

# Proof Transformation by CERES

Matthias Baaz, Stefan Hetzl, Alexander Leitsch,  
Clemens Richter, Hendrik Spohr  
Vienna University of Technology

*August 11, 2006*

*Mathematical Knowledge Management 2006*

## Motivation

- Cut-elimination theorem (Gentzen, 1934):  
Cut-rule can be eliminated from proofs in the sequent calculus **LK**  
⇒ Subformula property  
Math.: Eliminate lemmas from the proof of a theorem  
⇒ Only concepts appearing in the theorem appear in the proof
- Implementing cut-elimination: Computer-aided proof analysis
  - Automated generation of elementary proofs
  - Extraction of bounds
- Gentzen's method not designed for applications
- CERES - Cut-Elimination by RESolution  
on extended sequent calculus **LKDe**

## Overview

- Extending Gentzen's **LK**: The calculus **LKDe**
- The CERES method on **LKDe**
- Implementation: System demonstration

## Extending LK (1/2) - Adding Equality

Equality axioms (reflexivity):

$$\vdash t = t \text{ for all terms } t$$

Equality rules:

$$\frac{\Gamma_1 \vdash \Delta_1, s = t \quad A[s]_{\Lambda}, \Gamma_2 \vdash \Delta_2}{A[t]_{\Lambda}, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} =: l1$$

$$\frac{\Gamma_1 \vdash \Delta_1, t = s \quad A[s]_{\Lambda}, \Gamma_2 \vdash \Delta_2}{A[t]_{\Lambda}, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} =: l2$$

$$\frac{\Gamma_1 \vdash \Delta_1, s = t \quad \Gamma_2 \vdash \Delta_2, A[s]_{\Lambda}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A[t]_{\Lambda}} =: r1$$

$$\frac{\Gamma_1 \vdash \Delta_1, t = s \quad \Gamma_2 \vdash \Delta_2, A[s]_{\Lambda}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A[t]_{\Lambda}} =: r2$$

$\Lambda$  ... set of replacement positions

## Extending LK (2/2) - Adding Definitions

Atom definition:  $D(x_1, \dots, x_k) := F[x_1, \dots, x_k]$

Function definition:  $f(x_1, \dots, x_k) := t[x_1, \dots, x_k]$

$$\frac{F[t_1, \dots, t_k], \Gamma \vdash \Delta}{D(t_1, \dots, t_k), \Gamma \vdash \Delta} \text{def}_D : l \qquad \frac{\Gamma \vdash \Delta, F[t_1, \dots, t_k]}{\Gamma \vdash \Delta, D(t_1, \dots, t_k)} \text{def}_D : r$$

$$\frac{P(\dots t[t_1, \dots, t_k] \dots), \Gamma \vdash \Delta}{P(\dots f(t_1, \dots, t_k) \dots), \Gamma \vdash \Delta} \text{def}_f : l \qquad \frac{\Gamma \vdash \Delta, P(\dots t[t_1, \dots, t_k] \dots)}{\Gamma \vdash \Delta, P(\dots f(t_1, \dots, t_k) \dots)} \text{def}_f : r$$

Examples:

$$D(m, n) := (\exists r)m \cdot r = n$$

$$\text{PRIME}(n) := (\forall m)(D(m, n) \rightarrow (m = 1 \vee m = n))$$

## The CERES method (1/2)

Input: **LKDe**-proof  $\varphi$  of  $\Gamma \vdash \Delta$ , preprocessing: Skolemization  
 $\Omega \dots$  ancestors of cut-formulas

1. Construct the characteristic clause set  $CL(\varphi)$

(a)  $\nu$  occurrence of axiom sequent  $S(\nu)$ :  $\mathcal{C}_\nu := \{S(\nu) \setminus \Omega\}$

(b)  $\nu$  unary rule:  $\mathcal{C}_\nu := \mathcal{C}_{\nu'}$

(c)  $\nu$  binary rule, aux. formulas in  $\Omega$ :  $\mathcal{C}_\nu := \mathcal{C}_{\nu_1} \cup \mathcal{C}_{\nu_2}$

(d)  $\nu$  binary rule, aux. formulas not in  $\Omega$ :  $\mathcal{C}_\nu := \mathcal{C}_{\nu_1} \times \mathcal{C}_{\nu_2}$

where  $\mathcal{C} \times \mathcal{D} = \{C \circ D \mid C \in \mathcal{C}, D \in \mathcal{D}\}$

and  $\Sigma \vdash \Theta \circ \Pi \vdash \Lambda = \Sigma, \Pi \vdash \Theta, \Lambda$

$CL(\varphi)$  is unsatisfiable

## The CERES method (2/2)

2. Compute the projections  $\psi_1, \dots, \psi_n$  to  $\{C_1, \dots, C_n\} = \text{CL}(\varphi)$   
“delete rules working on ancestors of cut-formulas”

$$\psi_i : \Gamma \vdash \Delta \circ C_i$$

3. Use automated theorem prover: Resolution refutation  $\gamma$  of  $\text{CL}(\varphi)$

A ground resolution refutation is an **LKDe**-proof:

resolution  $\rightarrow$  atomic cut

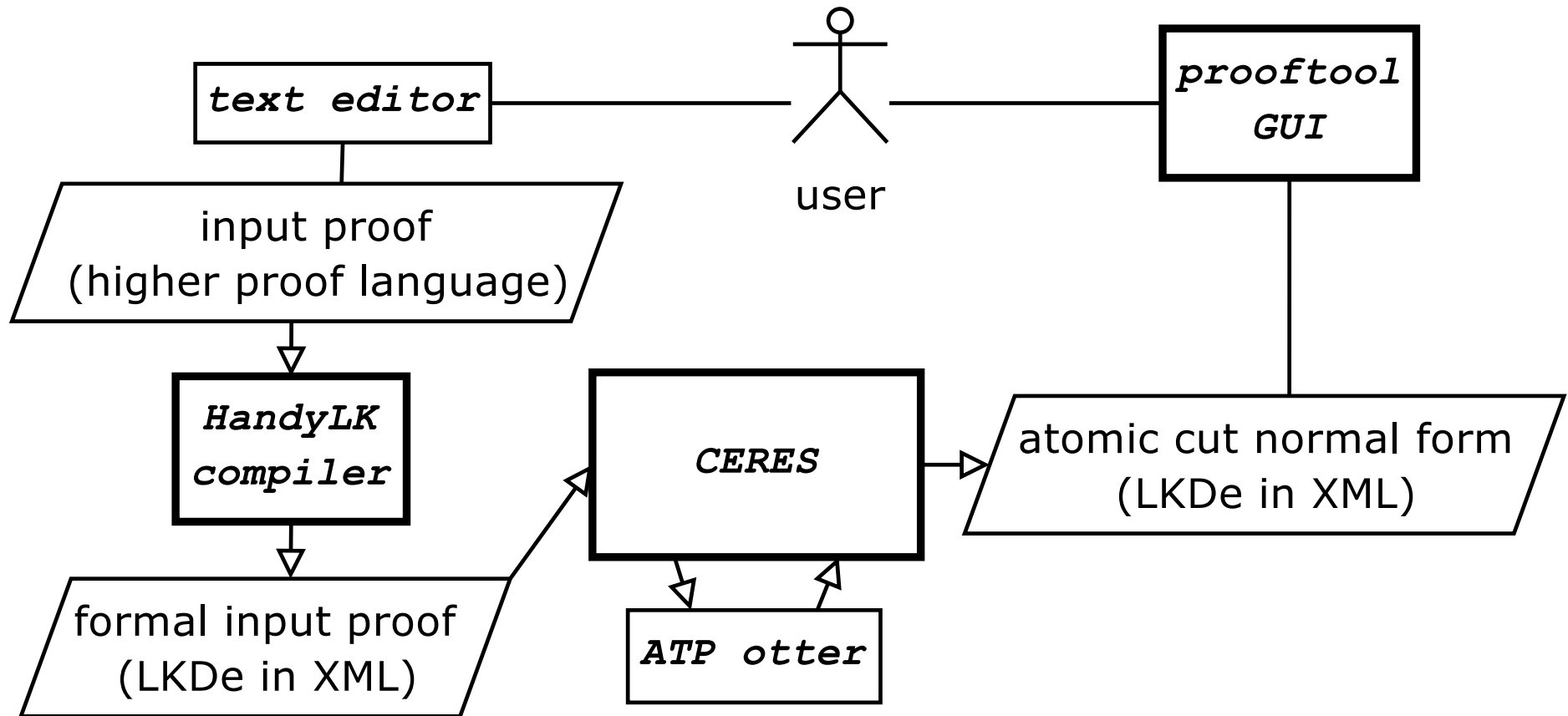
paramodulation  $\rightarrow$  equality rules

initial sequents: instances of  $C_i$

4. Plug-in  $\psi_i$  at leaves of  $\gamma$  to obtain a proof of  $\Gamma, \dots, \Gamma \vdash \Delta, \dots, \Delta$

Output: A proof of  $\Gamma \vdash \Delta$  with only atomic cuts

## The Implementation - Software Architecture



## Example - tape proof

Infinite tape, each cell containing either 0 or 1

$$A = (\forall x)(f(x) = 0 \vee f(x) = 1) \quad (\text{Assumption})$$

$$P = (\exists p)(\exists q)(p \neq q \wedge f(p) = f(q)) \quad (\text{Proposition})$$

From  $A$  we prove  $P$ : There are two different cells with the same value

$$I_0 = (\forall n)(\exists k)f(n+k) = 0 \quad (\text{Infinity 0})$$

$$I_1 = (\forall n)(\exists k)f(n+k) = 1 \quad (\text{Infinity 1})$$

$$\frac{\frac{\frac{(\tau)}{A \vdash I_0, I_1} \quad (\epsilon_0)}{A \vdash P, I_1} \quad cut \quad I_1 \vdash P}{A \vdash P} \quad cut}{A \vdash P} \quad cut$$

## Conclusion

- Gentzen's result: eliminating cuts is possible *in principle*
- CERES on **LKDe** makes this procedure *practically feasible* for realistic mathematical proofs
- Ex.: Eliminating topology from proof of number-theoretic statement

details of the method:

M. Baaz, A. Leitsch: *Cut-elimination and Redundancy-elimination by Resolution*, Journal of Symbolic Computation, 29, pp. 149–176, 2000

to try out / download CERES:  
<http://www.logic.at/ceres/>