Transforming and Analyzing Proofs in the \textit{CERES}-system

S. Hetzl  A. Leitsch  D. Weller  B. Woltzenlogel Paleo

KEAPPA, 22 November 2008
Outline

System Overview

The CERES System
  Writing Proofs
  Transforming proofs
  System demonstration

Future Work
Purpose

- Proof transformations
- In particular: cut-elimination by resolution
- Goal: obtain new (analytic) proofs from known ones
Overview

S. Hetzl, A. Leitsch, D. Weller, B. Woltzenlogel Paleo

Proofs in the CERES-system
Proof calculus: sequent calculus \textbf{LK}

Example

Rules for $\land$:

\[
\frac{\Gamma \vdash \Delta, A \quad \Pi \vdash \Lambda, B}{\Gamma, \Pi \vdash \Delta, \Lambda, A \land B} \quad \land : r
\]

\[
\frac{A, \Gamma \vdash \Delta}{A \land B, \Gamma \vdash \Delta} \quad \land : l1
\]

\[
\frac{A, \Gamma \vdash \Delta}{B \land A, \Gamma \vdash \Delta} \quad \land : l2
\]
LKDe

- Additional rules for easier proof formalization
LKDe

- Additional rules for easier proof formalization
- Definition introduction

\[
\frac{A(t_1, \ldots, t_k) \vdash \Delta}{P(t_1, \ldots, t_k) \vdash \Delta} \underset{\text{def}_P}{\implies} I
\]
LKDe

- Additional rules for easier proof formalization
- Definition introduction
- Equality handling

\[
\frac{\Gamma_1 \vdash \Delta_1, s = t \quad A[s], \Gamma_2 \vdash \Delta_2}{A[t], \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} = : \text{/1}
\]
Writing LKDe proofs

- Specialized language: *HandyLK*
- Why not Isabelle, Coq, etc.?
  - Higher-order logic vs. first-order method
  - Proof assistants focus on existence of proof, not proof object itself
The *HandyLK* language

- Between natural language and sequent calculus
  - closer to sequent calculus
- Supports many-sorted first-order language
HandyLK example - predicate definitions

- define predicate $I$ by $\forall x \exists k \ f(n + k) = x$;
- $\forall x \ (I(x) \leftrightarrow \forall n \exists k \ f(n + k) = x)$
HandyLK example - predicate definitions

- define predicate \( I \) by all \( n \) ex \( k \) \( f(n + k) = x \);
- \( \forall x (I(x) \leftrightarrow \forall n \exists k f(n + k) = x) \)
- with undef \( I \)
  \[ :- \text{ all } n \text{ ex } k f(n + k) = 0; \]
- \[
\frac{\Gamma \vdash \Delta, \forall n \exists k f(n + k) = 0}{\Gamma \vdash \Delta, I(0)} \quad \text{def}_I: \text{r}
\]
HandyLK features

- Prove propositional tautologies automatically
- Define proofs recursively
- Define proofs with parameters that can be instantiated
Proof transformations do not work directly on HandyLK proofs

- Compiled by HLK to LKDe in XML
- proofdatabase.dtd allows storage of proofs as DAGs
- Formulas, terms stored as trees
The CERES method

- Clause set $\text{CL}(\pi)$ is extracted from $\text{LKDe}$-proof $\pi$
- $\text{CL}(\pi)$ is refuted by a resolution theorem prover
- Resolution refutation is converted to an $\text{LK}$ refutation $\gamma$
- $\gamma$ is composed with material from $\pi$: $\text{LKDe}$-proof $\psi$
- $\psi$ contains at most atomic cuts
Background: Tape with infinitely many cells where each cell is labelled 0 or 1.

**Theorem**

*There are two distinct cells that are labelled the same.*

**Lemma**

*Either infinitely many cells are labelled 0, or infinitely many cells are labelled 1.*
System demonstration
Simplified Herbrand Sequent

\[
\begin{align*}
\text{f}(p_1) &= 0 \lor \text{f}(p_1) = 1, \\
\text{f}(p_2) &= 0 \lor \text{f}(p_2) = 1, \\
\text{f}(p_3) &= 0 \lor \text{f}(p_3) = 1, \\
\text{f}(p_4) &= 0 \lor \text{f}(p_4) = 1, \\
\text{f}(p_5) &= 0 \lor \text{f}(p_5) = 1, \\
\text{f}(p_6) &= 0 \lor \text{f}(p_6) = 1, \\
\text{f}(p_7) &= 0 \lor \text{f}(p_7) = 1
\end{align*}
\]

\[
\vdash p_1 \neq p_2 \land f(p_1) = f(p_2), \\
p_3 \neq p_1 \land f(p_3) = f(p_1), \\
p_3 \neq p_2 \land f(p_3) = f(p_2), \\
p_1 \neq p_4 \land f(p_1) = f(p_4), \\
p_5 \neq p_6 \land f(p_5) = f(p_6), \\
p_7 \neq p_5 \land f(p_7) = f(p_5), \\
p_7 \neq p_6 \land f(p_7) = f(p_6), \\
p_4 \neq p_7 \land f(p_4) = f(p_7).
\]

where the \(p_i\) are distinct positions on the tape.
Even More Simplified Herbrand Sequent

\[ f(p_1) = 0 \lor f(p_1) = 1, f(p_2) = 0 \lor f(p_2) = 1, f(p_3) = 0 \lor f(p_3) = 1, \]
\[ \vdash p_1 \neq p_2 \land f(p_1) = f(p_2), \]
\[ p_3 \neq p_1 \land f(p_3) = f(p_1), \]
\[ p_3 \neq p_2 \land f(p_3) = f(p_2). \]

where the \( p_i \) are distinct positions on the tape.
Future Work

- Extend CERES method to fragments of higher-order logic
- Enhance HLK by term-rewriting features to handle equational aspects of proofs
- Long term: Use existing proof assistants
- Simplify Herbrand sequent automatically