[1]Université Henri Poincaré [2]INRIA [3]LORIA

Cut Elimination in Deduction Modulo by Abstract Completion

Symposium on Logical Foundations of Computer Science

Guillaume Burel[1,3] Claude Kirchner[2,3]

June 5th, 2007

A simple proof?

$$\vdash 1 + 1 = 2$$

A simple proof?

$$\vdash s(0) + s(0) = s(s(0))$$

A simple proof?

$$\Gamma = \forall x\ y.\ s(x) + y = x + s(y),\ \forall x.\ 0 + x = x$$

$$\Gamma \vdash 1 + 1 = 2$$

A simple proof?

$$\Gamma = \forall x\ y.\ s(x) + y = x + s(y),\ \forall x.\ 0 + x = x$$

$$\forall\text{-I}\ \frac{\Gamma, 1 + 1 = 0 + 2 \vdash 1 + 1 = 2}{\Gamma \vdash 1 + 1 = 2}\ x := 0, y := s(0)$$

A simple proof?

$$\Gamma = \forall x\ y.\ s(x) + y = x + s(y),\ \forall x.\ 0 + x = x$$

$$\dfrac{\dfrac{\Gamma, 1+1=0+2, 0+2=2 \vdash 1+1=2}{\Gamma, 1+1=0+2 \vdash 1+1=2}\ \forall\text{-l}\ x := 2}{\Gamma \vdash 1+1=2}\ \forall\text{-l}\ x := 0, y := s(0)$$

A simple proof?

$\Gamma = \forall x\ y.\ s(x) + y = x + s(y),\ \forall x.\ 0 + x = x,\ \forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z$

$$\forall\text{-l}\ \dfrac{\Gamma, 1+1=0+2, 0+2=2,\ 1+1=0+2 \Rightarrow 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2}{\Gamma, 1+1=0+2, 0+2=2 \vdash 1+1=2}\ \begin{array}{l} x := 1+1 \\ y := 0+2 \\ z := 2 \end{array}$$

$$\forall\text{-l}\ \dfrac{\Gamma, 1+1=0+2, 0+2=2 \vdash 1+1=2}{\Gamma, 1+1=0+2 \vdash 1+1=2}\ x := 2$$

$$\forall\text{-l}\ \dfrac{\Gamma, 1+1=0+2 \vdash 1+1=2}{\Gamma \vdash 1+1=2}\ x := 0, y := s(0)$$

A simple proof?

$$\Gamma = \forall x\ y.\ s(x) + y = x + s(y),\ \forall x.\ 0 + x = x,\ \forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z$$

$$\Rightarrow\text{-l}\ \dfrac{1+1=2 \vdash 1+1=2 \qquad 0+2=2 \vdash 0+2=2}{\Gamma, 0+2=2,\ 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2}$$

$$\Rightarrow\text{-l}\ \dfrac{\Gamma, 0+2=2,\ 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2 \qquad 1+1=0+2 \vdash 1+1=0+2}{\Gamma, 1+1=0+2, 0+2=2,\ 1+1=0+2 \Rightarrow 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2}$$

$$\forall\text{-l}\ \dfrac{\Gamma, 1+1=0+2, 0+2=2,\ 1+1=0+2 \Rightarrow 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2}{\Gamma, 1+1=0+2, 0+2=2 \vdash 1+1=2}\ \begin{array}{l} x := 1+1 \\ y := 0+2 \\ z := 2 \end{array}$$

$$\forall\text{-l}\ \dfrac{\Gamma, 1+1=0+2, 0+2=2 \vdash 1+1=2}{\Gamma, 1+1=0+2 \vdash 1+1=2}\ x := 2$$

$$\forall\text{-l}\ \dfrac{\Gamma, 1+1=0+2 \vdash 1+1=2}{\Gamma \vdash 1+1=2}\ x := 0, y := s(0)$$

A simple proof?

$$\Gamma = \forall x\ y.\ s(x) + y = x + s(y),\ \forall x.\ 0 + x = x,\ \forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{1+1=2 \vdash 1+1=2}\text{Ax} \quad \dfrac{}{0+2=2 \vdash 0+2=2}\text{Ax}}{\Gamma, 0+2=2 \quad 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2}\Rightarrow\text{-l} \quad \dfrac{}{1+1=0+2 \vdash 1+1=0+2}\text{Ax}}{\Gamma, 1+1=0+2, 0+2=2 \quad 1+1=0+2 \Rightarrow 0+2=2 \Rightarrow 1+1=2 \vdash 1+1=2}\Rightarrow\text{-l}}{\Gamma, 1+1=0+2, 0+2=2 \vdash 1+1=2}\forall\text{-l}\ \begin{matrix} x := 1+1 \\ y := 0+2 \\ z := 2 \end{matrix}}{\Gamma, 1+1=0+2 \vdash 1+1=2}\forall\text{-l}\ x := 2}{\Gamma \vdash 1+1=2}\forall\text{-l}\ x := 0, y := s(0)$$

Proving vs. verifying

Poincaré 1902:
“Ce n’est pas une démonstration proprement dite [. . .] c’est une vérification”

Proving vs. verifying

Poincaré 1902:
"Ce n'est pas une démonstration proprement dite [...] c'est une vérification"

Poincaré's principle: identifying computation and deduction
$\rightsquigarrow$ deduction modulo [Dowek et al., 2003]

Deduction modulo

Computational part expressed as a rewrite system over terms and propositions

Deduction modulo

Computational part expressed as a rewrite system over terms and propositions
For instance

$$s(x) + y \rightarrow x + s(y)$$
$$x \times y = 0 \rightarrow x = 0 \vee y = 0$$

Deduction modulo

Computational part expressed as a rewrite system over terms and propositions
For instance

$$s(x) + y \longrightarrow x + s(y)$$
$$x \times y = 0 \longrightarrow x = 0 \vee y = 0$$

Inferences performed modulo this congruence:

$$\exists\text{-l}\ \frac{\Gamma, \{y/x\}P \vdash \Delta}{\Gamma, Q \vdash \Delta} \quad Q \overset{*}{\longleftrightarrow} \exists x.\ P,\ y \text{ fresh}$$

Example of a proof in deduction modulo

$$\top\text{-r}\ \frac{}{\vdash 1+1=2}\ 1+1=2 \xrightarrow{*} 2=2 \longrightarrow \top$$

Example of a proof in deduction modulo

$$\top\text{-r}\ \frac{}{\vdash 1+1=2}\ 1+1=2 \xrightarrow{*} 2=2 \longrightarrow \top$$

$$\forall\text{-r}\ \dfrac{\Rightarrow\text{-r}\ \dfrac{z \times z - 4z + 4 = 0 \vdash z = 2}{\vdash z \times z - 4z + 4 = 0 \Rightarrow z = 2}}{\vdash \forall x.\ x \times x - 4x + 4 = 0 \Rightarrow x = 2}\ z \text{ is fresh}$$

Example of a proof in deduction modulo

$$\top\text{-r}\ \frac{}{\vdash 1+1=2}\ 1+1=2 \xrightarrow{*} 2=2 \longrightarrow \top$$

$$\forall\text{-r}\ \dfrac{\Rightarrow\text{-r}\ \dfrac{\vee\text{-l}\ \dfrac{}{z\times z-4z+4=0 \vdash z=2}}{\vdash z\times z-4z+4=0 \Rightarrow z=2}}{\vdash \forall x.\ x\times x-4x+4=0 \Rightarrow x=2}\ z \text{ is fresh}$$

$$z\times z-4z+4=0 \xleftrightarrow{*} (z-2)\times(z-2)=0 \xleftrightarrow{*} z-2=0 \vee z-2=0$$

Example of a proof in deduction modulo

$$\top\text{-r}\ \frac{}{\vdash 1+1=2}\ 1+1=2 \xrightarrow{*} 2=2 \longrightarrow \top$$

$$z-2=0 \vdash z=2$$

$$\vdots$$

$$\forall\text{-r}\ \dfrac{\Rightarrow\text{-r}\ \dfrac{\vee\text{-l}\ \dfrac{z-2=0 \vdash z=2 \qquad \begin{matrix} z-2=0 \vdash z=2 \\ \vdots \end{matrix}}{z \times z - 4z + 4 = 0 \vdash z = 2}\ \begin{array}{l} z \times z - 4z + 4 = 0 \\ \xleftrightarrow{*} (z-2) \times (z-2) = 0 \\ \xleftrightarrow{*} z-2=0 \vee z-2=0 \end{array}}{\vdash z \times z - 4z + 4 = 0 \Rightarrow z = 2}}{\vdash \forall x.\ x \times x - 4x + 4 = 0 \Rightarrow x = 2}\ z \text{ is fresh}$$

Example of a proof in deduction modulo

$$\top\text{-r}\ \frac{}{\vdash 1+1=2}\ 1+1=2 \xrightarrow{*} 2=2 \longrightarrow \top$$

$$\text{Ax}\ \frac{}{z-2=0 \vdash z=2}\ \begin{array}{l} z-2=0 \\ \xleftrightarrow{*} z=2 \end{array}$$

$$\vdots$$

$$\vee\text{-l}\ \dfrac{\text{Ax}\ \dfrac{}{z-2=0 \vdash z=2}\ \begin{array}{l} z-2=0 \\ \xleftrightarrow{*} z=2 \end{array} \qquad \vdots}{z \times z - 4z + 4 = 0 \vdash z = 2}\ \begin{array}{l} z \times z - 4z + 4 = 0 \\ \xleftrightarrow{*} (z-2) \times (z-2) = 0 \\ \xleftrightarrow{*} z-2=0 \vee z-2=0 \end{array}$$

$$\Rightarrow\text{-r}\ \frac{z \times z - 4z + 4 = 0 \vdash z = 2}{\vdash z \times z - 4z + 4 = 0 \Rightarrow z = 2}$$

$$\forall\text{-r}\ \frac{\vdash z \times z - 4z + 4 = 0 \Rightarrow z = 2}{\vdash \forall x.\ x \times x - 4x + 4 = 0 \Rightarrow x = 2}\ z \text{ is fresh}$$

Asymmetric sequent calculus modulo

[Gentzen, 1934] sequent calculus:

$$\text{Cut}\ \frac{\Gamma, A \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma \vdash \Delta} \qquad \exists\text{-l}\ \frac{\Gamma, \{y/x\}P \vdash \Delta}{\Gamma, \exists x.\ P \vdash \Delta}\ y \text{ fresh}$$

$$\Rightarrow\text{-l}\ \frac{\Gamma, B \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma, A \Rightarrow B \vdash \Delta} \qquad \exists\text{-r}\ \frac{\Gamma \vdash \{t/x\}P, \exists x.\ P, \Delta}{\Gamma \vdash \exists x.\ P, \Delta}$$

$+$ externalized congruence rules:

$$\uparrow\text{-l}\ \frac{\Gamma, A, P \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{if } A \longrightarrow P \qquad \uparrow\text{-r}\ \frac{\Gamma \vdash A, P, \Delta}{\Gamma \vdash A, \Delta}\ \text{if } A \longrightarrow P$$

Important facts about deduction modulo

Simulates theories:

- Higher Order Logic [Dowek et al., 2001]
- Zermelo [Dowek and Miquel, 2007]
- Arithmetic [Dowek and Werner, 2005]
- Pure Type Systems [Cousineau and Dowek, 2007]

Proof search methods:

- Resolution: ENAR [Dowek et al., 2003]
- Tableaux: TaMed [Bonichon, 2004]

Proof-length speed-ups [Burel, 2007]

Deduction modulo and cut admissibility

Definition 1.
A rewrite systems R *admits* Cut if all sequents provable modulo R can be proved modulo R without Cut

$\emptyset$ admits Cut (Gentzen's Hauptsatz)
Cut admissibility implies

- subformula property
- completeness of automated provers

Do all rewrite systems admit Cut ?

Crabbé counterexample

Rewrite system: $A \to B \land \neg A$

Crabbé counterexample

Rewrite system: $A \longrightarrow B \wedge \neg A$

Search for a minimal counterexample:

$$\text{Cut}\ \frac{A \wedge B \vdash \qquad\qquad \vdash A \wedge B}{\vdash}$$

Crabbé counterexample

Rewrite system: $A \rightarrow B \wedge \neg A$

Search for a minimal counterexample:

$$
\text{Cut}\ \dfrac{\wedge\text{-l}\ \dfrac{\uparrow\text{-l}\ \dfrac{\wedge\text{-l}\ \dfrac{\neg\text{-l}\ \dfrac{\text{Ax}\ \dfrac{}{A, B, B \vdash A}}{A, B, \neg A, B \vdash}}{A, B \wedge \neg A, B \vdash}}{A, B \vdash}}{A \wedge B \vdash} \qquad \vdash A \wedge B}{\vdash}
$$

Crabbé counterexample

Rewrite system: $A \longrightarrow B \wedge \neg A$

Search for a minimal counterexample:

$$
\text{Cut}\;\dfrac{
\wedge\text{-l}\;\dfrac{
\uparrow\text{-l}\;\dfrac{
\wedge\text{-l}\;\dfrac{
\neg\text{-l}\;\dfrac{
\text{Ax}\;\dfrac{}{A, B, B \vdash A}
}{A, B, \neg A, B \vdash}
}{A, B \wedge \neg A, B \vdash}
}{A, B \vdash}
}{A \wedge B \vdash}
\qquad
\wedge\text{-r}\;\dfrac{
\uparrow\text{-r}\;\dfrac{
\wedge\text{-r}\;\dfrac{
\vdash A, B
\qquad
\neg\text{-r}\;\dfrac{
\text{Ax}\;\dfrac{}{A \vdash A}
}{\vdash A, \neg A}
}{\vdash A, B \wedge \neg A}
}{\vdash A}
\qquad
\vdash B
}{\vdash A \wedge B}
}{\vdash}
$$

Crabbé counterexample

Rewrite system: $A \longrightarrow B \wedge \neg A$

Search for a minimal counterexample:

$$
\text{Cut}\;\dfrac{
\wedge\text{-l}\;\dfrac{
\uparrow\text{-l}\;\dfrac{
\wedge\text{-l}\;\dfrac{
\neg\text{-l}\;\dfrac{
\text{Ax}\;\dfrac{}{B, A, B, B \vdash A}
}{B, A, B, \neg A, B \vdash}
}{B, A, B \wedge \neg A, B \vdash}
}{B, A, B \vdash}
}{B, A \wedge B \vdash}
\qquad
\wedge\text{-r}\;\dfrac{
\uparrow\text{-r}\;\dfrac{
\wedge\text{-r}\;\dfrac{
\text{Ax}\;\dfrac{}{B \vdash A, B}
\quad
\neg\text{-r}\;\dfrac{
\text{Ax}\;\dfrac{}{B, A \vdash A}
}{B \vdash A, \neg A}
}{B \vdash A, B \wedge \neg A}
}{B \vdash A}
\quad
\text{Ax}\;\dfrac{}{B \vdash B}
}{B \vdash A \wedge B}
}{B \vdash}
$$

Cut elimination

If there is no modulo, Cut is admissible (Gentzen's Hauptsatz)
There exists a cut elimination procedure:

$$\text{Cut}\,\dfrac{\wedge\text{-l}\,\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad \wedge\text{-l}\,\dfrac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}}{\Gamma \vdash \Delta}$$

becomes

$$\text{Cut}\,\dfrac{\text{Cut}\,\dfrac{\Gamma, A, B \vdash \Delta \qquad \Gamma, A \vdash B, \Delta}{\Gamma, A \vdash \Delta} \qquad \Gamma \vdash A, \Delta}{\Gamma \vdash \Delta}$$

Proofs with cuts are replaced by smaller counterexamples

Crabbé's counterexample (Cont.)

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

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{B, A, B, B \vdash A}\,\text{Ax}
}{B, A, B, \neg A, B \vdash}\,\neg\text{-l}
}{B, A, B \wedge \neg A, B \vdash}\,\wedge\text{-l}
}{B, A, B \vdash}\,\uparrow\text{-l}
\quad
\dfrac{}{B, A \vdash B}\,\text{Ax}
}{B, A \vdash}\,\text{Cut}
\quad
\dfrac{
\dfrac{
\dfrac{}{B \vdash B, A}\,\text{Ax}
\quad
\dfrac{
\dfrac{}{B, A \vdash A}\,\text{Ax}
}{B \vdash \neg A, A}\,\neg\text{-r}
}{B \vdash B \wedge \neg A, A}\,\wedge\text{-r}
}{B \vdash A}\,\uparrow\text{-r}
}{B \vdash}\,\text{Cut}
$$

Crabbé's counterexample (Cont.)

$$A \rightarrow B \wedge \neg A$$

$$
\text{Cut}\,\dfrac{
\uparrow\text{-l}\,\dfrac{
\wedge\text{-l}\,\dfrac{
\neg\text{-l}\,\dfrac{
\text{Ax}\,\dfrac{}{B, A, B \vdash A}
}{B, A, B, \neg A \vdash}
}{B, A, B \wedge \neg A \vdash}
}{B, A \vdash}
\qquad
\uparrow\text{-r}\,\dfrac{
\wedge\text{-r}\,\dfrac{
\text{Ax}\,\dfrac{}{B \vdash B, A}
\qquad
\neg\text{-r}\,\dfrac{
\text{Ax}\,\dfrac{}{B, A \vdash A}
}{B \vdash \neg A, A}
}{B \vdash B \wedge \neg A, A}
}{B \vdash A}
}{B \vdash}
$$

Crabbé's counterexample (Cont.)

$$A \rightarrow B \wedge \neg A$$

$$\text{Cut}\;\dfrac{\uparrow\text{-l}\;\dfrac{\wedge\text{-l}\;\dfrac{\neg\text{-l}\;\dfrac{\text{Ax}\;\dfrac{}{B, A, B \vdash A}}{B, A, B, \neg A \vdash}}{B, A, B \wedge \neg A \vdash}}{B, A \vdash} \qquad \uparrow\text{-r}\;\dfrac{\wedge\text{-r}\;\dfrac{\text{Ax}\;\dfrac{}{B \vdash B, A} \qquad \neg\text{-r}\;\dfrac{\text{Ax}\;\dfrac{}{B, A \vdash A}}{B \vdash \neg A, A}}{B \vdash B \wedge \neg A, A}}{B \vdash A}}{B \vdash}$$

$=$ minimal counterexample

Regaining Cut admissibility

Need to build a proof of $B \vdash$

Add a new rule to your system: $B \longrightarrow \bot$

$$\dfrac{\bot\text{-l}\ \dfrac{}{\bot \vdash}}{B \vdash}\ \uparrow\text{-l}$$

$\left\{ \begin{array}{l} A \longrightarrow B \wedge \neg A \\ B \longrightarrow \bot \end{array} \right.$ admits Cut

Term rewrite systems

[Dowek, 2003]: a *term* rewrite system is confluent iff it admits Cut

no longer true for *proposition* rewrite systems (Crabbé)

If a TRS is not confluent, use standard (a.k.a. Knuth-Bendix) completion to get an equivalent confluent TRS

$\rightsquigarrow$ a generalized completion procedure to recover cut admissibility ?

Outline

- Introduction
  - Deduction modulo
  - Cut admissibility
- **Limitations**
- A Formalism for Abstract Completion
- Example of application
- Conclusion

Undecidability of cut admissibility

Theorem 2.
The following problem is undecidable:
input: a rewrite system R
answer: determine if R admits Cut

Undecidability of cut admissibility

Theorem 2.

The following problem is undecidable:
input: a rewrite system R
answer: determine if R admits Cut

Proof:

Let P be a first order proposition, $r, \in$ not in P,

let $R_P = \Big\{ r \in r \to \forall y.\ (\forall x.\ y \in x \Rightarrow r \in x) \Rightarrow y \in r \Rightarrow P$

P is valid iff R_P admits Cut
(Models for deduction modulo [Hermant, 2003])

Outline

Abstract Canonical Systems [Dershowitz and Kirchner, 2006]

Based on proof ordering

General notion of canonicity, saturation, redundacy

Critical proofs = minimal counter-examples

Abstract definition of a completion procedure [Bonacina and Dershowitz, 2007]:
Adding the premises of proofs smaller than the critical ones

Proof ordering

Proofs are trees:
Recursive Path Ordering

Precedence

- Proofs with Cut are greater: Cut(P) $>$ r
- Compatible with the Cut elimination procedure:
  Cut(P) $>$ Cut(Q) if Q is a subformula of P

Critical Proofs

Lemma 3 (Form of critical proofs).

$$
\dfrac{\uparrow\text{-l}\ \dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma, A, P \vdash \Delta\end{matrix}}{\Gamma, A \vdash \Delta}\ A \longrightarrow P \qquad \uparrow\text{-r}\ \dfrac{\begin{matrix}\pi_2\\ \vdots\\ \Gamma \vdash A, Q, \Delta\end{matrix}}{\Gamma \vdash A, \Delta}\ A \longrightarrow Q}{\Gamma \vdash \Delta}\ \text{Cut}
$$

Critical Proofs

Lemma 3 (Form of critical proofs).

$$
\dfrac{\uparrow\text{-l}\ \dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma, A, P \vdash \Delta\end{matrix}}{\Gamma, A \vdash \Delta}\ A \longrightarrow P \qquad \uparrow\text{-r}\ \dfrac{\begin{matrix}\pi_2\\ \vdots\\ \Gamma \vdash A, Q, \Delta\end{matrix}}{\Gamma \vdash A, \Delta}\ A \longrightarrow Q}{\Gamma \vdash \Delta}\ \text{Cut}
$$

Note: it is also undecidable to know if a sequent is the conclusion of a critical proof or not

Smaller proofs

Try to build a Cut-free proof:

- Indifferently apply any inference rule (apply ∀-l and ∃-r only once)
- When reaching a sequent $\Gamma, A \vdash \Delta$ with A atomic, rewrite A into $A \wedge \forall x_1, \ldots, x_n.\ (\neg\Gamma \vee \Delta)$
- $\rightsquigarrow$ the branch can be close
  (also symmetrically for $\Gamma \vdash A, \Delta$)

complete the rewrite system with these new
$A \to A \wedge \forall x_1, \ldots, x_n.\ (\neg\Gamma \vee \Delta)$ and
$A \to A \vee \exists x_1, \ldots, x_n.\ (\Gamma \wedge \neg\Delta)$

Main theorem

Theorem 4.
Asymmetric deduction modulo is an instance of abstract canonical system

Corollary 5 (Cut Admissibility of the Limit).
$\Gamma \vdash \Delta$ *has a proof in* R_0 *if and only if it has a cut-free proof in* R_∞

Outline

Crabbé with quantifiers: $A \rightarrow (\exists x.\ \forall y.\ B \wedge P(x,y)) \wedge \neg A$
($Q(x)$ denotes $\forall y.\ B \wedge P(x,y)$)
Critical proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x.\ Q(x), A, \exists x.\ Q(x) \vdash A}\ \text{Ax}}{\exists x.\ Q(x), A, \exists x.\ Q(x), \neg A \vdash}\ \neg\text{-l}}{\exists x.\ Q(x), A, \exists x.\ Q(x) \wedge \neg A \vdash}\ \wedge\text{-l}}{\exists x.\ Q(x), A \vdash}\ \uparrow\text{-l} \qquad \dfrac{\dfrac{\dfrac{}{\exists x.\ Q(x) \vdash \exists x.\ Q(x), A}\ \text{Ax} \quad \dfrac{\dfrac{}{\exists x.\ Q(x), A \vdash A}\ \text{Ax}}{\exists x.\ Q(x) \vdash \neg A, A}\ \neg\text{-r}}{\exists x.\ Q(x) \vdash \exists x.\ Q(x) \wedge \neg A, A}\ \wedge\text{-r}}{\exists x.\ Q(x) \vdash A}\ \uparrow\text{-r}}{\exists x.\ Q(x) \vdash}\ \text{Cut}$$

Smaller proof:

$$\exists\text{-I}\ \dfrac{\forall\text{-I}\ \dfrac{\wedge\text{-I}\ \dfrac{Q(x), B, P(x,a) \vdash}{Q(x), B \wedge P(x,a) \vdash}}{Q(x) \vdash}\ y := a}{\exists x.\ Q(x) \vdash}\ x \text{ is fresh}$$

Smaller proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{Q(x), B, B \wedge \forall z.\ (\neg Q(z) \vee \neg P(z,a)), P(x,a) \vdash}{Q(x), B, P(x,a) \vdash}\ \uparrow\text{-l}}{Q(x), B \wedge P(x,a) \vdash}\ \wedge\text{-l}}{Q(x) \vdash}\ \forall\text{-l}\ y := a}{\exists x.\ Q(x) \vdash}\ \exists\text{-l}\ x \text{ is fresh}$$

New rule: $B \to B \wedge \forall z.\ (\neg Q(z) \vee \neg P(z,a))$.

Smaller proof:

$$\text{Ax}\ \frac{}{Q(x), B, P(x,a) \vdash Q(x)} \qquad \text{Ax}\ \frac{}{Q(x), B, P(x,a) \vdash P(x,a)}$$

$$\neg\text{-l}\ \frac{Q(x), B, P(x,a) \vdash Q(x)}{Q(x), B, \neg Q(x), P(x,a) \vdash} \qquad \neg\text{-l}\ \frac{Q(x), B, P(x,a) \vdash P(x,a)}{Q(x), B, \neg P(x,a), P(x,a) \vdash}$$

$$\vee\text{-l}\ \frac{Q(x), B, \neg Q(x), P(x,a) \vdash \qquad Q(x), B, \neg P(x,a), P(x,a) \vdash}{Q(x), B, \neg Q(x) \vee \neg P(x,a), P(x,a) \vdash}$$

$$\forall\text{-l}\ \frac{Q(x), B, \neg Q(x) \vee \neg P(x,a), P(x,a) \vdash}{Q(x), B, B, \forall z.\ (\neg Q(z) \vee \neg P(z,a)), P(x,a) \vdash}\ z := x$$

$$\wedge\text{-l}\ \frac{Q(x), B, B, \forall z.\ (\neg Q(z) \vee \neg P(z,a)), P(x,a) \vdash}{Q(x), B, B \wedge \forall z.\ (\neg Q(z) \vee \neg P(z,a)), P(x,a) \vdash}$$

$$\uparrow\text{-l}\ \frac{Q(x), B, B \wedge \forall z.\ (\neg Q(z) \vee \neg P(z,a)), P(x,a) \vdash}{Q(x), B, P(x,a) \vdash}$$

$$\wedge\text{-l}\ \frac{Q(x), B, P(x,a) \vdash}{Q(x), B \wedge P(x,a) \vdash}$$

$$\forall\text{-l}\ \frac{Q(x), B \wedge P(x,a) \vdash}{Q(x) \vdash}\ y := a$$

$$\exists\text{-l}\ \frac{Q(x) \vdash}{\exists x.\ Q(x) \vdash}\ x \text{ is fresh}$$

New rule: $B \to B \wedge \forall z.\ (\neg Q(z) \vee \neg P(z,a))$.

Outline

- use of the ACS to define a procedure to recover Cut admissibility in Deduction Modulo
- boundaries of the approach through undecidability results
- description precise enough to be implemented (in Tom/ocaml[1])

[1] `http://tom.loria.fr/`

Perspectives

- too many critical proofs: refinement of the proof ordering (for instance $A \to A \vee \exists x.\ P(x)$ subsumes $A \to A \vee P(t)$)
- provide cut admissibility but not normalization of proofs
- elimination of redundancies (simplification rules as in standard completion)
- link with superdeduction (new inference rules)

Bonacina, M. P. and Dershowitz, N. (2007).
Abstract canonical inference.
ACM Trans. Comput. Logic, 8(1).

Bonichon, R. (2004).
TaMeD: A tableau method for deduction modulo.
In Basin, D. A. and Rusinowitch, M., editors, *IJCAR*, volume 3097 of *Lecture Notes in Computer Science*, pages 445–459. Springer-Verlag.

Burel, G. (2007).
Unbounded proof-length speed-up in deduction modulo.
In *CSL*.

Cousineau, D. and Dowek, G. (2007).
Embedding pure type systems in the lambda-pi-calculus modulo.

In *TLCA*.
To appear.

Dershowitz, N. and Kirchner, C. (2006).
Abstract Canonical Presentations.
Theoretical Computer Science, 357:53–69.

Dowek, G. (2003).
Confluence as a cut elimination property.
In Nieuwenhuis, R., editor, *RTA*, volume 2706 of *Lecture Notes in Computer Science*, pages 2–13. Springer-Verlag.

Dowek, G., Hardin, T., and Kirchner, C. (2001).
HOL-$\lambda\sigma$ an intentional first-order expression of higher-order logic.
Mathematical Structures in Computer Science, 11(1):1–25.

Dowek, G., Hardin, T., and Kirchner, C. (2003).
Theorem proving modulo.
Journal of Automated Reasoning, 31(1):33–72.

Dowek, G. and Werner, B. (2005).
Arithmetic as a theory modulo.
In Giesl, J., editor, *RTA*, volume 3467 of *Lecture Notes in Computer Science*, pages 423–437. Springer-Verlag.

Gentzen, G. (1934).
Untersuchungen über das logische Schliessen.
Mathematische Zeitschrift, 39:176–210, 405–431.
Translated in Szabo, editor., *The Collected Papers of Gerhard Gentzen* as “Investigations into Logical Deduction”.

Hermant, O. (2003).

A model-based cut elimination proof.
In *2nd St-Petersburg Days of Logic and Computability*.