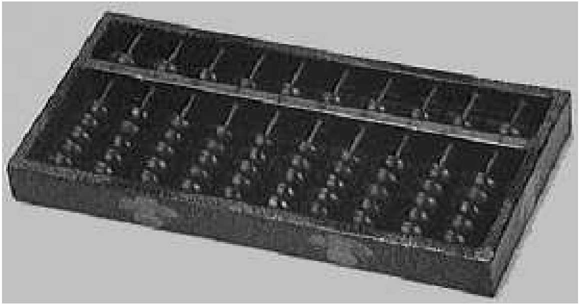
Deduction Modulo

Olivier HERMANT

Tuesday, December 12, 2006

Deduction and Computation



Deduction system: Gentzen's sequent calculus

$$\frac{}{\Gamma, P \vdash P}\text{axiom} \qquad \frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut}$$

$$\frac{\Gamma, P, P \vdash Q}{\Gamma, P \vdash Q}\text{contr-l} \qquad \frac{}{\Gamma, \bot \vdash Q}\bot\text{-g}$$

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R}\vee\text{-g} \qquad \frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q}\vee\text{-d} \qquad \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q}\vee\text{-d}$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \Rightarrow Q \vdash R}\Rightarrow\text{-g} \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash P \Rightarrow Q}\Rightarrow\text{-d}$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, \exists x P \vdash Q}\exists\text{-g}, \ c \text{ fresh} \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash \exists x P}\exists\text{-d}$$

The cut rule: a detour

$$\frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut}$$

- we prove $\Gamma \vdash P$
- we assume P and prove $\Gamma, P \vdash Q$
- it is a proof of $\Gamma \vdash Q$

The cut rule: a detour

$$\frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut}$$

- we prove $\Gamma \vdash P$
- we assume P and prove $\Gamma, P \vdash Q$
- it is a proof of $\Gamma \vdash Q$
- lemma application.

Deduction system: sequent calculus

$$\frac{}{\Gamma, P \vdash P}\text{axiom} \qquad \frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut}$$

$$\frac{\Gamma, P, P \vdash Q}{\Gamma, P \vdash Q}\text{contr-l} \qquad \frac{}{\Gamma, \bot \vdash Q}\bot\text{-g}$$

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R} \vee\text{-g} \qquad \frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q} \vee\text{-d} \qquad \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q} \vee\text{-d}$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \Rightarrow Q \vdash R} \Rightarrow\text{-g} \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash P \Rightarrow Q} \Rightarrow\text{-d}$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, \exists x P \vdash Q}\exists\text{-g},\ c \text{ fresh} \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash \exists x P}\exists\text{-d}$$

Axioms vs. rewriting

Axioms	Rewriting
$x + S(y) = S(x + y)$ $x + 0 = x$ $x * 0 = 0$ $x * S(y) = x + x * y$ $(x * y = 0) \Leftrightarrow (x = 0 \vee y = 0)$	$x + S(y) \rightarrow S(x + y)$ $x + 0 \rightarrow x$ $x * 0 \rightarrow 0$ $x * S(y) \rightarrow x + x * y$ $(x * y = 0) \rightarrow (x = 0 \vee y = 0)$
$\dfrac{\dfrac{\vdots}{\mathcal{T} \vdash 2 * 2 = 4}}{\mathcal{T} \vdash \exists x(2 * x = 4)}$	$\dfrac{\overline{\vdash_{\mathcal{R}} 4 = 4}}{\vdash_{\mathcal{R}} \exists x(2 * x = 4)}$

Deduction Modulo: rewrite rules allowed

- Shape:

$$l \longrightarrow r$$

- we use them through an equivalence relation $\equiv_R$

Deduction Modulo: rewrite rules allowed

- Shape:

$$l \longrightarrow r$$

- Using: If $t = l_\sigma$ then we replace it by r_σ

- we use them through an equivalence relation $\equiv_R$

Deduction Modulo: rewrite rules allowed

- Shape:

$$l \longrightarrow r$$

- Using: If $t = l_\sigma$ then we replace it by r_σ
- rewrite rules on terms:

$$x + S(y) \longrightarrow S(x + y)$$

- we use them through an equivalence relation $\equiv_R$

Deduction Modulo: rewrite rules allowed

- Shape:

$$l \longrightarrow r$$

- Using: If $t = l_\sigma$ then we replace it by r_σ
- rewrite rules on terms:

$$x + S(y) \longrightarrow S(x + y)$$

- and on **propositions** :

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

- we use them through an equivalence relation $\equiv_R$

Sequent calculus modulo

$$\frac{}{\Gamma, P \vdash Q}\text{axiom } P \equiv_{\mathcal{R}} Q \qquad \frac{\Gamma, P \vdash R \quad \Gamma \vdash Q}{\Gamma \vdash R}\text{cut } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, P, Q \vdash R}{\Gamma, P \vdash R}\text{contr-g } P \equiv_{\mathcal{R}} Q \qquad \frac{}{\Gamma, P \vdash Q}\bot\text{-g } P \equiv_{\mathcal{R}} \bot$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, S \vdash R} \Rightarrow\text{-g } P \Rightarrow Q \equiv_{\mathcal{R}} S \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash S} \Rightarrow\text{-d } P \Rightarrow Q \equiv_{\mathcal{R}} S$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, R \vdash Q}\exists\text{-g}^* \; \exists x P \equiv_{\mathcal{R}} R \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash R}\exists\text{-d } \exists x P \equiv_{\mathcal{R}} R$$

An example of rewriting theory: Peano/Heyting Arithmetic

As an axiomatic theory:

$$\forall(x)\forall(y)(S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \neg(0 = S(x))$$

$$\{0/x\}P \Rightarrow \forall y(\{y/x\}P \Rightarrow \{S(y)/x\}P) \Rightarrow \forall n\{n/x\}P$$

$$\forall y(O + y = y) \qquad \forall x\forall y(S(x) + y = S(x + y))$$

$$\forall y(0 \times y = 0) \qquad \forall x\forall y(S(x) \times y = x \times y + y)$$

An example of rewriting theory: Peano/Heyting Arithmetic

As an axiomatic theory:

$$\forall(x)\forall(y)(S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \neg(0 = S(x))$$

$$\{0/x\}P \Rightarrow \forall y(\{y/x\}P \Rightarrow \{S(y)/x\}P) \Rightarrow \forall n\{n/x\}P$$

$$\forall y(O + y = y) \qquad \forall x \forall y(S(x) + y = S(x + y))$$

$$\forall y(0 \times y = 0) \qquad \forall x \forall y(S(x) \times y = x \times y + y)$$

Orienting the last four equations is not hard:

$$0 + y \longrightarrow y \qquad S(x) + y \longrightarrow S(x + y)$$

$$0 \times y \longrightarrow 0 \qquad S(x) \times y \longrightarrow x \times y + y$$

Adding symbols

We define:

- a symbol *Pred* (for predecessor) and the axioms:

$$Pred(0) = 0 \qquad Pred(S(x)) = x$$

$$\forall x \forall y (x = y \Rightarrow Pred(x) = Pred(y))$$

Adding symbols

We define:

- a symbol *Pred* (for predecessor) and the axioms:

$$Pred(0) = 0 \qquad Pred(S(x)) = x$$

$$\forall x \forall y (x = y \Rightarrow Pred(x) = Pred(y))$$

- two predicate symbols N and $Null$, and the axioms:

$$N(0) \qquad \forall x (N(x) \Rightarrow N(S(x)))$$

$$Null(0) \qquad \forall x (\neg Null(S(x)))$$

$$\{0/x\}P \Rightarrow \forall y (N(y) \Rightarrow \{y/x\}P \Rightarrow \{S(y)/x\}P) \Rightarrow \forall n (N(n) \Rightarrow \{n/x\}P)$$

Adding symbols

We define:

- a symbol *Pred* (for predecessor) and the axioms:

$$Pred(0) = 0 \qquad Pred(S(x)) = x$$

$$\forall x \forall y (x = y \Rightarrow Pred(x) = Pred(y))$$

- two predicate symbols N and *Null*, and the axioms:

$$N(0) \qquad \forall x (N(x) \Rightarrow N(S(x)))$$

$$Null(0) \qquad \forall x (\neg Null(S(x)))$$

$$\{0/x\}P \Rightarrow \forall y (N(y) \Rightarrow \{y/x\}P \Rightarrow \{S(y)/x\}P) \Rightarrow \forall n (N(n) \Rightarrow \{n/x\}P)$$

it is a conservative extension over PA/HA, up to a formulas traduction:

$$|\forall x P| = \forall x (N(x) \Rightarrow P)$$

Handling equality and induction

We still have to handle the equality symbol and the induction scheme. Introduce:

- two sorts: ι, κ (*iota* stands for integers)

Handling equality and induction

We still have to handle the equality symbol and the induction scheme. Introduce:

- two sorts: ι, κ (*iota* stands for integers)
- a symbol $\in$ of rank $\langle \iota, \kappa \rangle$

Handling equality and induction

We still have to handle the equality symbol and the induction scheme. Introduce:

- two sorts: ι, κ (*iota* stands for integers)
- a symbol $\in$ of rank $\langle \iota, \kappa \rangle$
- for each **proposition** $P[x, y_1, \ldots, y_n]$, a function symbol $f_{x,y_1,\ldots,y_n,P}$ of rank $\langle \underbrace{\iota, \ldots, \iota}_{\text{n times}}, \kappa \rangle$

Handling equality and induction

We still have to handle the equality symbol and the induction scheme. Introduce:

- two sorts: ι, κ (*iota* stands for integers)
- a symbol $\in$ of rank $\langle \iota, \kappa \rangle$
- for each **proposition** $P[x, y_1, \ldots, y_n]$, a function symbol $f_{x,y_1,\ldots,y_n,P}$ of rank $\langle \underbrace{\iota, \ldots, \iota}_{\text{n times}}, \kappa \rangle$
- Why all this ?

Arithmetic reformulated

$$\forall y \forall z (y = z \Leftrightarrow \forall p (y \in p \Rightarrow z \in p))$$
$$\forall n (N(n) \Leftrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p))$$
$$\forall x \forall y_1 \ldots \forall y_n (x \in f_{x, y_1, \ldots, y_n, P}(y_1, \ldots, y_n) \Leftrightarrow P)$$

$$Pred(0) = 0 \qquad \forall x (Pred(S(x)) = x)$$
$$Null(0) \qquad \forall x (\neg Null(S(x)))$$

$$\forall y (0 + y) = y \qquad \forall x \forall y (S(x) + y = S(x + y))$$
$$\forall y (0 \times y = 0) \qquad \forall x \forall y (S(x) \times y = x \times y + y)$$

This formulation is conservative over PA

Arithmetic modulo

$$y = z \longrightarrow \forall p (y \in p \Rightarrow z \in p)$$

$$N(n) \longrightarrow \forall p (0 \in p \Rightarrow \forall y (N(y) \Rightarrow y \in p \Rightarrow S(y) \in p) \Rightarrow n \in p)$$

$$x \in f_{x,y_1,\ldots,y_n,P}(y_1, \ldots, y_n) \longrightarrow P$$

$$Pred(0) \longrightarrow 0 \qquad Pred(S(x)) \longrightarrow x$$

$$Null(0) \longrightarrow \top \qquad Null(S(x)) \longrightarrow \bot$$

$$0 + y \longrightarrow y \qquad S(x) + y \longrightarrow S(x + y)$$

$$0 \times y \longrightarrow 0 \qquad S(x) \times y \longrightarrow x \times y + y$$

This forms a rewrite system $\mathcal{R}_{HA}$

- One can express other axiomatic theories in deduction modulo: higher-order logic, Zermelo's Set theory for instance.

- One can express other axiomatic theories in deduction modulo: higher-order logic, Zermelo's Set theory for instance.
- the problem of cut elimination in presence of rewrite rules in presence of arbitrary $\mathcal{R}$ is no more trivial:

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

can prove: $\vdash \neg B$ with a cut on A

- One can express other axiomatic theories in deduction modulo: higher-order logic, Zermelo's Set theory for instance.
- the problem of cut elimination in presence of rewrite rules in presence of arbitrary $\mathcal{R}$ is no more trivial:

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

can prove: $\vdash \neg B$ with a cut on A

- even in presence of confluence/termination of $\mathcal{R}$, this can fail:

$$R \in R \rightarrow \forall y (y \simeq R \Rightarrow \neg y \in R)$$

- One can express other axiomatic theories in deduction modulo: higher-order logic, Zermelo's Set theory for instance.
- the problem of cut elimination in presence of rewrite rules in presence of arbitrary $\mathcal{R}$ is no more trivial:

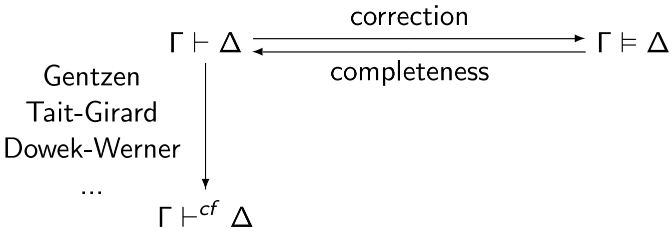
$$A \rightarrow \neg A \wedge B$$

  can prove: $\vdash \neg B$ with a cut on A
- even in presence of confluence/termination of $\mathcal{R}$, this can fail:

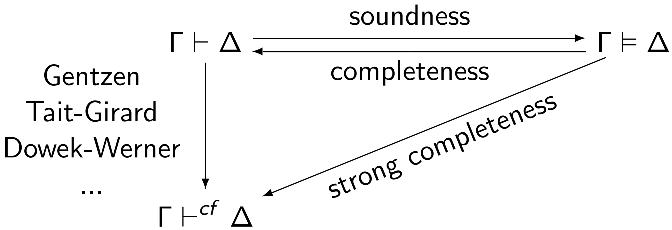
$$R \in R \rightarrow \forall y (y \simeq R \Rightarrow \neg y \in R)$$

- a cut in deduction modulo corresponds to *ad hoc* axiomatic cuts of axiomatic theories.

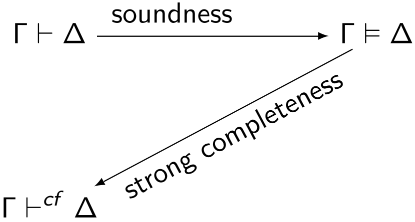
How to eliminate cut



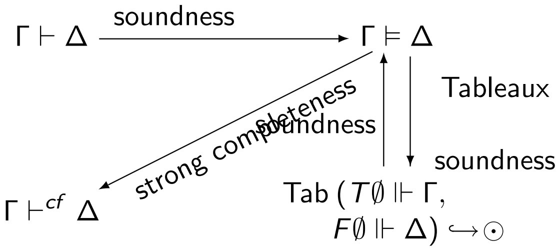
How to eliminate cut



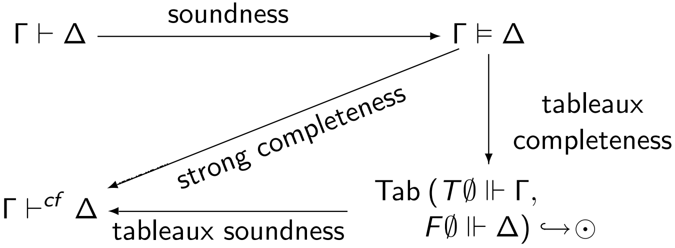
How to eliminate cut



How to eliminate cut



How to eliminate cut



- need for new definitions. In particular for models.

- need for new definitions. In particular for models.
- we construct Hintikka sets/ complete tableaux.

- need for new definitions. In particular for models.
- we construct Hintikka sets/ complete tableaux.
- we have to go further: the obtained Hintikka set has to be transformed into a model of $\mathcal{R}$ (most tedious part).

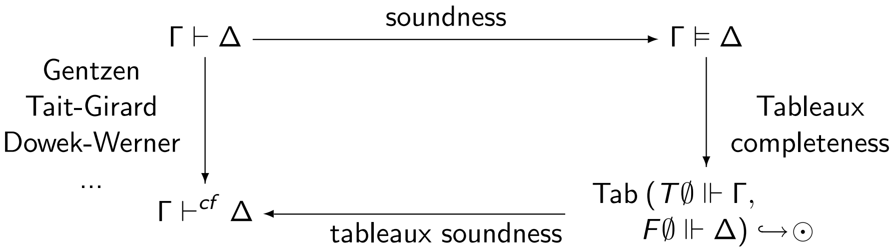
Results with the semantic method

Cut elimination for:

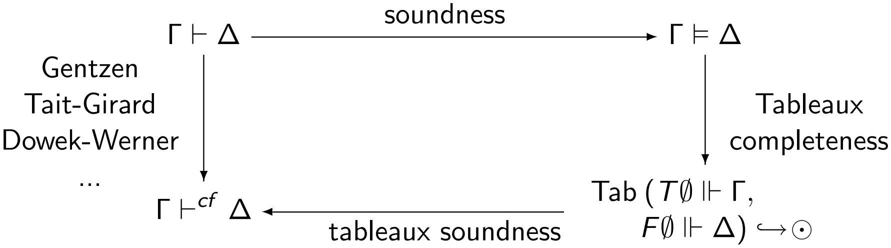
- a w.f.o. condition on $\mathcal{R}$
- a positivity condition on $\mathcal{R}$
- a mix of the two previous conditions
- HOL formulation in Deduction Modulo
- the rule:

$$R \in R \rightarrow \forall y(y \simeq R \Rightarrow (y \in R \Rightarrow (A \Rightarrow \neg A)))$$

does not have proof normalization, but has cut admissibility.



- both approach are not equivalent.



- both approach are not equivalent.
- this is still a field of investigations.