A Model-based cut-elimination proof in Deduction Modulo

Marktoberdorf

Olivier Hermant, INRIA, Paris
http ://pauillac.inria.fr/~hermant

Outline of the talk

- The deduction system
- Soundness and Completness
- Sketch of the the proof

Sequent Calculus modulo

With $\mathcal{P}$ Peano's Axioms, prove that $2+2=4$:

$$\cfrac{\cfrac{\cfrac{\cfrac{\text{Reflexivity}}{\mathcal{P} \vdash S(S(S(S(0)))) = S(S(S(S(0))))}}{\vdots}}{\mathcal{P} \vdash S(S(S(0))) + S(0) = S(S(S(S(0))))}}{\cfrac{\vdots}{\mathcal{P} \vdash S(S(0) + S(S(0) = S(S(S(S(0))))}}$$

Replacing axiom with rewrite rule
$x + S(y) \rightarrow S(x) + y$:

$$\cfrac{\text{Reflexivity}}{\vdash_{\mathcal{R}} S(S(0)) + S(S(0)) = S(S(S(S(0))))}$$

Adding rewrite rules :

- separates the computational content
- enhances performances of theorem provers
- adds power to theories
- allows to suppress some axioms

$$\begin{aligned} x * y = 0 &\quad\rightarrow\quad (x = 0) \vee (y = 0) \\ (x + y) + z &\quad\rightarrow\quad x + (y + z) \\ x * 0 &\quad\rightarrow\quad 0 \end{aligned}$$

We rewrite terms or atomic propositions.

Definitions

A set of rewrite rules is confluent iff :

$$\begin{array}{c} P \rightarrow^* P' \\ P \rightarrow^* P'' \end{array} \Rightarrow \begin{array}{c} P' \rightarrow^* Q \\ P'' \rightarrow^* Q \end{array}$$

A set of rewrite rule is terminating (or normalizing) iff each reduction sequence is finite.

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 latter, we will consider only such models.

Problem : in the general case, cut elimination (and even consistency) doesn't hold :

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

But for this case, holds :

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

We have to find a condition. Confluence and termination is not sufficient :

$$R \in R \longrightarrow \forall y ((\forall x (\neg x \in R \Rightarrow \neg x \in y)) \Rightarrow \neg R \in y)$$

Deduction rules

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

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

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

Some Rules of Sequent Calculus

Given $\mathcal{R}$ a set of rewrite rules, we add two rules to Sequent Calculus :

$$\frac{\Gamma, P \vdash_{\mathcal{R}} \Delta}{\Gamma, Q \vdash_{\mathcal{R}} \Delta}\text{rewrite-l if } P =_{\mathcal{R}} Q$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P, \Delta}{\Gamma \vdash_{\mathcal{R}} Q, \Delta}\text{rewrite-r if } P =_{\mathcal{R}} Q$$

$=_{\mathcal{R}}$ is the reflexive-transitive-symmetric closure of $\rightarrow$.

Hypotheses

We will consider a set of rewrite rules that is :

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

Following Smullyan, we define the subformula as follow :

- $A[t/x]$ is an immediate subformula of $\forall x\ A$, A is an immediate subformula of $A \wedge B$, ...
- Subformula is the transitive closure of the immediate subformula relation.

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

Soundness, Completness, Cut Elimination

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

Theorem[Completness] : If $\mathcal{T}$ is a cut free-consistent theory, it has a model.

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

Proof : if $\Gamma \vdash \Delta$, by soundness, we have $\Gamma \models \Delta$, hence $\Gamma, \neg\Delta$ doesn't have a model.

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

Completness

Lemma[Kleene] : Let $A =_{\mathcal{R}} \neg P$ be propositions. Id we have :

$$\Gamma, A \vdash^{cf}_{\mathcal{R}} \Delta$$

then we can construct a proof :

$$\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$$

Lemma : A is a normal atom. If

$$\Gamma, A \vdash^{cf}_{\mathcal{R}} \Delta$$
$$\Gamma \vdash^{cf}_{\mathcal{R}} A, \Delta$$

we can construct a proof of :

$$\Gamma \vdash_{\mathcal{R}} \Delta$$

Proof : by induction on the structure of the proof.

Completion of a consistent theory $\mathcal{T}$

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

$$A_0, ..., A_n, ...$$

At each step, check if $\Gamma_n, A_n \not\vdash^{cf}_{\mathcal{R}}$ or not, and define Γ_{n+1}.

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

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

Constructing a Herbrand model

We follow Bachmair and Gantzingers' contruction.

- For each proposition we construct its formation tree.
- Each branch is finite thanks to the order.
- Set for each normal atom $|A|_{\mathcal{M}} = True$ iff $A \in \Gamma$.
- With the tree, we are able to define a truth value for each proposition.

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