A Model-based cut-elimination proof

2nd Days of Logic And Computability

Olivier Hermant, INRIA, Paris
http://pauillac.inria.fr/~hermant
Outline of the talk

- The deduction system
- Soundness and Completeness
- Sketch of the the proof
Sequent Calculus modulo

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

\[
\begin{align*}
\text{Reflexivity} \\
\mathcal{P} &\vdash S(S(S(0))) = S(S(S(0))) \\
\vdots \\
\mathcal{P} &\vdash S(S(0)) + S(0) = S(S(S(0))) \\
\vdots \\
\mathcal{P} &\vdash S(0) + S(0) = S(S(S(0)))
\end{align*}
\]

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

\[
\begin{align*}
\text{Reflexivity} \\
\vdash_{\mathcal{R}} S(S(0)) + S(S(0)) = S(S(S(S(0))))
\end{align*}
\]
Adding rewrite rules:

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

\[
x \times y = 0 \quad \rightarrow \quad (x = 0) \lor (y = 0)
\]
\[
(x + y) + z \quad \rightarrow \quad x + (y + z)
\]
\[
x \times 0 \quad \rightarrow \quad 0
\]

We rewrite terms or atomic propositions.
Problem: in the general case, cut elimination (and even consistency) doesn’t hold:

\[ A \rightarrow B \land \neg A \]

But for this case, holds:

\[ A \rightarrow B \land A \]

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

\[ R \in R \rightarrow \forall y((\forall x(\neg x \in R \Rightarrow \neg x \in y)) \Rightarrow \neg R \in y) \]
Deduction rules

\[
\begin{align*}
\Gamma, P & \vdash P, \Delta & \text{axiom} \\
\Gamma, P, Q & \vdash \Delta & \text{-1} \\
\Gamma, \forall x P & \vdash \Delta & \text{-1}
\end{align*}
\]

\[
\begin{align*}
\Gamma, P & \vdash \Delta & \Gamma \vdash P, \Delta & \text{cut} \\
\Gamma & \vdash P, \Delta & \Gamma & \vdash Q, \Delta & \text{-r} \\
\Gamma & \vdash \{c/x\} P, \Delta & \Gamma & \vdash \forall x P, \Delta & \text{-r}
\end{align*}
\]

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

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

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

$=_{\mathcal{R}}$ is the reflexive-transitive-symmetric closure of $\rightarrow$. 
Soundness, Completeness, Cut Elimination

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

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

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

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

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

Lemma [Kleene]: Let $A =_R \neg P$ be propositions. If we have:

$$\Gamma, A \vdash^c_R \Delta$$

then we can construct a proof:

$$\Gamma \vdash^c_R P, \Delta$$

Lemma: $A$ is a normal atom. If

$$\Gamma, A \vdash^c_R \Delta$$

$$\Gamma \vdash^c_R A, \Delta$$

we can construct a proof of:

$$\Gamma \vdash_R \Delta$$

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 the language:

$$A_0, \ldots, A_n, \ldots$$

At each step, check if $\Gamma_n, A_n \not\vdash \mathcal{L}$ or not, and define $\Gamma_{n+1}$.

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

$\Gamma$ is complete, consistent, admits Henkin witnesses. (Moreover, it is a Hintikka set).
Constructing a Herbrand model

We follow Bachmair and Gantzingers’ construction.

- For each proposition we construct its formation tree.
- Each branch is finite thanks to the order.
- Set for each normal atom $|A|_M = True$ 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 $A \rightarrow Q$ 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: $A \triangleright B$ if

- $A \downarrow \triangleright B \downarrow$
- $A \downarrow = B \downarrow$ and $A \rightarrow^+ B$
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 completeness proof of Extended Narrowing and Resolution, 2001