Semantic Cut Elimination in Intuitionnistic Deduction Modulo

Olivier Hermant, INRIA Futurs, Ecole Polytechnique
http ://pauillac.inria.fr/˜ohermant

Types 2004
Dec. 15-18 Jouy-en-Josas

Outline of the talk

- The deduction system
- Soundness, Completeness and Cut Elimination
- Two conditions and the proofs
- Putting the two conditions together

Deduction Rules of Sequent Calculus

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

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

$$\frac{\Gamma \vdash Q}{\Gamma, P \vdash Q}\text{weak-l} \quad \frac{\Gamma \vdash P}{\Gamma, \neg P \vdash}\neg\text{-l} \qquad \frac{\Gamma, P \vdash}{\Gamma \vdash \neg P}\neg\text{-r} \quad \frac{\Gamma \vdash}{\Gamma \vdash P}\text{weak-r}$$

$$\frac{\Gamma, P, Q \vdash R}{\Gamma, P \wedge Q \vdash R}\wedge\text{-l} \qquad \frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}\wedge\text{-r}$$

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

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

$$\frac{\Gamma, \{t/x\}P \vdash Q}{\Gamma, \forall x P \vdash Q}\forall\text{-l} \qquad \frac{\Gamma \vdash \{c/x\}P}{\Gamma \vdash \forall x P}\forall^*\text{-r}$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, \exists x P \vdash Q}\exists^*\text{-l} \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash \exists x P}\exists\text{-r}$$

Addition of rewrite rules on terms and on propositions :

$$\begin{array}{rcl} x * y = 0 & \longrightarrow & (x = 0) \vee (y = 0) \\ (x + y) + z & \longrightarrow & x + (y + z) \\ x * 0 & \longrightarrow & 0 \end{array}$$

Some Rules of Sequent Calculus Modulo

$$\frac{}{\Gamma, P \vdash_{\mathcal{R}} Q}\text{axiom},\ P \equiv Q \qquad \frac{\Gamma, P \vdash_{\mathcal{R}} R \quad \Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} \Delta}\text{cut},\ P \equiv Q$$

$$\frac{\Gamma, P, Q \vdash_{\mathcal{R}} R}{\Gamma, S \vdash_{\mathcal{R}} R} \wedge\text{-l},\ S \equiv P \wedge Q \qquad \frac{\Gamma \vdash_{\mathcal{R}} P \quad \Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} S} \wedge\text{-r},\ S \equiv P \wedge Q$$

$$\frac{\Gamma, \{t/x\}P \vdash_{\mathcal{R}} R}{\Gamma, Q \vdash_{\mathcal{R}} R}\forall\text{-l},\ Q \equiv \forall x P \qquad \frac{\Gamma \vdash_{\mathcal{R}} \{c/x\}P}{\Gamma \vdash_{\mathcal{R}} Q}\forall^{*}\text{-r},\ Q \equiv \forall x P$$

In the general case, cut elimination doesn't hold (even in confluent terminating cases) :

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

Theorem[Soundness] : If $\Gamma \vdash_{\mathcal{R}} P$ (with possible cuts) then $\Gamma \models P$.

Theorem[Completness] : If $\mathcal{T}$ is a P-cut free-consistent theory, it has a model that is not a model of P.

Corollary[Cut elimination] : If $\Gamma \vdash_{\mathcal{R}} P$ then $\Gamma \vdash_{\mathcal{R}}^{cf} P$.

Proof : if $\Gamma \vdash_{\mathcal{R}} P$, by soundness, we have $\Gamma \models P$.

By completness theorem, this means that Γ is P-cut free-inconsistent, i.e. $\Gamma \vdash_{\mathcal{R}}^{cf} P$.

Our semantic will be Kripke Structure, extended to deduction modulo with the condition :

$$\text{if } P \equiv Q \text{ then } \alpha \Vdash P \Leftrightarrow \alpha \Vdash Q$$

A Kripke Structure :

- a poset $K, \geq$
- a domain for each $\alpha \in K$, $D(\alpha)$. D is monotone wrt $\geq$
- a forcing relation $\Vdash$ defined by induction

$$\alpha \Vdash P \Rightarrow Q \text{ iff } \forall \beta \geq \alpha \beta \Vdash P \Rightarrow \beta \Vdash Q$$

We also need other definitions than the usual ones ones

A-consistency	:	$\Gamma \nvdash_{\mathcal{R}}^{cf} A$
A-completeness	:	$P \in \Gamma$ or $\Gamma, P \vdash_{\mathcal{R}}^{cf} A$
A-Henkin witnesses	:	$\Gamma, \exists x P \nvdash_{\mathcal{R}}^{cf} A \Rightarrow \{c/x\}P \in \Gamma$

Completion of an A-consistent theory $\mathcal{T}$

Put $\Gamma_0 = \mathcal{T}$, enumerate all the propositions of the language :

$$P_0, ..., P_n, ...$$

At each step, check if $\Gamma_n, P_n \nvdash^{cf}_{\mathcal{R}} A$ or not, and define Γ_{n+1} consequently. Add Henkin witness if P_n is an existential formula.

Take $\Gamma = \bigcup_{n=0}^{\infty} \Gamma_n$.

Γ is A-complete, A-consistent, admits A-Henkin witnesses. (Moreover, it is a Hintikka set).

All of this is valid under the only hypothesis of confluence of $\mathcal{R}$

First condition

We will consider a set of rewrite rules that is :

- confluent
- terminating
- compatible with a well-founded order $\succ$ having the subformula property.

E.g. the rule $P[0] \rightarrow \forall x P[x]$ is not compatible with such an order, because $\forall x\ P[x] \succ P[0]$.

We prove the completeness theorem : given a theory $\mathcal{T}$ expressed in a language $\mathcal{L}_0$, we construct a Kripke Structure and find a node $\alpha \Vdash \mathcal{T}$

Consider a denumerable family of set of new constants C_n.
Define the languages $L_0, ..., L_n$ such that $L_{n+1} = L_n \cup C_n$,

- $K = \{\Gamma\}$, Γ is an A-consistent, A-complete theory of some L_i, admitting A-Henkin witnesses
- $\geq$ is the inclusion.
- $D(\Gamma) = clos(L_n)$
- if A is a normal atom, $\Gamma \Vdash A$ iff $A \in \Gamma$.
- if A is a non-normal atom, set $\Gamma \Vdash A$ iff $\Gamma \Vdash A \downarrow$.
- define as usual the interpretation of non atomic propositions.

  Definition is well-founded, thanks to $\succ$. This is a Kripke Structure for $\mathcal{R}$, and $\Gamma \Vdash \mathcal{T}$

Second condition

We consider a positive rewrite system $\mathcal{R}$:
in a rewrite rule $A \to P$ atoms of P occurs positively

$$A \longrightarrow \forall x A$$
$$A \longrightarrow (\neg B) \Rightarrow C$$

Model construction

AS before, we define a family of languages.

- $K = \{\Gamma\}$, Γ is an A-consistent, A-complete theory of some L_i, admitting A-Henkin witnesses
- $\geq$ is the inclusion.
- $D(\Gamma) = clos(L_n)$
- at a world Γ, if $B \in \Gamma$ is atomic, we let $\Gamma \Vdash B$
- moreover, if $Gamma \vdash^{cf}_{\mathcal{R}} B$ and $\Gamma, B \vdash^{cf}_{\mathcal{R}} A$ (where Γ is A-consistent,complete), and B is atomic, we let $\Gamma \Vdash B$.
- else, $\Gamma \nvdash^{cf}_{\mathcal{R}} B$, we let $\Gamma \nVdash B$.

It is a Kripke Structure. It remains to prove that it admits rewrite rule ... the key lemma :

Lemma 1

$$\begin{array}{cc} \Gamma, P^+ \vdash^{cf}_{\mathcal{R}} A & \Gamma, Q^- \vdash^{cf}_{\mathcal{R}} A \\ \Gamma \vdash^{cf}_{\mathcal{R}} P^+ & \Gamma \vdash^{cf}_{\mathcal{R}} Q^- \end{array}$$

implies $\Gamma \Vdash P^+$ *and* $\Gamma \nVdash Q^-$.

So when $A \to P$, we are done.

Two conditions together

- R $= \mathcal{R}_> \cup \mathcal{R}_+$
- for any atomic proposition A normal $for \mathcal{R}_>$, any P st $A \equiv_{\mathcal{R}_+} P$ any instance of any atom of P is normal for $\mathcal{R}_>$.

Model Construction

We define the Kripke Structure as usual except for the forcing relation :

- if A is a normal atom for $\mathcal{R}_>$, $\Gamma \Vdash A$ iff $\Gamma \vdash^{cf}_{\mathcal{R}} A$.
- if A is a non-normal atom for $\mathcal{R}_>$, set $\Gamma \Vdash A$ iff $\Gamma \Vdash A \downarrow_>$.
- in the non-atomic case, set the forcing relation according to the Kripke Structure definition

This is a model for $\mathcal{R}_>$. We prove as in the positive case, the lemma :

Lemma 2

$$\begin{array}{cc} \Gamma, P^+ \vdash^{cf}_{\mathcal{R}} A & \Gamma, Q^- \vdash^{cf}_{\mathcal{R}} A \\ \Gamma \vdash^{cf}_{\mathcal{R}} P^+ & \Gamma \vdash^{cf}_{\mathcal{R}} Q^- \end{array}$$

implies $\Gamma \Vdash P^+$ *and* $\Gamma \not\Vdash Q^-$.

Example :

$$\begin{array}{rcl} A & \rightarrow & (\forall x B) \wedge C \text{ compatible with an order} \\ B(0) & \rightarrow & \forall x B \text{ a positive, orthogonal rewrite rule} \end{array}$$

Application : Quantifier-free rewrite systems

We consider only rules $A \to Q$ where Q doesn't contain quantifiers. We need confluence and termination of the set of rules.

The pair $< q, c >$ is a well-founded order on normal terms.

Extend it : $A \succ B$ if

- $A{\downarrow} \succ B{\downarrow}$
- $A{\downarrow} = B{\downarrow}$ and $A \to^{+} B$

Further work

- see what happen if we don't take the well-founded order (the only change is the model construction step).
- what is the link with strong normalization and pre-model construction
- extend this result to more powerful systems (HOL, CC)

Short bibliography

- R. Cori, D. Lascar, Logique Mathématique, 1993
- G. Dowek, Th. Hardin, Cl. Kirchner, Theorem Proving Modulo, 1998
- G. Dowek, B. Werner, Proof normalization modulo, 1998
- R. Smullyan, First Order Logic, 1968
- J. Stuber, A model-based completness proof of Extended Narrowing and Resolution, 2001

$$\frac{}{\Gamma, P \vdash_{\mathcal{R}} Q}\text{axiom if } P \equiv Q \qquad \frac{\Gamma, P \vdash_{\mathcal{R}} Q \quad \Gamma \vdash_{\mathcal{R}} R}{\Gamma \vdash_{\mathcal{R}} Q}\text{cut if } P \equiv R$$

$$\frac{\Gamma, P, R \vdash_{\mathcal{R}} Q}{\Gamma, P \vdash_{\mathcal{R}} Q}\text{contr-l if } P \equiv R \qquad \frac{}{\Gamma, P \vdash_{\mathcal{R}} Q}\bot\text{-l if } P \equiv \bot$$

$$\frac{\Gamma \vdash_{\mathcal{R}} Q}{\Gamma, P \vdash_{\mathcal{R}} Q}\text{weak-l} \qquad \frac{\Gamma \vdash_{\mathcal{R}}}{\Gamma \vdash_{\mathcal{R}} P}\text{weak-r}$$

$$\frac{\Gamma, P, Q \vdash_{\mathcal{R}} R}{\Gamma, S \vdash_{\mathcal{R}} R}\wedge\text{-l if } P \wedge Q \equiv S \qquad \frac{\Gamma \vdash_{\mathcal{R}} P \quad \Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} R}\wedge\text{-r if } P \wedge Q \equiv R$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} R \quad \Gamma, Q \vdash_{\mathcal{R}} R}{\Gamma, S \vdash_{\mathcal{R}} R}\vee\text{-l if } P \vee Q \equiv S \qquad \frac{\Gamma \vdash_{\mathcal{R}} P}{\Gamma \vdash_{\mathcal{R}} S}\vee\text{-r if } P \vee Q \equiv R \qquad \frac{\Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} R}\vee\text{-r if } P \vee Q \equiv R$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P \quad \Gamma, Q \vdash_{\mathcal{R}} R}{\Gamma, S \vdash_{\mathcal{R}} R}\Rightarrow\text{-l if } P \Rightarrow Q \equiv S \qquad \frac{\Gamma, P \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} S}\Rightarrow\text{-r if } P \Rightarrow Q \equiv S$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P}{\Gamma, Q \vdash_{\mathcal{R}}}\neg\text{-l if } \neg P \equiv Q \qquad \frac{\Gamma, P \vdash_{\mathcal{R}}}{\Gamma \vdash_{\mathcal{R}} Q}\neg\text{-r if } \neg P \equiv Q$$

$$\frac{\Gamma, \{t/x\}P \vdash_{\mathcal{R}} Q}{\Gamma, R \vdash_{\mathcal{R}} Q}\forall\text{-l if } \forall x P \equiv R \qquad \frac{\Gamma \vdash_{\mathcal{R}} \{c/x\}P}{\Gamma \vdash_{\mathcal{R}} Q}\forall\text{-r, if } \forall x P \equiv Q c \text{ fresh constant}$$

$$\frac{\Gamma, \{c/x\}P \vdash_{\mathcal{R}} Q}{\Gamma, R \vdash_{\mathcal{R}} Q}\exists\text{-l, if } \exists x P \equiv R c \text{ fresh constant} \qquad \frac{\Gamma \vdash_{\mathcal{R}} \{t/x\}P}{\Gamma \vdash_{\mathcal{R}} Q}\exists\text{-r if } \exists x P \equiv Q$$

Fig. 1 – Deduction rule of intuitionnistic sequent calculus modulo

A model $\mathcal{M}$ is a model of the rewrite rules iff :

$$P =_{\mathcal{R}} Q \Rightarrow |P|_{\mathcal{M}} = |Q|_{\mathcal{M}}$$

In the later, we will consider only such models.