}}\text{Coup}$$

On a prouvé $B \Rightarrow \perp$, on ajoute la règle

$$B \longrightarrow B \wedge \perp$$

Notre Approche par l'Exemple

Crabbé : $A \longrightarrow B \wedge \neg A$

$$
\dfrac{
\dfrac{
\dfrac{
B \vdash B, A \qquad
\dfrac{\dfrac{}{B, A \vdash A}\ \text{Axiome}}{B \vdash \neg A, A}\ \neg\text{-d}
}{B \vdash B \wedge \neg A, A}\ \wedge\text{-d}
}{B \vdash A}\ \uparrow\text{-d}
\qquad
\dfrac{
\dfrac{
\dfrac{\dfrac{}{B, A, B \vdash A}\ \text{Axiome}}{B, A, B, \neg A \vdash}\ \neg\text{-g}
}{B, A, B \wedge \neg A \vdash}\ \wedge\text{-g}
}{B, A \vdash}\ \uparrow\text{-g}
}{B \vdash}\ \text{Coup}
$$

On a prouvé $B \Rightarrow \perp$, on ajoute la règle

$$B \longrightarrow \perp$$

Notre Approche par l'Exemple (suite)

Paradoxe de Russell : $R \in R \longrightarrow \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C$ où

$$y \sim z \quad \stackrel{!}{=} \quad \forall x.\, (y \in x \Rightarrow z \in x)$$

Notre Approche par l'Exemple (suite)

Paradoxe de Russell : $R \in R \ \longrightarrow \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C$ où

$$y \sim z \quad \overset{!}{=} \quad \forall x.\, (y \in x \Rightarrow z \in x)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{R \in t_0, c_0 \in R \vdash R \in R, C \qquad c_0 \in R \vdash c_0 \in t_0, R \in R, C}{c_0 \in t_0 \Rightarrow R \in t_0, c_0 \in R \vdash R \in R, C}\ \Rightarrow\text{-g}}{c_0 \sim R, c_0 \in R \vdash R \in R, C}\ \forall\text{-g}}{c_0 \sim R \vdash R \in R, c_0 \in R \Rightarrow C}\ \Rightarrow\text{-d}}{\vdash R \in R, c_0 \sim R \Rightarrow c_0 \in R \Rightarrow C}\ \Rightarrow\text{-d}}{\vdash R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C}\ \forall\text{-d}}{\vdash R \in R}\ \uparrow\text{-d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{R \in R, C \vdash \qquad R \in R \vdash t_1 \in R}{R \in R, t_1 \in R \Rightarrow C \vdash}\ \Rightarrow\text{-g} \qquad \dfrac{\dfrac{R \in R, t_1 \in c_1 \vdash R \in c_1}{R \in R \vdash t_1 \in c_1 \Rightarrow R \in c_1}\ \Rightarrow\text{-d}}{R \in R \vdash t_1 \sim R}\ \forall\text{-d}}{R \in R, t_1 \sim R \Rightarrow t_1 \in R \Rightarrow C \vdash}\ \Rightarrow\text{-g}}{R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C \vdash}\ \forall\text{-g}}{R \in R \vdash}\ \uparrow\text{-g}$$

$$\dfrac{\vdash R \in R \qquad R \in R \vdash}{\vdash}\ \text{Coup}$$

Notre Approche par l'Exemple (suite)

Paradoxe de Russell : $R \in R \longrightarrow \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C$ où

$$y \sim z \quad \overset{!}{=} \quad \forall x.\, (y \in x \Rightarrow z \in x)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{R \in t_0, c_0 \in R \vdash R \in R, C \qquad c_0 \in R \vdash c_0 \in t_0, R \in R, C}{c_0 \in t_0 \Rightarrow R \in t_0, c_0 \in R \vdash R \in R, C}\ \Rightarrow\text{-g}}{c_0 \sim R, c_0 \in R \vdash R \in R, C}\ \forall\text{-g}}{c_0 \sim R \vdash R \in R, c_0 \in R \Rightarrow C}\ \Rightarrow\text{-d}}{\vdash R \in R, c_0 \sim R \Rightarrow c_0 \in R \Rightarrow C}\ \Rightarrow\text{-d}}{\vdash R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C}\ \forall\text{-d}}{\vdash R \in R}\ \uparrow\text{-d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{R \in R, C \vdash \qquad R \in R \vdash t_1 \in R}{R \in R, t_1 \in R \Rightarrow C \vdash}\ \Rightarrow\text{-g} \qquad \dfrac{\dfrac{R \in R, t_1 \in c_1 \vdash R \in c_1}{R \in R \vdash t_1 \in c_1 \Rightarrow R \in c_1}\ \Rightarrow\text{-d}}{R \in R \vdash t_1 \sim R}\ \forall\text{-d}}{R \in R, t_1 \sim R \Rightarrow t_1 \in R \Rightarrow C \vdash}\ \Rightarrow\text{-g}}{R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C \vdash}\ \forall\text{-g}}{R \in R \vdash}\ \uparrow\text{-g}}{\vdash}\ \text{Coup}$$

Unification (sur les t_i) : $t_0 = R, t_1 = R$

Notre Approche par l'Exemple (suite)

Paradoxe de Russell : $R \in R \longrightarrow \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C$ où

$$y \sim z \quad \overset{!}{=} \quad \forall x.\, (y \in x \Rightarrow z \in x)$$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
R \in t_0, c_0 \in R \vdash R \in R, C \qquad c_0 \in R \vdash c_0 \in t_0, R \in R, C
}{
c_0 \in t_0 \Rightarrow R \in t_0, c_0 \in R \vdash R \in R, C
}\;\Rightarrow\text{-g}
}{
c_0 \sim R, c_0 \in R \vdash R \in R, C
}\;\forall\text{-g}
}{
c_0 \sim R \vdash R \in R, c_0 \in R \Rightarrow C, C
}\;\Rightarrow\text{-d}
}{
\vdash R \in R, c_0 \sim R \Rightarrow c_0 \in R \Rightarrow C, C
}\;\Rightarrow\text{-d}
}{
\vdash R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C, C
}\;\forall\text{-d}
}{
\vdash R \in R, C
}\;\uparrow\text{-d}
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{
{\color{red} R \in R, C \vdash C} \qquad R \in R \vdash t_1 \in R, C
}{
R \in R, t_1 \in R \Rightarrow C \vdash C
}\;\Rightarrow\text{-g}
\qquad
\dfrac{
\dfrac{
R \in R, t_1 \in c_1 \vdash R \in c_1, C
}{
R \in R \vdash t_1 \in c_1 \Rightarrow R \in c_1, C
}\;\Rightarrow\text{-d}
}{
R \in R \vdash t_1 \sim R, C
}\;\forall\text{-d}
}{
R \in R, t_1 \sim R \Rightarrow t_1 \in R \Rightarrow C \vdash C
}\;\Rightarrow\text{-g}
}{
R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C \vdash C
}\;\forall\text{-g}
}{
R \in R \vdash C
}\;\uparrow\text{-g}
$$

$$\dfrac{\vdash R \in R, C \qquad R \in R \vdash C}{\vdash C}\;\text{Coup}$$

Unification (sur les t_i) : $t_0 = R, t_1 = R$

Notre Approche par l'Exemple (suite)

Paradoxe de Russell : $R \in R \longrightarrow \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C$ où
$y \sim z \quad \stackrel{!}{=} \quad \forall x.\, (y \in x \Rightarrow z \in x)$

$$
\begin{prooftree}
\AxiomC{$R \in t_0, c_0 \in R \vdash R \in R, C$}
\AxiomC{$c_0 \in R \vdash c_0 \in t_0, R \in R, C$}
\RightLabel{$\Rightarrow$-g}
\BinaryInfC{$c_0 \in t_0 \Rightarrow R \in t_0, c_0 \in R \vdash R \in R, C$}
\RightLabel{$\forall$-g}
\UnaryInfC{$c_0 \sim R, c_0 \in R \vdash R \in R, C$}
\RightLabel{$\Rightarrow$-d}
\UnaryInfC{$c_0 \sim R \vdash R \in R, c_0 \in R \Rightarrow C, C$}
\RightLabel{$\Rightarrow$-d}
\UnaryInfC{$\vdash R \in R, c_0 \sim R \Rightarrow c_0 \in R \Rightarrow C, C$}
\RightLabel{$\forall$-d}
\UnaryInfC{$\vdash R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C, C$}
\RightLabel{$\uparrow$-d}
\UnaryInfC{$\vdash R \in R, C$}
\AxiomC{$R \in R, C \vdash C$}
\AxiomC{$R \in R \vdash t_1 \in R, C$}
\RightLabel{$\Rightarrow$-g}
\BinaryInfC{$R \in R, t_1 \in R \Rightarrow C \vdash C$}
\AxiomC{$R \in R, t_1 \in c_1 \vdash R \in c_1, C$}
\RightLabel{$\Rightarrow$-d}
\UnaryInfC{$R \in R \vdash t_1 \in c_1 \Rightarrow R \in c_1, C$}
\RightLabel{$\forall$-d}
\UnaryInfC{$R \in R \vdash t_1 \sim R, C$}
\RightLabel{$\Rightarrow$-g}
\BinaryInfC{$R \in R, t_1 \sim R \Rightarrow t_1 \in R \Rightarrow C \vdash C$}
\RightLabel{$\forall$-g}
\UnaryInfC{$R \in R, \forall y.\, y \sim R \Rightarrow y \in R \Rightarrow C \vdash C$}
\RightLabel{$\uparrow$-g}
\UnaryInfC{$R \in R \vdash C$}
\RightLabel{Coup}
\BinaryInfC{$\vdash C$}
\end{prooftree}
$$

Unification (sur les t_i) : $t_0 = R, t_1 = R$

Nouvelle règle :

$$C \longrightarrow \top$$

Perspectives

- Possibilité de traiter les théories avec quantificateurs

Perspectives

- Possibilité de traiter les théories avec quantificateurs
- Pas besoin de modèle $\Rightarrow$ appliquable aux théories inconsistantes

Perspectives

- Possibilité de traiter les théories avec quantificateurs
- Pas besoin de modèle $\Rightarrow$ appliquable aux théories inconsistantes

mais ...

- 3 propositions atomiques ou plus dans la preuve avec coupure ? 0 ?

Perspectives

- Possibilité de traiter les théories avec quantificateurs
- Pas besoin de modèle $\Rightarrow$ appliquable aux théories inconsistantes

mais . . .

- 3 propositions atomiques ou plus dans la preuve avec coupure ? 0 ?
- Complexité ?

Perspectives

- Possibilité de traiter les théories avec quantificateurs
- Pas besoin de modèle $\Rightarrow$ appliquable aux théories inconsistantes

mais . . .

- 3 propositions atomiques ou plus dans la preuve avec coupure ? 0 ?
- Complexité ?

Il reste à :

- trouver un ordre convenable pour que les preuves critiques correspondent à celle décrites

Perspectives

- Possibilité de traiter les théories avec quantificateurs
- Pas besoin de modèle $\Rightarrow$ appliquable aux théories inconsistantes

mais . . .

- 3 propositions atomiques ou plus dans la preuve avec coupure ? 0 ?
- Complexité ?

Il reste à :

- trouver un ordre convenable pour que les preuves critiques correspondent à celle décrites
- bien définir la relation entre règle de réécriture sur les propositions et conclusion d'une preuve

BACHMAIR (L.), *Proof methods for equational theories*.
Thèse de doctorat, University of Illinois, Urbana-Champaign, (Ill., USA), 1987.
Version révisée, août 1988.

BONACINA (M. P.) et DERSHOWITZ (N.), « Abstract Canonical Inference », *ACM Transactions on Computational Logic*, 2005.

DERSHOWITZ (N.), « Canonicity », dans DAHN (I.) et VIGNERON (L.), éditeurs, *Fourth International Workshop on First-Order Theorem Proving (FTP)*, vol. 86. Electronic Notes in Theoretical Computer Science, juin 2003.

DERSHOWITZ (N.) et KIRCHNER (C.), « Abstract Canonical Presentations », *Theorical Computer Science*, 2004.
Soumis.

DOWEK (G.), « What is a theory ? », dans *STACS '02 : Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science*, p. 50–64, London, UK, 2002. Springer-Verlag.

DOWEK (G.), « Confluence as a cut elimination property. », dans NIEUWENHUIS (R.), éditeur, *RTA*, vol. 2706 (coll. *Lecture Notes in Computer Science*), p. 2–13. Springer, 2003.

DOWEK (G.), HARDIN (T.) et KIRCHNER (C.), « Theorem proving modulo », *J. Autom. Reason.*, vol. 31, n^{o} 1, 2003, p. 33–72.

HUET (G.), « A complete proof of correctness of the Knuth-Bendix completion algorithm ».
Rapport technique n^{o} 25, INRIA, août 1980.

KNUTH (D. E.) et BENDIX (P. B.), « Simple word problems in universal algebras », dans LEECH (J.), éditeur, *Computational Problems in Abstract Algebra*, p. 263–297. Pergamon Press, Oxford, 1970.

MESEGUER (J.), « Conditional rewriting logic as a unified model of concurrency », *Theoretical Computer Science*, vol. 96, n^{o} 1, 1992, p. 73–155.

NEWMAN (M. H. A.), « On theories with a combinatorial definition of equivalence », dans *Annals of Math*, vol. 43, p. 223–243, 1942.

Règles d'Inférence de la Complétion Standard [Knuth et Bendix, 1970, Bachmair, 1987]

Déduit : Si $s = t \in CP(R)$

$$E, R \quad \rightsquigarrow \quad E \cup \{s = t\}, R$$

Oriente : Si $s \gg t$

$$E \cup \{s = t\}, R \quad \rightsquigarrow \quad E, R \cup \{s \rightarrow t\}$$

Supprime :

$$E \cup \{s = s\}, R \quad \rightsquigarrow \quad E, R$$

Simplifie : Si $s \xrightarrow[R]{} u$

$$E \cup \{s = t\}, R \quad \rightsquigarrow \quad E \cup \{u = t\}, R$$

Compose : Si $t \xrightarrow[R]{} u$

$$E, R \cup \{s \rightarrow t\} \quad \rightsquigarrow \quad E, R \cup \{s \rightarrow u\}$$

Combine : Si $s \xrightarrow[v \rightarrow w \in R]{} u$, et $s \blacktriangleright v$,

$$E, R \cup \{s \rightarrow t\} \quad \rightsquigarrow \quad E \cup \{u = t\}, R$$

Retour