

Fast Cut-Elimination by CERES

A. Leitsch
TU-Vienna
joint work with M. Baaz

Aim

- ▶ Identify subclasses of **LK**-proofs where **cut-elimination is fast** (i.e. elementary).
- ▶ Find out which kind of cut-derivations are **essential** (in compressing proofs).

Aim

- ▶ Identify subclasses of **LK**-proofs where **cut-elimination is fast** (i.e. elementary).
- ▶ Find out which kind of cut-derivations are **essential** (in compressing proofs).
- ▶ to this aim use CERES.

Cut-Elimination

Cut: Rule for using lemmas in a proof.

Cut-Elimination:

- ▶ Elimination of lemmas from proofs.
- ▶ Transformation to elementary proofs.
- ▶ Obtain proofs with sub-formula property.

Cut-Elimination

Cut: Rule for using lemmas in a proof.

Cut-Elimination:

- ▶ Elimination of lemmas from proofs.
- ▶ Transformation to elementary proofs.
- ▶ Obtain proofs with sub-formula property.

Example:

proofs of theorems in number theory may use *topological structures*. Cut-elimination yields proofs without topology.

other applications:

- ▶ extraction of bounds via Herbrand's theorem
- ▶ extraction of programs from proofs

Gentzen's Hauptsatz:

For every (LK-) proof of a formula A there exists a proof of A without cuts (which can be constructed effectively).

Sequent Calculus

Sequent: $\mathcal{A} \vdash \mathcal{B}$, for finite multi-sets of formulas \mathcal{A}, \mathcal{B} .

$A_1, \dots, A_n \vdash B_1, \dots, B_m$ represents

$\bigwedge A_i \rightarrow \bigvee B_j$.

\vdash : separation-symbol.

LK: calculus on sequents, based on **logical** and **structural** rules.

axioms: $A \vdash A$ for atoms A .

I. The logical rules:

\wedge -introduction:

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \wedge : l1 \qquad \frac{B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \wedge : l2$$
$$\frac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B} \wedge : r$$

\vee -introduction:

$$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta} \vee : l$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \vee : r1 \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B} \vee : r2$$

\rightarrow -introduction:

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \rightarrow B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \rightarrow : l$$
$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \rightarrow B} \rightarrow : r$$

\neg -introduction:

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta} \neg : l$$

$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \neg : r$$

\forall -introduction (eigenvariable cond. for $\forall : r$):

$$\frac{A(x/t), \Gamma \vdash \Delta}{(\forall x)A(x), \Gamma \vdash \Delta} \forall : l$$

$$\frac{\Gamma \vdash \Delta, A(x/y)}{\Gamma \vdash \Delta, (\forall x)A(x)} \forall : r$$

\exists -introduction (the eigenvariable conditions for $\exists : l$ are these for $\forall : r$):

$$\frac{A(x/y), \Gamma \vdash \Delta}{(\exists x)A(x), \Gamma \vdash \Delta} \exists : l$$

$$\frac{\Gamma \vdash \Delta, A(x/t)}{\Gamma \vdash \Delta, (\exists x)A(x)} \exists : r$$

II. The structural rules:

weakening:

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \quad w : r$$

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \quad w : l$$

contraction:

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \quad c : l$$

$$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A} \quad c : r$$

cut:

$$\frac{\Gamma \vdash \Delta, A \quad A, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda} \quad cut(A)$$

Let A be a formula s.t. A occurs in Δ and in Π . Then the *mix* is defined as:

$$\frac{\Gamma \vdash \Delta \quad \Pi \vdash \Lambda}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda} \quad mix(A)$$

where $\Pi^* = \Pi$ after elimination of A , similar for Δ .

LK-proof without cut:

$$\begin{array}{c}
 \frac{P(y) \vdash P(y)}{P(y) \vdash P(b), P(y)} \text{w : r} \\
 \frac{P(y) \vdash P(b), P(y)}{P(y), \neg P(y) \vdash P(b)} \neg : l \quad \frac{P(b) \vdash P(b)}{P(y), P(b) \vdash P(b)} \text{w : l} \\
 \frac{P(y), \neg P(y) \vdash P(b)}{P(y), \neg P(y) \vee P(b) \vdash P(b)} \vee : l \\
 \frac{P(y), (\forall x)(\neg P(x) \vee P(b)) \vdash P(b)}{(\exists x)P(x), (\forall x)(\neg P(x) \vee P(b)) \vdash P(b)} \forall : l \\
 \frac{(\exists x)P(x), (\forall x)(\neg P(x) \vee P(b)) \vdash P(b)}{(\forall x)(\neg P(x) \vee P(b)) \vdash (\exists x)P(x) \rightarrow P(b)} \exists : l \\
 \frac{(\forall x)(\neg P(x) \vee P(b)) \vdash (\exists x)P(x) \rightarrow P(b)}{\vdash (\forall x)(\neg P(x) \vee P(b)) \rightarrow ((\exists x)P(x) \rightarrow P(b))} \rightarrow : r
 \end{array}$$

LK-proof with cut:

$$\frac{\frac{(\varphi_1)}{(\forall x)(\neg P(x) \vee P(b)) \vdash A} \quad \frac{(\varphi_2)}{A \vdash (\exists x)P(x) \rightarrow P(b)}}{(\forall x)(\neg P(x) \vee P(b)) \vdash (\exists x)P(x) \rightarrow P(b)} \text{ cut}}{\vdash (\forall x)(\neg P(x) \vee P(b)) \rightarrow ((\exists x)P(x) \rightarrow P(b))} \rightarrow: r$$

for $A = (\forall x)\neg P(x) \vee P(b)$ and

$\varphi_2 =$

$$\frac{\frac{\frac{P(y) \vdash P(y)}{P(y) \vdash P(b), P(y)} w : r}{P(y), \neg P(y) \vdash P(b)} \neg : l}{P(y), (\forall x)\neg P(x) \vdash P(b)} \forall : l \quad \frac{P(b) \vdash P(b)}{P(y), P(b) \vdash P(b)} w : l}{\frac{P(y), (\forall x)\neg P(x) \vee P(b) \vdash P(b)}{(\exists x)P(x), (\forall x)\neg P(x) \vee P(b) \vdash P(b)} \exists : l} \forall : l} {\frac{(\forall x)\neg P(x) \vee P(b) \vdash (\exists x)P(x) \rightarrow P(b)}{(\forall x)\neg P(x) \vee P(b) \vdash (\exists x)P(x) \rightarrow P(b)} \rightarrow: r}$$

Gentzen's method of cut-elimination:

- ▶ reduction of *rank* and *grade*.
- ▶ “peeling” the cut-formulas from outside.
- ▶ elimination of an uppermost cut.

The method can be described as a

normal form computation

based on a set of rules \mathcal{R} .

Gentzen's method of cut-elimination:

- ▶ reduction of *rank* and *grade*.
- ▶ “peeling” the cut-formulas from outside.
- ▶ elimination of an uppermost cut.

The method can be described as a

normal form computation

based on a set of rules \mathcal{R} .

Computational features:

- ▶ very slow.
- ▶ weak in detecting redundancy.

Example of a Gentzen reduction:

$$\frac{\frac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)} \forall: l \quad \frac{P(b) \vdash P(b)}{(\forall x)P(x) \vdash P(b)} \forall: l}{(\forall x)P(x) \vdash P(a) \wedge P(b)} \wedge: r \quad \frac{P(a) \vdash P(a)}{P(a) \wedge P(b) \vdash P(a)} \wedge: l}{P(a) \wedge P(b) \vdash (\exists x)P(x)} \exists: r}{(\forall x)P(x) \vdash (\exists x)P(x)} \text{cut}$$

rank = 3, grade = 1.

reduce to rank = 2, grade = 1:

$$\frac{\frac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)} \forall: l \quad \frac{P(b) \vdash P(b)}{(\forall x)P(x) \vdash P(b)} \forall: l}{(\forall x)P(x) \vdash P(a) \wedge P(b)} \wedge: r \quad \frac{P(a) \vdash P(a)}{P(a) \wedge P(b) \vdash P(a)} \wedge: l}{(\forall x)P(x) \vdash P(a)} \text{cut}}{(\forall x)P(x) \vdash (\exists x)P(x)} \exists: r$$

$$\frac{\frac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)} \forall: l \quad \frac{P(b) \vdash P(b)}{(\forall x)P(x) \vdash P(b)} \forall: l}{(\forall x)P(x) \vdash P(a) \wedge P(b)} \wedge: r \quad \frac{P(a) \vdash P(a)}{P(a) \wedge P(b) \vdash P(a)} \wedge: l}{\frac{(\forall x)P(x) \vdash P(a)}{(\forall x)P(x) \vdash (\exists x)P(x)} \exists: r} \text{cut}$$

rank = 2, grade = 1. Reduce to grade = 0, rank = 3:

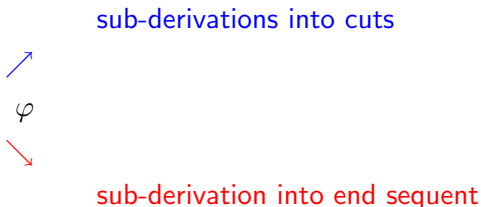
$$\frac{\frac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)} \forall: l \quad P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)} \text{cut}}{\frac{(\forall x)P(x) \vdash P(a)}{(\forall x)P(x) \vdash (\exists x)P(x)} \exists: r}$$

eliminate cut with axiom:

$$\frac{\frac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)} \forall: l}{(\forall x)P(x) \vdash (\exists x)P(x)} \exists: r$$

Cut-elimination by Resolution (CERES)

based on a **structural analysis** of **LK**-proofs.



$CL(\varphi)$: **characteristic clause set**,

carries substantial information on derivations of cut formulas.

clause = atomic sequent.

cut-elimination = **reduction to atomic cuts**.

The Method CERES

Example: $\varphi =$

$$\frac{\varphi_1 \quad \varphi_2}{(\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y))} \text{ cut}$$

$\varphi_1 =$

$$\frac{\frac{\frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow: l}{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)} \rightarrow: r}{P(u) \rightarrow Q(u) \vdash (\exists y)(P(u) \rightarrow Q(y))} \exists: r}{(\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(u) \rightarrow Q(y))} \forall: l}{(\forall x)(P(x) \rightarrow Q(x)) \vdash (\forall x)(\exists y)(P(x) \rightarrow Q(y))} \forall: r$$

$$S = \{P(u) \vdash\} \times \{\vdash Q(u)\}.$$

Example

$\varphi =$

$$\frac{\varphi_1 \quad \varphi_2}{(\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y))} \text{ cut}$$

$\varphi_2 =$

$$\frac{\frac{\frac{P(a) \vdash P(a) \quad Q(v) \vdash Q(v)}{P(a), P(a) \rightarrow Q(v) \vdash Q(v)} \rightarrow : I}{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)} \rightarrow : r}{P(a) \rightarrow Q(v) \vdash (\exists y)(P(a) \rightarrow Q(y))} \exists : r}{(\exists y)(P(a) \rightarrow Q(y)) \vdash (\exists y)(P(a) \rightarrow Q(y))} \exists : I}{(\forall x)(\exists y)(P(x) \rightarrow Q(y)) \vdash (\exists y)(P(a) \rightarrow Q(y))} \forall : I$$

$$S' = \{\vdash P(a)\} \cup \{Q(v) \vdash\}.$$

cut-ancestors in axioms:

$$S_1 = \{P(u) \vdash\}, S_2 = \{\vdash Q(u)\}, S_3 = \{\vdash P(a)\}, S_4 = \{Q(v) \vdash\}.$$

$$S = S_1 \times S_2 = \{P(u) \vdash Q(u)\}.$$

$$S' = S_3 \cup S_4 = \{\vdash P(a); Q(v) \vdash\}.$$

characteristic clause set:

$$\text{CL}(\varphi) = S \cup S' = \{P(u) \vdash Q(u); \vdash P(a); Q(v) \vdash\}.$$

Projection of φ to $CL(\varphi)$

- ▶ *Skip inferences leading to cuts.*
- ▶ Obtain cut-free proof of end-sequent + a clause in $CL(\varphi)$.

proof φ of S



cut-free proof $\varphi(C)$ of $S \circ C$.

Let φ be the proof of the sequent

$S: (\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y))$ shown above.

$$CL(\varphi) = \{P(u) \vdash Q(u); \vdash P(a); Q(v) \vdash\}.$$

Skip inferences in φ_1 leading to cuts:

$$\frac{\frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow: I}{P(u), (\forall x)(P(x) \rightarrow Q(x)) \vdash Q(u)} \forall: I$$

$\varphi(C_1) =$

$$\frac{\frac{\frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow: I}{P(u), (\forall x)(P(x) \rightarrow Q(x)) \vdash Q(u)} \forall: I}{P(u), (\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y)), Q(u)} w: r$$

φ proof of

$S: (\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y))$

$CL(\varphi) = \{P(u) \vdash Q(u); \vdash P(a); Q(v) \vdash\}$.

For $C_2 = \vdash P(a)$ we obtain the projection $\varphi(C_2)$:

$$\frac{\frac{\frac{P(a) \vdash P(a)}{P(a) \vdash P(a), Q(v)} w : r}{\vdash P(a) \rightarrow Q(v), P(a)} \rightarrow : r}{\vdash (\exists y)(P(a) \rightarrow Q(y)), P(a)} \exists : I}{(\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y)), P(a)} w : I$$

The Method CERES

given proof φ ,

- ▶ extract characteristic clause set $CL(\varphi)$,
- ▶ compute the projections of φ to clauses in $CL(\varphi)$,
- ▶ **construct an R-refutation γ of $CL(\varphi)$,**
- ▶ insert the projections of φ into $\gamma \Rightarrow$ **CERES normal form** of φ .

Example

φ proof of

$S: (\forall x)(P(x) \rightarrow Q(x)) \vdash (\exists y)(P(a) \rightarrow Q(y))$

$CL(\varphi) = \{C_1 : P(u) \vdash Q(u), C_2 : \vdash P(a), C_3 : Q(u) \vdash\}$.

a resolution refutation δ of $CL(\varphi)$:

$$\frac{\frac{\vdash P(a) \quad P(u) \vdash Q(u)}{\vdash Q(a)} R \quad Q(v) \vdash}{\vdash} R$$

ground projection γ of δ :

$$\frac{\frac{\vdash P(a) \quad P(a) \vdash Q(a)}{\vdash Q(a)} R \quad Q(a) \vdash}{\vdash} R$$

via $\sigma = \{u \leftarrow a, v \leftarrow a\}$.

Example

end sequent S of φ , $S = B \vdash C$.

$\gamma =$

$$\frac{\frac{\vdash P(a) \quad P(a) \vdash Q(a)}{\vdash Q(a)} R \quad Q(a) \vdash R}{\vdash R} R$$

CERES-normal form $\varphi(\gamma) =$

$$\frac{\frac{\frac{(\chi_2) \quad B \vdash C, P(a) \quad P(a), B \vdash C, Q(a)}{B, B \vdash C, C, Q(a)} \text{ cut} \quad (\chi_3) \quad Q(a), B \vdash C}{\frac{B, B, B \vdash C, C, C}{S} \text{ contractions}} \text{ cut}}$$

- ▶ SK = set of all **LK**-derivations with **skolemized end-sequents**.
- ▶ SK_{\emptyset} = set of all cut-free proofs in SK .
- ▶ SK^i = derivations in SK with cut-formulas of complexity $\leq i$.
- ▶ **Goal** reduction to derivations with only atomic cuts, i.e.
transform $\varphi \in SK$ into $\psi \in SK^0$.

first step: construction of the *characteristic clause set*

Characteristic Clause Set:

Let φ be an **LK**-derivation of S and let Ω be the set of all occurrences of cut formulas in φ . We define the set of clauses $CL(\varphi)$ inductively:

Let ν be the occurrence of an initial sequent in φ and seq_ν the corresponding sequent. Then

$$S/\nu = \{seq(\nu, \Omega)\}$$

where $seq(\nu, \Omega)$ is the subsequence of seq_ν containing the ancestors of Ω .

Assume:

S/ν already constructed for $\text{depth}(\nu) \leq k$.

$\text{depth}(\nu) = k + 1$:

(a) ν is the consequent of μ :

$S/\nu = S/\mu$.

(b) ν is the consequent of μ_1 and μ_2 :

(b1) The auxiliary formulas of ν are *ancestors* of Ω , i.e. the formulas occur in $\text{seq}(\mu_1, \Omega), \text{seq}(\mu_2, \Omega)$:

(+) $S/\nu = S/\mu_1 \cup S/\mu_2$.

(b2) The auxiliary formulas of ν are *not ancestors* of Ω :

(\times) $S/\nu = S/\mu_1 \times S/\mu_2$.

$\text{CL}(\varphi) = S/\nu_0$ where ν_0 is the occurrence of the end-sequent.

If φ is a cut-free proof then there are no occurrences of cut formulas in φ and $\text{CL}(\varphi) = \{\top\}$.

Proposition:

Let φ be an **LK**-derivation. Then $\text{CL}(\varphi)$ is unsatisfiable.

Projection:

Lemma: Let φ be a deduction in SK of a sequent $S : \Gamma \vdash \Delta$. Let $C : \bar{P} \vdash \bar{Q}$ be a clause in $CL(\varphi)$. Then there exists a deduction

$$\varphi(C) \text{ of } \bar{P}, \Gamma \vdash \Delta, \bar{Q}$$

s.t.

$$\varphi(C) \in SK_{\emptyset} \text{ and } I(\varphi(C)) \leq I(\varphi).$$

Projection of φ to C : construct $\varphi(C)$.

the remaining steps:

- Construct an R-refutation γ of $CL(\varphi)$,
- insert the projections of φ into γ .
- add some contractions and obtain a proof with (only) atomic cuts.
- (• eliminate the atomic cuts)

Generality of CERES

CERES does *not only* work for **LK**.

- ▶ any sound sequent calculus for classical logic (with cut) does the job.
- ▶ unary rules do not “count”.
- ▶ *necessary*: auxiliary formulas, principal formulas, ancestor relation

Example: LKDe

LK + equality rules + definition introduction.

Important to *formalization of mathematical proofs*.

Corresponding clausal calculus: resolution + paramodulation.

Experiments with CERES

- ▶ underlying theorem prover: Prover9.
- ▶ very large proofs can be handled.
- ▶ Analysis of an example from C. Urban.
mathematically different proofs obtained by CERES.
- ▶ Analysis of Fürstenberg's proof of the infinity of primes.
Extraction of Euclid's construction.

Complexity of cut-elimination

- ▶ complexity of cut-elimination is **nonelementary**.

Orevkov, Statman (1979):

There exists a sequence of **LK**-proofs φ_n of sequents S_n s.t.

- ▶ $\|\varphi_n\| \leq 2^{k^*n}$ and
- ▶ for all cut-free proofs ψ of φ_n : $\|\psi\| > s(n)$ where

$$s(0) = 1, s(n+1) = 2^{s(n)}.$$

There exists no cheap way of cut-elimination **in principle!**

Complexity

Let $e : \mathbb{N}^2 \rightarrow \mathbb{N}$ be the following function

$$\begin{aligned}e(0, m) &= m \\e(n + 1, m) &= 2^{e(n, m)}.\end{aligned}$$

- ▶ $f : \mathbb{N}^k \rightarrow \mathbb{N}^m$ for $k, m \geq 1$ is called **elementary** if there exists an $n \in \mathbb{N}$ and a Turing machine π computing f s.t. for the computing time T_π of π :

$$T_\pi(l_1, \dots, l_k) \leq e(n, |(l_1, \dots, l_k)|)$$

where $|| = \text{maximum norm on } \mathbb{N}^k$.

- ▶ $s : \mathbb{N} \rightarrow \mathbb{N}$ is defined as $s(n) = e(n, 1)$ for $n \in \mathbb{N}$.

s and e are **nonelementary**.

Complexity of CERES

essential source of complexity:

- ▶ **resolution refutation** γ of $\text{CL}(\varphi)$.
- ▶ $\|\text{CL}(\varphi)\|$ is at most exponential in $\|\varphi\|$.
- ▶ Computing the global m.g.u. σ and a p-resolution refutation γ' from γ is at most exponential in $\|\gamma\|$.
- ▶ Let

$$r(\gamma') = \max\{\|t\| \mid t \text{ is a term occurring in } \gamma'\}.$$

Then $r(\gamma') \leq \|\gamma'\|$ and, for any clause $C \in \text{CL}(\varphi)$:

$$\|C\sigma\| \leq \|C\| * r(\gamma'),$$

$$\|\varphi(C\sigma)\| \leq \|\varphi(C)\| * r(\gamma') \leq \|\varphi\| * r(\gamma').$$

Complexity of CERES

φ : **LK**-proof of S .

Let γ be a resolution refutation of $CL(\varphi)$ and γ' be a corresponding ground projection.

Then there exists a CERES-normal form ψ of S s.t.

$$\|\psi\| \leq c * \|\gamma'\| * r(\gamma') * \|\varphi\|.$$

Complexity of CERES

- ▶ **Resolution complexity:**

Let \mathcal{C} be an unsatisfiable set of clauses. Then the *resolution complexity of \mathcal{C}* is defined as

$$rc(\mathcal{C}) = \min\{\|\gamma\| \mid \gamma \text{ is a resolution refutation of } \mathcal{C}\}.$$

Complexity of CERES

- ▶ **Resolution complexity:**

Let \mathcal{C} be an unsatisfiable set of clauses. Then the *resolution complexity of \mathcal{C}* is defined as

$$rc(\mathcal{C}) = \min\{\|\gamma\| \mid \gamma \text{ is a resolution refutation of } \mathcal{C}\}.$$

- ▶ **Definition:**

Let \mathcal{P} be a class of skolemized proofs. We say that

CERES is fast on \mathcal{P}

if there exists an elementary function f s.t. for all φ in \mathcal{P} :

$$rc(\text{CL}(\varphi)) \leq f(\|\varphi\|).$$

CERES is superior to Gentzen:

nonelementary speed-up of Gentzen by CERES:

- ▶ There exists a sequence of LK-proofs φ_n s.t.
 - ▶ $\|\varphi_n\| \leq 2^{k*n}$ and
 - ▶ all Gentzen-eliminations are of size $> s(n)$.
 - ▶ CERES is fast on $\{\varphi_n \mid n \in \mathbb{N}\}$.

- ▶ There is **no** nonelementary speed-up of CERES by reductive methods based on \mathcal{R} !

Fast Cut-Elimination Classes

problem: how to identify fast classes?

Fast Cut-Elimination Classes

problem: how to identify fast classes?

answer: use resolution decision theory for identification.

- ▶ Most well-known decidable subclasses K of first-order logic are elementary and
- ▶ decidable by resolution!

Fast Cut-Elimination Classes

problem: how to identify fast classes?

answer: use resolution decision theory for identification.

- ▶ Most well-known decidable subclasses K of first-order logic are elementary and
- ▶ decidable by resolution!

Consider clause forms \mathcal{K} of K s.t.

- ▶ $rc(\mathcal{C})$ is elementarily bounded in $\|C\|$ for $C \in \mathcal{K}$.
- ▶ Find a class of proofs P s.t. for $\varphi \in P$ $CL(\varphi) \in \mathcal{K}$.

Then CERES is fast on P .

A simple example:

Definition:

UIE is the class of all skolemized **LK**-proofs

- ▶ with atomic axioms of form $A \vdash A$,
- ▶ where all inferences **going into the end-sequent** are **unary**.

Proposition:

Cut-elimination is at most exponential on **UIE**.

exponentiality: based on m.g.u.

monotone cut-formulas

- ▶ fact: cut-elimination on proofs with a **single monotone cut** is nonelementary (Baaz, L. 1999).
- ▶ restriction on the arity of inferences in the proofs \Rightarrow elementary cut-elimination class.

Definition: UILM is the class of all skolemized **LK**-proofs φ with

- ▶ atomic axioms of form $A \vdash A$, s.t.
- ▶ φ contains only one cut which is **monotone**,
- ▶ all inferences in the **left cut-derivation** which go into the end-sequent are **unary**.

Theorem: Cut-elimination is elementary on **UILM**.
(generalized in M. Rukhaia's Master Thesis, 2009)

Let φ be a proof in **UILM** then $\varphi = \varphi[\psi]_\nu$ where ψ is the only cut-derivation in φ . Assume that $\psi =$

$$\frac{(\psi_1) \quad (\psi_2)}{\Gamma \vdash \Delta, A \quad A, \Pi \vdash \Lambda} \text{ cut}$$

$CL(\psi)$ is of the form $\mathcal{C}_1 \cup \mathcal{C}_2$, where

$$\mathcal{C}_1 = \{\vdash A_1; \dots; \vdash A_n\}, \text{ and}$$

$$\mathcal{C}_2 \subseteq \bigcup \{B_{j_1}, \dots, B_{j_k} \vdash \mid \{j_1, \dots, j_k\} \subseteq \{1, \dots, m\}, k \leq m\}.$$

$CL(\psi)$ is unsatisfiable \Rightarrow refutation ρ by hyperresolution of $CL(\psi)$.
 No mixed clauses in $CL(\psi) \Rightarrow \rho$ must consist of single
 hyperresolvent

$$\frac{\frac{\frac{\vdash A_{i_1} \quad B'_{j_1}, \dots, B'_{j_k} \vdash}{\vdots \vdots}}{\vdash A_{i_k} \quad B'_{j_k} \vdash}}{\vdash}}{\vdash}$$

ψ' : CERES-normal form of ψ . Define $\varphi' = \varphi[\psi']_\nu$.

$$\|\varphi'\| \leq \|\varphi\| + \|\psi'\| \leq \|\varphi\| + 2^{r^*} \|\varphi\|.$$

\Rightarrow cut-elimination is elementary on **UILM**.

The class MC

MC = class of all skolemized **LK**-proofs

- ▶ with axioms $A \vdash A$ (A quantifier-free),
- ▶ containing only **unary** function symbols,
- ▶ all predicate symbols **occurring in cut-formulas** are **monadic**.

The class **MC**

MC = class of all skolemized **LK**-proofs

- ▶ with axioms $A \vdash A$ (A quantifier-free),
- ▶ containing only **unary** function symbols,
- ▶ all predicate symbols **occurring in cut-formulas** are **monadic**.

note: end-sequents of **MC** define an undecidable class!

The class **MC**

MC = class of all skolemized **LK**-proofs

- ▶ with axioms $A \vdash A$ (A quantifier-free),
- ▶ containing only **unary** function symbols,
- ▶ all predicate symbols **occurring in cut-formulas** are **monadic**.

note: end-sequents of **MC** define an undecidable class!

Let $\psi \in \mathbf{MC}$:

cut formulas:

- ▶ **monadic** function symbols and
- ▶ **monadic** predicate symbols.

CERES on MC

adapt **MC** to CERES:

replace $A \vdash A$ (for nonatomic A) by a proof of $A \vdash A$ from atomic axioms (complexity linear) \Rightarrow proof transformation ρ .

$\psi \in \mathbf{MC} \Rightarrow$ consider $\varphi = \rho(\psi)$.

proof φ : the ancestors of the cuts in the axioms are

- ▶ $\vdash A$ or $A \vdash$ where A is of the form
- ▶ $P(f_1 \dots f_n s)$ for $s \in \text{CS} \cup V$.

We may **omit tautologies** in the construction of $\text{CL}(\varphi)$!

$\tau(A)$ = maximal term depth in A .

$\tau(C)$ = $\max\{\tau(A) \mid A \text{ in } C\}$.

$\tau_{\max}(x, A)$ = maximal depth of x in A .

$V(A)$ = set of variables in A .

depth ordering: A, B : we define $A <_d B$ if

(1) $V(A) \subseteq V(B)$,

(2) $\tau(A) < \tau(B)$ and

(3) for all $x \in V(A)$: $\tau_{\max}(x, A) < \tau_{\max}(x, B)$.

$<_d$ is an atom ordering.

ordered resolution

Let $C, D \in \mathcal{C}$, R a resolvent of C, D with resolved atom A .

$N_C(R) \in \rho_{<_d}(C)$ iff there is no atom B in R s.t. $A <_d B$.

The corresponding resolution operator is defined by:

$$R_{<_d}(C) = C \cup \rho_{<_d}(C), \quad R_{<_d}^*(C) = \bigcup_{i=0}^{\infty} R_{<_d}^i(C).$$

$R_{<_d}$ is **complete**, i.e. $\vdash \in R_{<_d}^*(C)$ if C is unsatisfiable.

The class \mathbb{K}

\mathbb{K} is the set of all finite condensed sets of clauses \mathcal{C} s.t. for all $C \in \mathcal{C}$: $|V(A)| \leq 1$ for all atoms A occurring in C .

Lemma I: $R_{<d}^*(\mathcal{C})$ is finite for each $\mathcal{C} \in \mathbb{K}$ and $\tau(R_{<d}^*(\mathcal{C})) \leq 2 * \tau(\mathcal{C})$. proof: (C. Fermüller 1991, L. 1997).

K_{mon} is the subclass of K containing only monadic predicate symbols and monadic function symbols.

K_{mon} is the subclass of K containing only monadic predicate symbols and monadic function symbols.

Lemma II: Let $\mathcal{C} \in K_{mon}$. Then

- (1) $|R_{<d}^*(\mathcal{C})| \leq 2^{3s^2}$, and
- (2) $\max\{\|C\| \mid C \in R_{<d}^*(\mathcal{C})\} \leq 2s(\tau(\mathcal{C}) + 2)$

for $s = 2|\text{PS}(\Sigma)||\text{FS}(\Sigma)|^{2\tau(\mathcal{C})}(|\text{CS}(\Sigma)| + 1)$
where $\Sigma = \text{signature of } \mathcal{C}$.

Theorem: CERES is fast on **MC**. As a consequence, cut-elimination is elementary on **MC**.

proof:

The clause set $CL(\varphi)$ (defined by union and product) only consists of clauses built from atoms of type

$$P(f_1 \dots f_n s) \text{ for } s \in CS \cup V.$$

$CL(\varphi)$ itself need not be in K_{mon} ,
but its condensation $\mathcal{C}: N_c(CL(\varphi))$ is in K_{mon} .

By Lemma II we get

$$|R_{<d}^*(\mathcal{C})| \leq 2^{3s^2}$$

for $s = 2|\text{PS}(\Sigma)||\text{FS}(\Sigma)|^{2\tau(\mathcal{C})}(|\text{CS}(\Sigma)| + 1)$ and $\Sigma = \Sigma(\mathcal{C})$.

$$\max\{\|C\| \mid C \in R_{<d}^*(\mathcal{C})\} \leq 2s(\tau(\mathcal{C}) + 2).$$

\mathcal{C} is unsatisfiable



resolution refutation containing at most

$\leq 2^{3s^2}$ different clauses of length $\leq 2s(\tau(\mathcal{C}) + 2)$.

Theorem:

Gentzen's cut-elimination method is nonelementary on **MC**.

proof:

Consider the worst-case proof sequence $(\rho_n)_{n \in \mathbb{N}}$ of V.P. Orevkov.

- the (skolemized) end sequents of ρ_n :

$$\begin{array}{l}
 (\forall w)P(w, c, f(w)), \\
 (\forall u, v, w)((\exists y)(P(y, c, u) \wedge (\exists z)(P(v, y, z) \wedge P(z, y, w))) \rightarrow \\
 P(v, u, w)) \\
 \vdash \\
 (\exists v_n)(P(c, c, v_n) \wedge (\exists v_{n-1})(P(c, v_n, v_{n-1}) \wedge \dots \wedge (\exists v_0)P(c, v_1, v_0) \dots))
 \end{array}$$

- the cut formulas $A_n(c)$ of ρ_n :

$$A_0(\alpha) \equiv (\forall w_0)(\exists v_0)P(w_0, \alpha, v_0), \quad \bar{A}_0(\alpha, \delta) \equiv (\exists v_0)P(\alpha, \delta, v_0),$$

$$\bar{A}_{i+1}(\alpha, \delta) \equiv (\exists v_{i+1})(A_i(v_{i+1}) \wedge P(\alpha, \delta, v_{i+1})),$$

$$A_{i+1}(\alpha) \equiv (\forall w_{i+1})(A_i(w_{i+1}) \rightarrow \bar{A}_{i+1}(w_{i+1}, \alpha)).$$

Gentzen on MC

$(\rho_n)_{n \in \mathbb{N}}$ contains

- ▶ one unary function symbol f ,
- ▶ one ternary predicate symbol P .
- ▶ cut-elimination on $(\rho_n)_{n \in \mathbb{N}}$ is **nonelementary**.
- ★ replace the predicate $\lambda x, y, z. P(x, y, z)$
- ▶ by the conjunction of new unary predicates

$$\lambda x, y, z. ((Q_1(x) \wedge Q_2(y)) \wedge Q_3(z)).$$

everywhere in ρ_n .

⇒ new sequence $(\varphi_n)_{n \in \mathbb{N}}$ in **MC**.

Every reduction step on φ_n is completely isomorphic to steps performed on ρ_n !

⇒

the sequence of cut-elimination steps on $(\varphi_n)_{n \in \mathbb{N}}$ is **as long** as that on the original sequence $(\rho_n)_{n \in \mathbb{N}}$.

Gentzen is of *nonelementary complexity* on $(\rho_n)_{n \in \mathbb{N}}$.

holds for all reductive methods based on \mathcal{R} !

impossible to prove **MC** fast via \mathcal{R} !

CERES versus Gentzen

is it possible to prove fast cut-elimination of a class P by Gentzen,
but CERES "fails" on P ?

CERES versus Gentzen

is it possible to prove fast cut-elimination of a class P by Gentzen, but CERES "fails" on P ?

The answer is **NO!**

CERES versus Gentzen

is it possible to prove fast cut-elimination of a class P by Gentzen, but CERES "fails" on P ?

The answer is **NO!**

- ▶ no nonelementary **speed-up** of CERES by Gentzen!
- ▶ it is **impossible** that fast cut-elimination is provable by Gentzen, but not by CERES!

Characteristic Clause Sets and Cut-Reduction

Main Lemma:

Let φ, φ' be **LK**-derivations with $\varphi > \varphi'$ for a cut reduction relation $>$ based on \mathcal{R} . Then

$$\text{CL}(\varphi) \leq_{ss} \text{CL}(\varphi').$$

proof:

by cases according to the definitions of $>$ and \mathcal{R} . ◇

\mathcal{R} = set of cut-reduction rules extracted from Gentzen's proof.

\leq_{ss} : **subsumption relation** on clause sets.

Characteristic Clause Sets and Cut-Reduction

Theorem: Let φ be an **LK**-deduction and ψ be a normal form of φ under a cut reduction relation $>$ based on \mathcal{R} . Then

$$\text{CL}(\varphi) \leq_{ss} \text{CL}(\psi).$$

Theorem: Let φ be an **LK**-derivation and ψ be a normal form of φ under a cut reduction relation $>_{\mathcal{R}}$ based on \mathcal{R} . Then there exists a resolution refutation γ of $\text{CL}(\varphi)$ s.t.

$$\gamma \leq_{ss} \text{RES}(\psi).$$

$\text{RES}(\psi) =$ (canonic) resolution refutation of $\text{CL}(\psi)$.

results above improved by S. Hetzl and B. Woltzenlogel Paleo.

Characteristic Clause Sets and Cut-Reduction

Corollary 1:

Let φ be an **LK**-derivation and ψ be a normal form of φ under a cut reduction relation $>_{\mathcal{R}}$ based on \mathcal{R} . Then there exists a resolution refutation γ of $\text{CL}(\varphi)$ s.t.

$$l(\gamma) \leq l(\text{RES}(\psi)) \leq l(\psi) * 2^{2 * l(\psi)}.$$

Corollary 2:

Let φ be an **LK**-derivation and ψ be a normal form of φ under a cut reduction relation $>_{\mathcal{R}}$ based on \mathcal{R} . Then there exists a proof CERES-normal form χ of φ s.t.

$$l(\chi) \leq l(\varphi) * l(\psi) * 2^{2 * l(\psi)}.$$

proof: χ is defined by inserting the projections of φ into a refutation γ of $\text{CL}(\varphi)$.



Corollary 3: a nonelementary speed-up of CERES by \mathcal{R} is impossible!

There exists **no** sequence of proofs $(\varphi_n)_{n \in \mathbb{N}}$ s.t.

(a) there exists an m and \mathcal{R} -normal forms $\hat{\varphi}_n$ of φ_n s.t.

$$\|\hat{\varphi}_n\| \leq e(m, \|\varphi_n\|) \text{ for all } n$$

and

(b) for all $k \in \mathbb{N}$ there exists a number m s.t. for all $n \geq m$ and for all CERES-normal forms ψ of φ_n

$$\|\psi\| > e(k, \|\varphi_n\|).$$

Cut Reduction Rules:

If a cut-derivation ψ is transformed to ψ' then we define

$$\psi > \psi'$$

where $\psi =$

$$\frac{\begin{array}{c} (\rho) \\ \Gamma \vdash \Delta \end{array} \quad \begin{array}{c} (\sigma) \\ \Pi \vdash \Lambda \end{array}}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda} \textit{cut}$$

3.11. rank = 2.

The last inferences in ρ, σ are logical ones and the cut-formula is the principal formula of these inferences:

3.113.31.

$$\frac{\frac{\frac{(\rho_1)}{\Gamma \vdash \Delta, A} \quad \frac{(\rho_2)}{\Gamma \vdash \Delta, B}}{\Gamma \vdash \Delta, A \wedge B} \wedge : r \quad \frac{(\sigma')}{A, \Pi \vdash \Lambda} \wedge : l}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{cut}(A \wedge B)$$

transforms to

$$\frac{\frac{(\rho_1)}{\Gamma \vdash \Delta, A} \quad \frac{(\sigma')}{A, \Pi \vdash \Lambda} \text{cut}(A)}{\frac{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda} w : *}$$

For the other form of $\wedge : l$ the transformation is straightforward.

3.113.33.

$$\frac{\frac{(\rho'[\alpha])}{\Gamma \vdash \Delta, B_\alpha^x} \quad \forall : r \quad \frac{(\sigma')}{B_t^x, \Pi \vdash \Lambda} \quad \forall : l}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{cut}((\forall x)B)$$

transforms to

$$\frac{\frac{(\rho'[t])}{\Gamma \vdash \Delta, B_t^x} \quad (\sigma')}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda} \text{cut}(B_t^x)}{\Gamma, \Pi \vdash \Delta, \Lambda} w : *$$

3.113.34. The last inferences in ρ, σ are $\exists : r, \exists : l$: symmetric to 3.113.33.

3.12. rank > 2 :

3.121. right-rank > 1 :

3.121.2. The cut formula does not occur in the antecedent of the end-sequent of ρ .

3.121.23. The last inference in σ is binary:

3.121.231. The case $\wedge : r$. Here

$$\frac{\frac{(\rho) \quad \frac{(\sigma_1) \quad \Gamma \vdash \Delta, B \quad (\sigma_2) \quad \Gamma \vdash \Delta, C}{\Gamma \vdash \Delta, B \wedge C} \wedge : r}{\Pi \vdash \Lambda} \quad \text{cut}(A)}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, B \wedge C} \text{cut}(A)$$

transforms to

$$\frac{\frac{(\rho) \quad \frac{(\sigma_1) \quad \Gamma \vdash \Delta, B}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, B} \text{cut}(A)}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, B \wedge C} \quad \frac{(\rho) \quad \frac{(\sigma_2) \quad \Gamma \vdash \Delta, C}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, C} \text{cut}(A)}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, B \wedge C} \wedge : r$$

3.121.232. The case $\vee : I$. Then ψ is of the form

$$\frac{(\rho) \quad \frac{(\sigma_1) \quad B, \Gamma \vdash \Delta \quad C, \Gamma \vdash \Delta}{B \vee C, \Gamma \vdash \Delta} \vee : I}{\Pi, (B \vee C)^*, \Gamma^* \vdash \Lambda^*, \Delta} \text{cut}(A)$$

$(B \vee C)^*$ is empty if $A = B \vee C$ and $B \vee C$ otherwise.

We first define the proof τ :

$$\frac{\frac{(\rho) \quad \frac{(\sigma_1) \quad B, \Gamma \vdash \Delta}{B^*, \Pi, \Gamma^* \vdash \Lambda^*, \Delta} \text{cut}(A)}{B, \Pi, \Gamma^* \vdash \Lambda^*, \Delta} x \quad \frac{(\rho) \quad \frac{(\sigma_2) \quad C, \Gamma \vdash \Delta}{C^*, \Pi, \Gamma^* \vdash \Lambda^*, \Delta} \text{cut}(A)}{C, \Pi, \Gamma^* \vdash \Lambda^*, \Delta} x}{B \vee C, \Pi, \Gamma^* \vdash \Lambda^*, \Delta} \vee : I$$

Note that, in case $A = B$ or $A = C$, the inference x is $w : I$; otherwise x is the identical transformation and can be dropped.

If $(B \vee C)^* = B \vee C$ then ψ transforms to τ .

If, on the other hand, $(B \vee C)^*$ is empty (i.e. $B \vee C = A$) then we transform ψ to

$$\frac{\frac{(\rho)}{\Pi \vdash \Lambda} \quad \tau}{\Pi, \Pi^*, \Gamma^* \vdash \Lambda^*, \Lambda^*, \Delta} \text{ cut}(A)}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta} c : *$$

3.121.233. The last inference in ψ_2 is $\rightarrow: I$. Then ψ is of the form:

$$\frac{\frac{(\psi_1) \quad \Gamma \vdash \Theta, B \quad C, \Delta \vdash \Lambda}{\Pi \vdash \Sigma} \quad \rightarrow: I}{\Pi, (B \rightarrow C)^*, \Gamma^*, \Delta^* \vdash \Sigma^*, \Theta, \Lambda} \text{cut}(A)$$

As in 3.121.232 $(B \rightarrow C)^* = B \rightarrow C$ for $B \rightarrow C \neq A$ and $(B \rightarrow C)^*$ empty otherwise.

3.121.233.1. A occurs in Γ and in Δ . Again we define a proof τ :

$$\frac{\frac{(\psi_1) \quad \Gamma \vdash \Theta, B}{\Pi, \Gamma^* \vdash \Sigma^*, \Theta, B} \text{cut}(A) \quad \frac{\frac{(\psi_1) \quad \Pi \vdash \Sigma \quad C, \Delta \vdash \Lambda}{C^*, \Pi, \Delta^* \vdash \Sigma^*, \Lambda} \text{cut}(A)}{C, \Pi, \Delta^* \vdash \Sigma^*, \Lambda} \times}{B \rightarrow C, \Pi, \Gamma^*, \Pi, \Delta^* \vdash \Sigma^*, \Theta, \Sigma^*, \Lambda} \rightarrow: I$$

If $(B \rightarrow C)^* = B \rightarrow C$ then, as in 3.121.232, ψ is transformed to τ + some additional contractions. Otherwise an additional cut with cut formula A is appended.

3.121.233.2 A occurs in Δ , but not in Γ . As in 3.121.233.1 we define a proof τ :

$$\frac{\frac{\frac{(\chi_1)}{\Gamma \vdash \Theta, B} \quad \frac{\frac{(\psi_1)}{\Pi \vdash \Sigma} \quad \frac{(\chi_2)}{C, \Delta \vdash \Lambda}}{C^*, \Pi, \Delta^* \vdash \Sigma^*, \Lambda} \text{cut}(A)}{C, \Pi, \Delta^* \vdash \Sigma^*, \Lambda} \times}{B \rightarrow C, \Gamma, \Pi, \Delta^* \vdash \Theta, \Sigma^*, \Lambda} \rightarrow: l$$

Again we distinguish the cases $B \rightarrow C = A$ and $B \rightarrow C \neq A$ and define the transformation of ψ exactly like in 3.121.233.1.

References:

M. Baaz, A. Leitsch: [Cut-Elimination and Redundancy-Elimination by Resolution](#), *Journal of Symbolic Computation*, 29, pp. 149-176, 2000.

M. Baaz, A. Leitsch: [Towards a Clausal Analysis of Cut-Elimination](#), *Journal of Symbolic Computation*, 41, pp. 381–410, 2006.

M. Baaz, A. Leitsch: [Fast Cut-Elimination by CERES](#), Tribute Series 13, College Publications 2010.

M. Baaz, A. Leitsch: [Methods of Cut-Elimination](#), Trends in Logic 34, Springer 2011.

website: <http://www.logic.at/ceres/>