On proof mining by cut-elimination

Alex Leitsch

Vienna University of Technology

Aim

- Are proofs just verifications?

Aim

- Are proofs just verifications?
- proofs may provide more information

Aim

- Are proofs just verifications?
- proofs may provide more information

Proof Mining:

- Extraction of explicit information from proofs

Aim

- Are proofs just verifications?
- proofs may provide more information

Proof Mining:

- Extraction of explicit information from proofs

- to this aim use Cut-Elimination.

Cut-Elimination

Cut: Rule for using lemmas in a proof.

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

Applications:
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 φ of a formula A there exists a proof φ' of A without cuts; φ' can be constructed algorithmically.

Sequent Calculus

Sequent: $\mathcal{A} \vdash \mathcal{B}$, for finite multi-sets of formulas $\mathcal{A}, \mathcal{B}$.
$A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ represents
$\bigwedge A_i \to \bigvee B_j$.
$\vdash$: separation-symbol.

LK: calculus on sequents, based on logical and structural rules.
axioms: $A \vdash A$ for atoms A.

The logical rules of **LK**

$\wedge$-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:

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

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

The logical rules of **LK**

$\neg$-introduction:

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

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

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

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

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

The structural rules of **LK**

weakening:

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

contraction:

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

cut:

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

example: proof with cut

Let $\varphi =$

$$\dfrac{\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{P(a) \vdash P(a) \lor Q(a)}\;\lor: r_1}{P(a) \vdash \exists y(P(y) \lor Q(y))}\;\exists: r \qquad \dfrac{\dfrac{Q(b) \vdash Q(b)}{Q(b) \vdash P(b) \lor Q(b)}\;\lor: r_2}{Q(b) \vdash \exists y(P(y) \lor Q(y))}\;\exists: r}{P(a) \lor Q(b) \vdash \exists y(P(y) \lor Q(y))}\;\lor: l \qquad \overset{(\chi)}{\exists y(P(y) \lor Q(y)), \forall x.\neg P(x) \vdash \exists z.Q(z)}}{P(a) \lor Q(b), \forall x.\neg P(x) \vdash \exists z.Q(z)}\;cut$$

for $\chi =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha) \vdash P(\alpha)}{P(\alpha), \neg P(\alpha) \vdash}\;\neg: l}{P(\alpha), \neg P(\alpha) \vdash Q(\alpha)}\;w: r \qquad \dfrac{Q(\alpha) \vdash Q(\alpha)}{Q(\alpha), \neg P(\alpha) \vdash Q(\alpha)}\;w: l}{P(\alpha) \lor Q(\alpha), \neg P(\alpha) \vdash Q(\alpha)}\;\lor: l}{P(\alpha) \lor Q(\alpha), \neg P(\alpha) \vdash \exists z.Q(z)}\;\exists: r}{P(\alpha) \lor Q(\alpha), \forall x.\neg P(x) \vdash \exists z.Q(z)}\;\forall: l}{\exists y(P(y) \lor Q(y)), \forall x.\neg P(x) \vdash \exists z.Q(z)}\;\exists: l$$

proof without cut

$\psi =$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{P(a) \vdash P(a)}{P(a), \neg P(a) \vdash}\ \neg : l
    }{P(a), \neg P(a) \vdash Q(b)}\ w : r
    \qquad
    \dfrac{Q(b) \vdash Q(b)}{Q(b), \neg P(a) \vdash Q(b)}\ w : l
  }{P(a) \vee Q(b), \neg P(a) \vdash {\color{blue}Q(b)}}\ \vee : l
}{
  \dfrac{P(a) \vee Q(b), \neg P(a) \vdash {\color{blue}\exists z. Q(z)}}{P(a) \vee Q(b), \forall x. \neg P(x) \vdash {\color{blue}\exists z. Q(z)}}\ \forall : l
}\ \exists : r
$$

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:

$$
\dfrac{\dfrac{\dfrac{P(a)\vdash P(a)}{(\forall x)P(x)\vdash P(a)}\;\forall\colon l \qquad \dfrac{P(b)\vdash P(b)}{(\forall x)P(x)\vdash P(b)}\;\forall\colon l}{(\forall x)P(x)\vdash P(a)\wedge P(b)}\;\wedge\colon r \qquad \dfrac{\dfrac{P(a)\vdash P(a)}{P(a)\wedge P(b)\vdash P(a)}\;\wedge\colon l}{P(a)\wedge P(b)\vdash (\exists x)P(x)}\;\exists\colon r}{(\forall x)P(x)\vdash (\exists x)P(x)}\;cut
$$

$\mathrm{rank}=3,\ \mathrm{grade}=1.$

reduce to $\mathrm{rank}=2,\ \mathrm{grade}=1$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{P(a)\vdash P(a)}{(\forall x)P(x)\vdash P(a)}\;\forall\colon l \qquad \dfrac{P(b)\vdash P(b)}{(\forall x)P(x)\vdash P(b)}\;\forall\colon l}{(\forall x)P(x)\vdash P(a)\wedge P(b)}\;\wedge\colon r \qquad \dfrac{P(a)\vdash P(a)}{P(a)\wedge P(b)\vdash P(a)}\;\wedge\colon l}{(\forall x)P(x)\vdash P(a)}\;cut}{(\forall x)P(x)\vdash (\exists x)P(x)}\;\exists\colon r
$$

$$
\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)}\ \forall\colon l \qquad \dfrac{P(b) \vdash P(b)}{(\forall x)P(x) \vdash P(b)}\ \forall\colon l}{(\forall x)P(x) \vdash P(a) \land P(b)}\ \land\colon r \qquad \dfrac{P(a) \vdash P(a)}{P(a) \land P(b) \vdash P(a)}\ \land\colon l}{\dfrac{(\forall x)P(x) \vdash P(a)}{(\forall x)P(x) \vdash (\exists x)P(x)}\ \exists\colon r}\ cut
$$

$\mathrm{rank} = 2,\ \mathrm{grade} = 1.$ Reduce to $\mathrm{grade} = 0,\ \mathrm{rank} = 3$:

$$
\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)}\ \forall\colon l \qquad P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)}\ cut}{(\forall x)P(x) \vdash (\exists x)P(x)}\ \exists\colon r
$$

eliminate cut with axiom:

$$
\dfrac{\dfrac{P(a) \vdash P(a)}{(\forall x)P(x) \vdash P(a)}\ \forall\colon l}{(\forall x)P(x) \vdash (\exists x)P(x)}\ \exists\colon r
$$

Cut-elimination by Resolution (CERES)

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

$$
\begin{array}{ll}
 & \text{sub-derivations into cuts} \\
\nearrow & \\
\varphi & \\
\searrow & \\
 & \text{sub-derivation into end sequent}
\end{array}
$$

$\mathrm{CL}(\varphi)$: **characteristic clause set**,
carries substantial information on derivations of cut formulas.
clause $=$ atomic sequent.
cut-elimination $=$ reduction to *atomic cuts*.

The Method CERES

Example: $\varphi =$

$$\dfrac{\varphi_1 \qquad \varphi_2}{(\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y))}\ cut$$

$\varphi_1 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(u) \vdash P(u) \qquad Q(u) \vdash Q(u)}{P(u), P(u) \to Q(u) \vdash Q(u)}\ \to: l}{P(u) \to Q(u) \vdash P(u) \to Q(u)}\ \to: r}{P(u) \to Q(u) \vdash (\exists y)(P(u) \to Q(y))}\ \exists: r}{(\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(u) \to Q(y))}\ \forall: l}{(\forall x)(P(x) \to Q(x)) \vdash (\forall x)(\exists y)(P(x) \to Q(y))}\ \forall: r$$

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

Example

$\varphi =$

$$\dfrac{\varphi_1 \qquad \varphi_2}{(\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y))}\ cut$$

$\varphi_2 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(a) \vdash P(a) \qquad Q(v) \vdash Q(v)}{P(a), P(a) \to Q(v) \vdash Q(v)} \to: l}{P(a) \to Q(v) \vdash P(a) \to Q(v)} \to: r}{P(a) \to Q(v) \vdash (\exists y)(P(a) \to Q(y))} \exists : r}{(\exists y)(P(a) \to Q(y)) \vdash (\exists y)(P(a) \to Q(y))} \exists : l}{(\forall x)(\exists y)(P(x) \to Q(y)) \vdash (\exists y)(P(a) \to Q(y))} \forall : l$$

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

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:

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

Projection of φ to $\mathrm{CL}(\varphi)$

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

$$\text{proof } \varphi \text{ of } S$$
$$\Downarrow$$
$$\text{cut-free proof } \varphi(C) \text{ of } S \circ C.$$

Let φ be the proof of the sequent
$S\colon (\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y))$ shown above.

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

Skip inferences in φ_1 leading to cuts:

$$\dfrac{\dfrac{\color{red}{P(u)} \vdash P(u) \quad Q(u) \vdash \color{red}{Q(u)}}{\color{red}{P(u)}, P(u) \to Q(u) \vdash \color{red}{Q(u)}} \to : l}{\color{red}{P(u)}, (\forall x)(P(x) \to Q(x)) \vdash \color{red}{Q(u)}} \ \forall : l$$

$\varphi(C_1) =$

$$\dfrac{\dfrac{\dfrac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \to Q(u) \vdash Q(u)} \to : l}{P(u), (\forall x)(P(x) \to Q(x)) \vdash Q(u)} \ \forall : l}{P(u), (\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y)), Q(u)} \ w : r$$

φ proof of
$S\colon (\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y))$

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{P(a) \vdash P(a), Q(v)}\ w:r}{\vdash P(a) \to Q(v), P(a)}\ \to: r}{\vdash (\exists y)(P(a) \to Q(y)), P(a)}\ \exists : l}{(\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y)), P(a)}\ w:l$$

The Method CERES

given proof φ,

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

Example

φ proof of
$S\colon (\forall x)(P(x) \to Q(x)) \vdash (\exists y)(P(a) \to Q(y))$

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

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

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

ground projection γ of δ:

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

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

Example

end sequent S of φ, $S = B \vdash C$.

$\gamma =$

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

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

$$\cfrac{\cfrac{\cfrac{\cfrac{(\chi_2)}{B \vdash C, P(a)} \quad \cfrac{(\chi_1)}{P(a), B \vdash C, Q(a)}}{B, B \vdash C, C, Q(a)}\,cut \quad \cfrac{(\chi_3)}{Q(a), B \vdash C}}{B, B, B \vdash C, C, C}\,cut}{S}\,\text{contractions}$$

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.

instantiation sequents

instantiation sequent:

Let S be a sequent of the form

$$(\forall \bar{x}_1)F_1, \ldots, (\forall \bar{x}_n)F_n \vdash (\exists \bar{y}_1)G_1, \ldots, (\exists \bar{y}_m)G_m,$$

where $\forall \bar{x}_i$ stands for $(\forall x_{1,i}) \ldots (\forall x_{k_i,i})$. Let $\mathcal{F}_i = F'_{i,1}, \ldots F'_{i,k_i}$ and $\mathcal{G}_j = G'_{j,1}, \ldots G'_{j,l_j}$, where the $F'_{i,m}$ are instances of F_i, the $G'_{j,r}$ instances of the G_j. Then a sequent of the form

$$S^*: \ \mathcal{F}_1, \mathcal{F}_2, \ldots \mathcal{F}_n \vdash \mathcal{G}_1, \ldots \mathcal{G}_m$$

is called an instantiation sequent of S

instantiation sequents: examples

$$S = (\forall x)P(x) \vdash P(a) \wedge P(b).$$

$P(a) \vdash P(a) \wedge P(b)$,
$P(b) \vdash P(a) \wedge P(b)$,
$P(a), P(b) \vdash P(a) \wedge P(b)$
are instantiation sequents of S.

$$S_1 = P(a), (\forall x)(P(x) \rightarrow P(f(x)) \vdash (\exists y)P(f(f(y)))$$

$$P(a), P(a) \rightarrow P(f(a)), P(f(a)) \rightarrow P(f(f(a))) \vdash P(f(f(a)))$$

is an instantiation sequent of S_1.

an application of cut-elimination: Herbrand's theorem

Let φ be an **LK**-proof of a sequent S of the form

$$(\forall \bar{x}_1)F_1, \ldots, (\forall \bar{x}_n)F_n \vdash (\exists \bar{y}_1)G_1, \ldots, (\exists \bar{y}_m)G_m,$$

where $\forall \bar{x}_i$ stands for $(\forall x_{1,i}) \ldots (\forall x_{k_i,i})$. Then there exists an instantiation sequent S^* of S which is **LK**-provable. S^* is called a Herbrand sequent of S.

proof (given in Gentzen's midsequent theorem) by

- cut-elimination on φ yielding a proof ψ,
- construction of S^* via ψ by induction on the number of inferences in ψ and by permuting the order of inferences

full cut-elimination is not necessary: quantifier-free cuts are admitted!

construction of a Herbrand sequent

given a proof φ without quantified cuts of

$$S: \ (\forall \bar{x}_1) F_1, \ldots, (\forall \bar{x}_n) F_n \vdash (\exists \bar{y}_1) G_1, \ldots, (\exists \bar{y}_m) G_m.$$

- collect all instances F_i', G_j' appearing in φ,
- construct an instantiation sequent S^* of S with this instances.
- then S^* is a Herbrand sequent.

construction of a Herbrand sequent: example

proof:

$$
\dfrac{
\dfrac{
\dfrac{P(a) \vdash P(a) \quad P(f(a)) \vdash P(f(a))}{P(a), P(a) \to P(f(a)) \vdash P(f(a))}\ \to: l
}{P(a), (\forall x)(P(x) \to P(f(x))) \vdash P(f(a))}\ *
\quad
\dfrac{
\dfrac{P(f(a)) \vdash P(f(a)) \quad P(f(f(a))) \vdash P(f(f(a)))}{P(f(a)), P(f(a)) \to P(f(f(a))) \vdash P(f(f(a)))}\ \to: l
}{P(f(a)), (\forall x)(P(x) \to P(f(x))) \vdash P(f(f(a)))}\ *
}{
\dfrac{P(a), (\forall x)(P(x) \to P(f(x))), (\forall x)(P(x) \to P(f(x))) \vdash P(f(f(a)))}{P(a), (\forall x)(P(x) \to P(f(x))) \vdash P(f(f(a)))}\ c: l
}\ cut
$$

extracted Herbrand sequent:

$$P(a), P(a) \to P(f(a)), P(f(a)) \to P(f(f(a))) \vdash P(f(f(a))).$$

Herbrand sequents: importance

- reduction of a theorem in predicate logic to a theorem in propositional logic.
- Herbrand sequents contain the key information of mathematical proofs,
- quantifier-instances are crucial in "real" proofs,
- Herbrand sequents are compact representations of cut-free proofs; this is important in automated proof analysis.
- Herbrand sequents are a basis for automated cut-introduction methods.

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

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

- $f : \mathbb{N}^k \to \mathbb{N}^m$ 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:

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

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

- $s : \mathbb{N} \to \mathbb{N}$ 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 $\mathrm{CL}(\varphi)$.
- $\|\mathrm{CL}(\varphi)\|$ 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 $C \in \mathrm{CL}(\varphi)$:

$$\begin{aligned} \|C\sigma\| &\leq \|C\| * r(\gamma'), \\ \|\varphi(C\sigma)\| \leq \|\varphi(C)\| * r(\gamma') &\leq \|\varphi\| * r(\gamma'). \end{aligned}$$

Complexity of CERES

φ: **LK**-proof of S.

Let γ be a resolution refutation of $\mathrm{CL}(\varphi)$ 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 $\mathcal{P}$:

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

Efficiency of CERES

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 $\mathcal{R}$!

CERES versus Gentzen

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

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!
- there is no class where CERES is slow, but Gentzen reduction is fast.

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

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

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

$\mathcal{R} =$ 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

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

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 $\mathrm{CL}(\varphi)$ s.t.

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

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

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 $\mathrm{CL}(\varphi)$ s.t.

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

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 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 $\mathrm{CL}(\varphi)$.

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

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

Fürstenberg's proof of the infinitude of primes

Arithmetic progressions can be used as a basis for a topology over the natural numbers. We will denote an arithmetic progression by

$$\nu(a, b) = \{a + bn \mid n \in \mathbb{N}\}$$

for $a \in \mathbb{N}$ and $b \in \mathbb{N} \setminus \{0\}$.

Proposition:

By defining a set $A \subseteq \mathbb{N}$ as open, when A is either empty or for each $x \in A$ exists an $a \in \mathbb{N} \setminus \{0\}$ such that $\nu(x, a) \subseteq A$, one obtains a topology over $\mathbb{N}$.

An analysis of Fürstenberg's proof

Lemma:
Every arithmetic progression starting at 0 is closed.

Theorem: There are infinintely many primes.

proof:
P: set of all primes. Assume P is finite. Define

$$X = \bigcup \{\nu(0, p) \mid p \in P\}.$$

By the above lemma every $\nu(0, p)$ for $p \in P$ is closed,
so X is a finite union of closed sets and therefore closed.
Every number different from 1 has a prime divisor, thus $\bar{X} = \{1\}$.
X is a complement of a closed set, so $\bar{X}$ is open.
But $\{1\}$ is neither empty nor does it contain an arithmetic progression, and so $\{1\}$ is not open. Contradiction!

An analysis of Fürstenberg's proof

1. step: formalization in 2nd-order arithmetic

(a) $m \in \nu(k, l) \;\equiv\; \exists n(m = k + n * l)$.

(b) $\mathrm{DIV}(l, k) \equiv \exists m. l * m = k$.

(c) $\mathrm{PRIME}(k) \equiv 1 < k \wedge \forall l(\mathrm{DIV}(l, k) \rightarrow (l = 1 \vee l = k))$.

(d) $X \subseteq Y \equiv \forall n(n \in X \rightarrow n \in Y)$, and $X = Y \equiv X \subseteq Y \wedge Y \subseteq X$.

(e) $n \in \overline{X} \equiv n \notin X$.

(f) A function $p \colon \mathbb{N} \rightarrow \mathbb{N}$ which enumerates primes is one that fulfills the property:

$$\forall i \forall k(p(i) = k \rightarrow \mathrm{PRIME}(k)).$$

Definition of p needs the comprehension principle!

(g) $n \in \mathrm{S}[l] \equiv \exists m(m \leq l \wedge n \in \nu(0, p(m)))$.
$\mathrm{S}[l]$ describes the set of all elements n which occur in some $\nu(0, k)$, where k is one of the first $l + 1$ primes enumerated by p. In mathematical notation we get

$$\mathrm{S}[l] = \bigcup_{m=0}^{l} \nu(0, p(m)).$$

(h) $\mathrm{F}[l] \equiv \forall k(\mathrm{PRIME}(k) \leftrightarrow \exists m(m \leq l \wedge k = p(m)))$.
$\mathrm{F}[l]$ is a formula which asserts that there are only $l + 1$ primes, namely $\{p(0), \ldots, p(l)\}$.

(i) $\mathrm{O}(X) \equiv \forall m(m \in X \rightarrow \exists l\ \nu(m, l + 1) \subseteq X)$.

(j) $\mathrm{C}(X) \equiv \mathrm{O}(\overline{X})$.

(k) $\infty(X) \equiv \forall k \exists l\ k + l + 1 \in X$.

translation to schema of first-order proofs:

Take two-sorted (individuals, sets) first-order logic.
(a), (b) and (c) can be taken over. For the others we get:

(d') $x \subseteq y \equiv \forall n(n \in x \rightarrow n \in y)$, and
$x = y \equiv x \subseteq y \wedge y \subseteq x$.

(e') $n \in \overline{x} \equiv n \notin x$.

(f') Instead of p we introduce a finite set $\mathrm{P}[k]$ defined by

$$\mathrm{P}[k] \equiv \{p_0\} \cup \cdots \cup \{p_k\}.$$

(g') $\mathrm{S}[k] \equiv \nu(0, p_0) \cup \cdots \cup \nu(0, p_k)$.

(h') $\mathrm{F}[k] \equiv \forall m(\mathrm{PRIME}(m) \leftrightarrow m \in \mathrm{P}[k])$.

(i') $\mathrm{O}(x) \equiv \forall m(m \in x \rightarrow \exists l\ \nu(m, l+1) \subseteq x)$.

(j') $\mathrm{C}(x) \equiv \mathrm{O}(\overline{x})$.

(k') $\infty(x) \equiv \forall k \exists l\ k + l + 1 \in x$.

An analysis of Fürstenberg's proof

- avoid (further) inductions!
- introduce three axioms provable in Peano arithmetic:
  1. Every number greater than 0 has a predecessor,
  2. every number is in a remainder class modulo l for some l,
  3. every number has a prime divisor.

(1) $\mathrm{PRE} \equiv \forall k(0 < k \to \exists m\ k = m + 1)$

(2) $\mathrm{REM} \equiv \forall l(0 < l \to \forall m \exists k(k < l \land m \in \nu(k, l)))$

(3) $\text{PRIME-DIV} \equiv \forall m(m \neq 1 \to \exists l(\mathrm{PRIME}(l) \land \mathrm{DIV}(l, m)))$

proof schema $\varphi_1(k)$ (lemmas proving that $\{1\}$ is open):

$$\varphi_1(k) :=$$

$$\dfrac{\dfrac{\begin{array}{c}\psi_{1,k}(k)\\ \vdots \\ \mathrm{F}[k], \text{PRIME-DIV} \vdash \mathrm{S}[k] = \overline{\{1\}}\end{array} \quad \begin{array}{c}\psi_{2,k}(k)\\ \vdots \\ \mathrm{F}[k], \mathrm{PRE}, \mathrm{REM} \vdash \mathrm{C}(\mathrm{S}[k])\end{array}}{\mathrm{F}[k], \Gamma \vdash \mathrm{C}(\overline{\{1\}})} =: r \qquad \begin{array}{c}\vdots \\ \mathrm{C}(\overline{\{1\}}) \vdash \mathrm{O}(\{1\})\end{array}}{\mathrm{F}[k], \Gamma \vdash \mathrm{O}(\{1\})} \ cut$$

For $\Gamma = \mathrm{F}[k], \text{PRIME-DIV}, \mathrm{PRE}, \mathrm{REM}$.

$\mathrm{S}[k] \equiv \nu(0, p_0) \cup \cdots \cup \nu(0, p_k)$.

$\mathrm{F}[k] \equiv \forall m(\mathrm{PRIME}(m) \leftrightarrow m \in \mathrm{P}[k])$.

An analysis of Fürstenberg's proof

Main proof schema:

$\varphi(k) :=$

$$
\begin{prooftree}
\AxiomC{$\vdots$}
\noLine
\UnaryInfC{$\vdash \{1\} \neq \emptyset$}
\AxiomC{$\varphi_1(k)$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathrm{F}[k], \Gamma \vdash \mathrm{O}(\{1\})$}
\AxiomC{φ_2}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\vdash \forall x((\mathrm{O}(x) \land x \neq \emptyset) \to \infty(x))$}
\AxiomC{$\vdots$}
\noLine
\UnaryInfC{$\therefore$}
\RightLabel{cut}
\BinaryInfC{$\mathrm{O}(\{1\}), \{1\} \neq \emptyset \vdash \infty(\{1\})$}
\RightLabel{cut}
\BinaryInfC{$\{1\} \neq \emptyset, \mathrm{F}[k], \Gamma \vdash \infty(\{1\})$}
\RightLabel{cut}
\BinaryInfC{$\mathrm{F}[k], \Gamma \vdash \infty(\{1\})$}
\AxiomC{$\vdots$}
\noLine
\UnaryInfC{$\infty(\{1\}) \vdash$}
\RightLabel{cut}
\BinaryInfC{$\mathrm{F}[k], \Gamma \vdash$}
\RightLabel{$\neg : r$}
\UnaryInfC{$\underbrace{\text{PRIME-DIV}, \mathrm{PRE}, \mathrm{REM}}_{\Gamma} \vdash \neg \mathrm{F}[k]$}
\end{prooftree}
$$

$$\mathrm{F}[k] \equiv \forall m(\mathrm{PRIME}(m) \leftrightarrow m \in \mathrm{P}[k]).$$

An analysis of Fürstenberg's proof

the characteristic clause sets of the schema:
after tautology elimination and subsumption

$$\mathrm{CL}_r := \mathcal{C}_r \cup \mathrm{AX} \text{ where } \mathcal{C}_r := A \cup \bigcup_{i=0}^{r} B_i \cup \{C_r\} \text{ for}$$

$$C_r := \ \vdash m_0 = 1, s_1(m_0) = p_0, \ldots, s_1(m_0) = p_r,$$

$B_i :=$

$$0 < p_i \vdash p_i = s_7(p_i) + 1$$
$$0 < p_i \vdash t_0 = s_5(p_i, t_0) + (s_6(p_i, t_0) * p_i)$$
$$0 < p_i, s_5(p_i, t_0) = 0 \vdash t_0 = 0 + (s_6(p_i, t_0) * p_i)$$
$$0 < p_i \vdash s_5(p_i, t_0) < p_i$$
$$t_0 = p_i, m_0 * n_0 = t_0 \vdash m_0 = 1, m_0 = t_0$$
$$t_0 = p_i \vdash 1 < t_0$$
$$t_0 = p_i, 1 = n_0 * t_0 \vdash$$

An analysis of Fürstenberg's proof

$A :=$

$$\vdash m_0 = 1, s_1(m_0) * s_4(m_0) = m_0$$

$$\vdash m_0 + (((k * (l_0 + (1 + 1))) + (l_0 * (m_0 + 1))) + 1) = k + ((k + (m_0 + 1)) * (l_0 + 1))$$

$$m_0 = k_0 + (r_0 * ((t_0 + 1) * (t_1 + 1))) \vdash m_0 = k_0 + ((r_0 * (t_0 + 1)) * (t_1 + 1))$$

$$m_0 = k_0 + (r_0 * ((t_0 + 1) * (t_1 + 1))) \vdash m_0 = k_0 + ((r_0 * (t_1 + 1)) * (t_0 + 1))$$

$$\vdash (((t_0 + 1) * t_1) + t_0) + 1 = (t_0 + 1) * (t_1 + 1)$$

An analysis of Fürstenberg's proof

resolution refutation schema for CL_r defined.

- obtained $E_r \colon 1 < t_r \vdash$
  for $t_r = p_0 * \ldots * p_r + 1$
- transform $t_r = p_0 * \ldots * p_r + 1$ into $E'_r \colon 1 < (s_r + 1) + 1 \vdash$
  for some term s_r by resolution and paramodulation.
- derive $G \colon \ \vdash 1 < (w + 1) + 1$.
- G and E'_r resolve to $\vdash$. contradiction!
- Euclid's construction obtained by unification in the resolution calculus!

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, S. Hetzl, A. Leitsch, C. Richter, H. Spohr: CERES: An Analysis of Fürstenberg's Proof of the Infinity of Primes. *Theoretical Computer Science*, 403 (2–3), pp. 160-175, 2008.

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/`

Thank you for your attention!