# Étude et instances de systèmes de preuves ordonnées

## École Jeunes Chercheurs en Programmation

Guillaume Burel

LORIA – Université Henri Poincaré
Encadrant : Claude Kirchner

juin 2006


# Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques : séquents, preuves équationnelles, formes clausales. . .

# Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques : séquents, preuves équationnelles, formes clausales. . .

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

# Introduction

Démonstration automatique et interactive : de nombreux formalismes logiques : séquents, preuves équationnelles, formes clausales. . .

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 : séquents, preuves équationnelles, formes clausales. . .

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 : séquents, preuves équationnelles, formes clausales. . .

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 : séquents, preuves équationnelles, formes clausales. . .

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 (SCA) introduit par N.Dershowitz et C. Kirchner : la notion de bonne preuve est traduite par un ordre sur les preuves

# Introduction

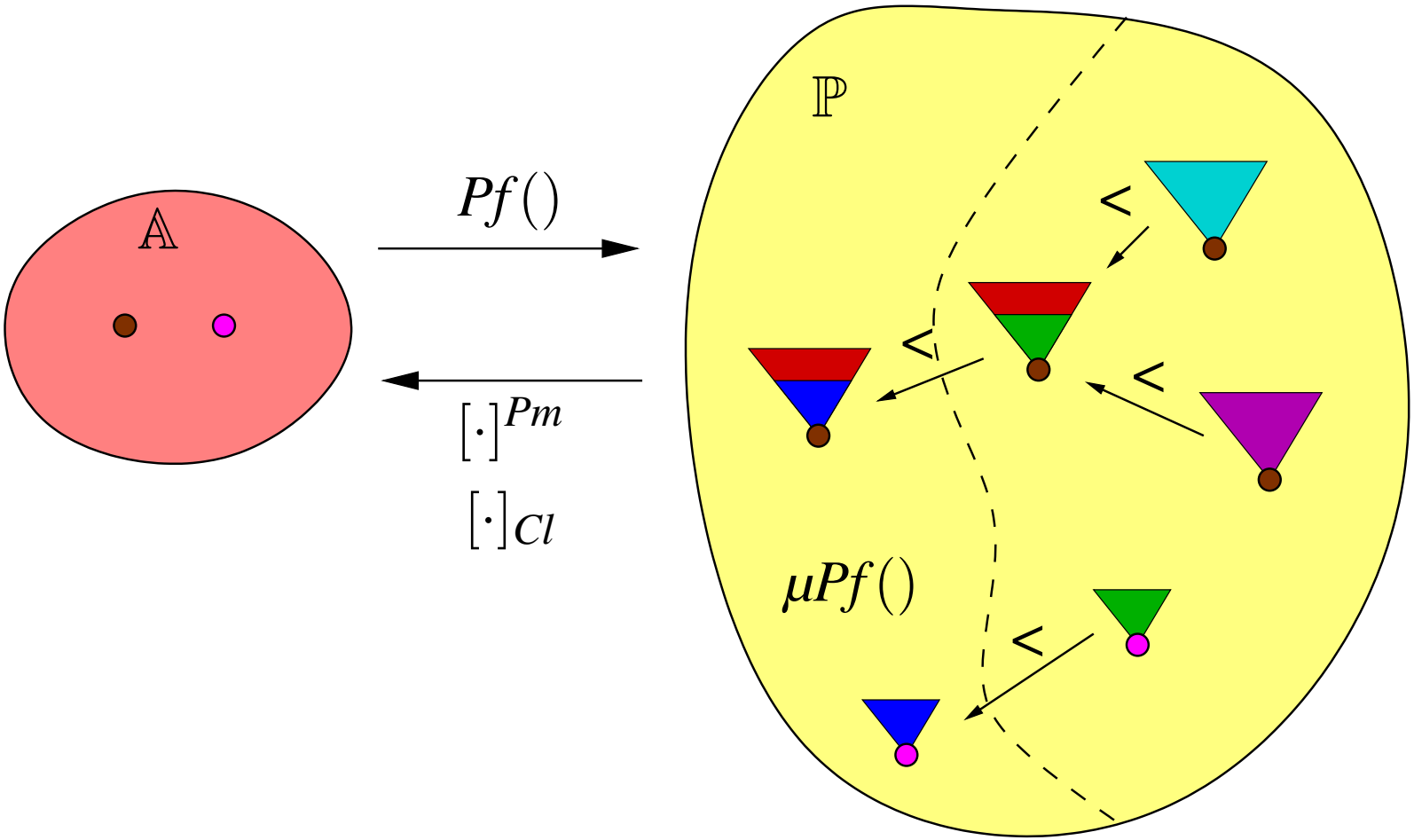
Démonstration automatique et interactive : de nombreux formalismes logiques : séquents, preuves équationnelles, formes clausales. . .

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 (SCA) introduit par N.Dershowitz et C. Kirchner : la notion de bonne preuve est traduite par un ordre sur les preuves

Notion de complétion abstraite qui permet de retrouver un système ayant les bonnes propriétés ; ici on va l'appliquer à la déduction modulo pour recouvrer l'élimination des coupures

# Définitions




+ 5 postulats

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

# Complétion

**Définition 1 (Preuves Critiques).**

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

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

# Complétion

**Définition 1 (Preuves Critiques).**

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

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

La complétion consiste à ajouter les conclusions des preuves critiques :

$$A \rightsquigarrow A \cup \{[p]_{Cl} : p \text{ critique}\}$$

# Complétion

## Définition 1 (Preuves Critiques).

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

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

La complétion consiste à ajouter les conclusions des preuves critiques :

$$A \rightsquigarrow A \cup \{[p]_{Cl} : p \text{ critique}\}$$

## Théorème 1 (Complétude).

*La limite $A_\infty$ de cette procédure est complète :*

$$ThA_0 \subseteq [Pf(A_\infty) \cap \mu Pf(ThA_0)]_{Cl}$$

# Calcul des Séquents Modulo

Déduction modulo = déduction + calcul (principe de Poincaré)

# Calcul des Séquents Modulo

Déduction modulo = déduction + calcul (principe de Poincaré)

Déduction : calcul des séquents de Gentzen

$$\frac{}{\Gamma, A \vdash A, \Delta}\ \text{Axiom}$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A, \Delta}\ \neg\text{-d}$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge\text{-d}$$

$$\frac{\Gamma \vdash \{t/x\}A, \Delta}{\Gamma \vdash \exists x.\ A, \Delta}\ \exists\text{-d}$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma \vdash A, \Delta}{\Gamma \vdash \Delta}\ \text{Coup}$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}\ \Rightarrow\text{-d}$$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee\text{-d}$$

$$\frac{\Gamma \vdash \{c/x\}A, \Delta}{\Gamma \vdash \forall x.\ A, \Delta}\ \forall\text{-d}\ \text{avec } c \text{ fraîche}$$

# Calcul des Séquents Modulo

Déduction modulo = déduction + calcul (principe de Poincaré)

Déduction : calcul des séquents de Gentzen

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

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

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

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

Calcul : règles de conversion :

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

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

Il n'y a pas de preuve sans coupure de $B \vdash$

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

Il n'y a pas de preuve sans coupure de $B \vdash$

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

$$B \longrightarrow B \wedge \bot$$

# Preuve critique en déduction modulo

Congruence (Crabbé) : $A \longrightarrow B \wedge \neg A$

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

Il n'y a pas de preuve sans coupure de $B \vdash$

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

$$B \longrightarrow \bot$$

Avec cette règle ajoutée, le système a la propriété d'élimination des coupures

# Perspectives

- Les quantificateurs posent problème dans certains cas $\longrightarrow$ étude par exemple de l'inférence profonde comme système canonique abstrait, de façon à obtenir un algorithme de complétion donnant la propriété d'élimination des coupures pour toute formule du premier ordre

# Perspectives

- Les quantificateurs posent problème dans certains cas $\longrightarrow$ étude par exemple de l'inférence profonde comme système canonique abstrait, de façon à obtenir un algorithme de complétion donnant la propriété d'élimination des coupures pour toute formule du premier ordre
- Implémentation (à l'aide d'une variante de la méthode des tableaux pour la déduction modulo) $\longrightarrow$ TOM, OCaml/Zenon ?

# Perspectives

- Les quantificateurs posent problème dans certains cas $\longrightarrow$ étude par exemple de l'inférence profonde comme système canonique abstrait, de façon à obtenir un algorithme de complétion donnant la propriété d'élimination des coupures pour toute formule du premier ordre
- Implémentation (à l'aide d'une variante de la méthode des tableaux pour la déduction modulo) $\longrightarrow$ TOM, OCaml/Zenon ?
- Étude d'autres systèmes de preuves, par exemple ceux qui évoluent avec la théorie, comme la déduction surnaturelle introduite par B. Wack, éventuellement modification des systèmes canoniques abstraits pour couvrir ces cas