COMPUTATIONAL ANALYSIS OF PROOFS

CERES: Cut-Elimination by Resolution

Gentzen-type methods of cut-elimination:

- reduction of cut-complexity.
- “peeling” the cut-formulas from outside.

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.
- application to complex proofs impossible in practice

Example of a Gentzen reduction:

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

rank = 3, grade = 1.

reduce to rank = 2, grade = 1:

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

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

rank = 2, grade = 1.

reduce to grade = 0, rank = 3:

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

eliminate cut with axiom:

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

Cut-elimination by Resolution (CERES):

based on a structural (algebraic) analysis of **LK**-proofs.

sub-derivation into cuts

φ

sub-derivation into end sequent

$\Theta(\varphi)$: *characteristic clause term*,
carries substantial information on derivations of cut formulas.

$\Theta(\varphi) \Rightarrow \mathrm{CL}(\varphi)$ (*characteristic clause set*)

clause = atomic sequent.

sequent $= \Gamma \vdash \Delta$. Γ, Δ multisets of formulas

cut-elimination = reduction to *atomic cuts*.

C-Terms (Clause Terms):

Definition 1 (C-term)

- (Finite) sets of clauses are C-terms.
- If X, Y are C-terms then $(X \oplus Y)$ is a C-term.
- If X, Y are C-terms then $(X \otimes Y)$ is a C-term.

Definition 2 We define a mapping $|\ |$ from C-terms to sets of clauses in the following way:

$$\begin{aligned} |\mathcal{C}| &= \mathcal{C} \text{ for sets of clauses } \mathcal{C}, \\ |X \oplus Y| &= |X| \cup |Y|, \\ |X \otimes Y| &= |X| \times |Y|. \end{aligned}$$

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

and "$\circ$" denotes merging, i.e.

$(\Gamma \vdash \Delta) \circ (\Pi \vdash \Lambda) = \Gamma, \Pi \vdash \Delta, \Lambda$

for multisets $\Gamma, \Delta, \Pi, \Lambda$.

We define C-terms to be equivalent if the corresponding sets of clauses are equal, i.e. $X \sim Y$ iff $|X| = |Y|$.

The Method CERES:

Example:

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

$\varphi_1 =$

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

$\varphi_2 =$

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

$X_1 = \{P(u) \vdash\},\ X_2 = \{\vdash Q(u)\},$
$X_3 = \{\vdash P(a)\},\ X_4 = \{Q(v) \vdash\}.$

$Y_1 = X_1 \otimes X_2.$

$Y_2 = X_3 \oplus X_4.$

$\Theta(\varphi) = Y_1 \oplus Y_2 =$
$(\{P(u) \vdash\} \otimes \{\vdash Q(u)\}) \oplus (\{\vdash P(a)\} \oplus \{Q(v) \vdash\})$

$\mathsf{CL}(\varphi) = |\Theta(\varphi)| =$
$\{P(u) \vdash Q(u),\ \vdash P(a),\ Q(v) \vdash\}.$

Projection to $\mathrm{CL}(\varphi)$**:**

- Skip inferences leading to cuts.

- Obtain cut-free proof of end-sequent
  $+$ a clause in $\mathrm{CL}(\varphi)$.

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.

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

Skip inferences in φ_1 leading to cuts:

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

$\varphi(C_1) =$

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

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

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

next step:

- Construct an R-refutation γ of CL(φ),
- insert projections of φ into γ.

Let φ be the proof of

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

as defined above. Then

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

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

First we define a resolution refutation δ of CL(φ):

$$\dfrac{\dfrac{\vdash P(a) \qquad P(u) \vdash Q(u)}{\vdash Q(a)}\,R \qquad Q(v) \vdash}{\vdash}\,R$$

$R =$ atomic mix + most general unification.

ground projection γ of δ:

$$\dfrac{\dfrac{\vdash P(a) \qquad P(a) \vdash Q(a)}{\vdash Q(a)}\,R \qquad Q(a) \vdash}{\vdash}\,R$$

The ground substitution defining the ground projection is

$\sigma : \{u \leftarrow a, v \leftarrow a\}$.

Let $\chi_1 = \varphi(C_1)\sigma$,
$\chi_2 = \varphi(C_2)\sigma$ and
$\chi_3 = \varphi(C_3)\sigma$.

$B = (\forall x)(P(x) \rightarrow Q(x))$,

$C = (\exists y)(P(a) \rightarrow Q(y))$.

Then $\varphi(\gamma) =$

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

The problem of Skolemization:

CERES: end-sequents must be skolemized.
 no projections with strong variables in end-sequent.

example:

$\varphi =$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{P\alpha \vdash P\alpha \quad Q\alpha \vdash Q\alpha}{P\alpha, P\alpha \to Q\alpha \vdash Q\alpha} \to : l
}{P\alpha, (\forall x)(Px \to Qx) \vdash Q\alpha} \forall : l + p
}{(\forall x)Px, (\forall x)(Px \to Qx) \vdash Q\alpha} \forall : l
}{(\forall x)Px, (\forall x)(Px \to Qx) \vdash (\forall x)Qx} \forall : r
\quad
\dfrac{
\dfrac{
\dfrac{Q\beta \vdash Q\beta}{Q\beta \vdash Q\beta \vee R\beta)} \vee : r
}{(\forall x)Qx \vdash Q\beta \vee R\beta} \forall : l
}{(\forall x)Qx \vdash (\forall x)(Qx \vee Rx)} \forall : r
}{(\forall x)Px, (\forall x)(Px \to Qx) \vdash (\forall x)(Qx \vee R(x))} \mathit{cut}
$$

$\mathrm{CL}(\varphi) = \{\vdash Q\alpha;\ Q\beta \vdash\}.$

Skolemization of Proofs

a. skolemization of formulas:

Definition 3 (strong and weak quantifiers) If $(\forall x)$ occurs positively (negatively) in B then $(\forall x)$ is called a strong (weak) quantifier. If $(\exists x)$ occurs positively (negatively) in B then $(\exists x)$ is called a weak (strong) quantifier.

Skolemization *removes strong quantifiers.*

structural skolemization operator sk:

Definition 4 (skolemization) sk is a function which maps closed formulas into closed formulas; it is defined in the following way:

$$
\begin{aligned}
sk(F) &= F \\
&\quad \text{if } F \text{ does not contain strong quantifiers,} \\
&= sk(F_{(Qy)}\{y \leftarrow f(x_1, \ldots, x_n)\}) \\
&\quad \text{if } (Qy) \text{ is in the scope of the} \\
&\quad \text{weak quantifiers } (Q_1 x_1), \ldots, (Q_n x_n).
\end{aligned}
$$

where (Qy) is the first strong quantifier in F.

$F_{(Qy)} = F$ after omission of (Qy).

$f \in FS \cup CS$ and f not in F.

b. skolemization of sequents:

Definition 5 Let S be the sequent

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_m$$

where A_i, B_j are closed and

$$(A'_1 \wedge \ldots \wedge A'_n) \rightarrow (B'_1 \vee \ldots \vee B'_m)$$

be the structural skolemization of $(A_1 \wedge \ldots \wedge A_n) \rightarrow (B_1 \vee \ldots \vee B_m)$. Then

$$S' : A'_1, \ldots, A'_n \vdash B'_1, \ldots, B'_m$$

is called the *skolemization* of S.

Example: Let S be the sequent

$$(\forall x)(\exists y)P(x,y) \vdash (\forall x)(\exists y)P(x,y).$$

skolemization of S is S':

$$(\forall x)P(x, f(x)) \vdash (\exists y)P(c,y)$$

for $f \in \mathsf{FS}_1$ and $c \in \mathsf{CS}$.

Definition 6 Let φ be an arbitrary **LK**-proof. By $\|\varphi\|_l$ we denote the number of logical inferences and mixes (or cuts) in φ. Structural rules like weakening, contraction and permutation are not counted.

Proposition 1 *Let φ be an* **LK***-proof of S from an atomic axiom set $\mathcal{A}$. Then there exists a proof $sk(\varphi)$ of $sk(S)$ (the structural skolemization of S) from $\mathcal{A}$ s.t.* $\|sk(\varphi)\|_l \leq \|\varphi\|_l$.

Example: Let $\varphi =$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{P(c,\alpha) \vdash P(c,\alpha) \quad Q(\alpha) \vdash Q(\alpha)}{P(c,\alpha), P(c,\alpha) \rightarrow Q(\alpha) \vdash Q(\alpha)} \rightarrow: l + p : l}{P(c,\alpha) \rightarrow Q(\alpha), (\forall x)P(c,x) \vdash Q(\alpha)} \forall : l + p : l}{P(c,\alpha) \rightarrow Q(\alpha), (\forall x)P(c,x) \vdash (\exists y)Q(y)} \exists : r}{(\exists y)(P(c,y) \rightarrow Q(y)), (\forall x)P(c,x) \vdash (\exists y)Q(y)} \exists : l}{(\forall x)P(c,x), (\forall x)(\exists y)(P(x,y) \rightarrow Q(y)) \vdash (\exists y)Q(y)} \forall : l + p : l$$

Then $sk(\varphi) =$

$$\cfrac{\cfrac{\cfrac{\cfrac{P(c,f(c)) \vdash P(c,f(c)) \quad Q(f(c)) \vdash Q(f(c))}{P(c,f(c)), P(c,f(c)) \rightarrow Q(f(c)) \vdash Q(f(c))} \rightarrow: l + p : l}{P(c,f(c)) \rightarrow Q(f(c)), (\forall x)P(c,x) \vdash Q(f(c))} \forall : l + p : l}{P(c,f(c)) \rightarrow Q(f(c)), (\forall x)P(c,x) \vdash (\exists y)Q(y)} \exists : r}{(\forall x)P(c,x), (\forall x)(P(x,f(x)) \rightarrow Q(f(x))) \vdash (\exists y)Q(y)} \forall : l + p : l$$

$\|\varphi\|_l = 5$ and $\|sk(\varphi)\|_l = 4$.

Definition 7

- $\mathcal{SK}$ = set of all **LK**-derivations with skolemized end-sequents.

- $\mathcal{SK}_\emptyset$ = set of all cut-free proofs in $\mathcal{SK}$.

- $\mathcal{SK}^i$ = derivations in $\mathcal{SK}$ with cut-formulas of formula complexity $\leq i$. $\sharp$

Goal: reduction to derivations with only atomic cuts, i.e.

transform $\varphi \in \mathcal{SK}$ into $\psi \in \mathcal{SK}^0$.

first step: construction of the

characteristic C-term

Characteristic Terms:

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 *characteristic term* $\Theta(\varphi)$ inductively:

Let ν be the occurrence of an initial sequent S' in φ. Then

$$\Theta(\varphi)/\nu = S(\nu, \Omega)$$

where $S(\nu, \Omega)$ is the subsequent of S containing the ancestors of Ω.

Assume: $\Theta(\varphi)/\nu$ are already constructed for depth(ν) $\leq k$.

depth(ν) $= k + 1$:

(a) ν is the consequent of μ:
$\Theta(\varphi)/\nu = \Theta(\varphi)/\mu$.

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

(b1) The auxiliary formulas of X are *ancestors* of Ω, i.e. the formulas occur in $S(\mu_1, \Omega), S(\mu_2, \Omega)$:

(+) $\Theta(\varphi)/\nu = \Theta(\varphi)/\mu_1 \oplus \Theta(\varphi)/\mu_2$.

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

($\times$) $\Theta(\varphi)/\nu = \Theta(\varphi)/\mu_1 \otimes \Theta(\varphi)/\mu_2$.

$\Theta(\varphi) = \Theta(\varphi)/\nu$ where ν is the occurrence of the end-sequent.

Remark: If φ is a cut-free proof then there are no occurrences of cut formulas in φ and $\Theta(\varphi)$ is a product of $\{\vdash\}$. $\sharp$

Definition 8 (characteristic clause set)
Let φ be an **LK**-derivation and $\Theta(\varphi)$ be the characteristic term of φ. Then $\mathrm{CL}(\varphi)\colon |\Theta(\varphi)|$ is called the *characteristic clause set* of φ. $\sharp$

Proposition 2
*Let φ be an **LK**-derivation. Then $\mathrm{CL}(\varphi)$ is unsatisfiable.*

Projection:

Lemma 1
Let φ *be a deduction in* $\mathcal{SK}$ *of a sequent* S : $\Gamma \vdash \Delta$. *Let* $C\colon \bar{P} \vdash \bar{Q}$ *be a clause in* $\mathrm{CL}(\varphi)$. *Then there exists a deduction*

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

s.t.

$$\varphi(C) \in \mathcal{SK}_{\emptyset} \text{ and } l(\varphi(C)) \leq l(\varphi).$$

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

the remaining steps:

• Construct an R-refutation γ of CL(φ),

• insert the projections of φ into γ.

• add some contractions and obtain a proof with (only) atomic cuts.

(• eliminate the atomic cuts)

Complexity:

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!*

CERES:

main point of complexity: resolution proof.

φ: **LK**-proof of S.
Let γ be a resolution refutation of CL(φ).
Then there exists a proof ψ of S with (only) atomic cuts s.t.

$\|\psi\| \leq 2 * \|\gamma\| * \|\varphi\|$.

Moreover there exists a cut-free proof ψ' of S s.t.

$\|\psi'\| \leq 2^{d*\|\gamma\|*\|\varphi\|}$.

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 produces $\leq 2^{m*n}$ symbols.

- There is no nonelementary speed-up of CERES by Gentzen!

Characteristic Clause Terms and Cut-Reduction

Definition 9
Let θ be a substitution. We define the application of θ to C-terms as follows:

$$
\begin{aligned}
X\theta &= \mathcal{C}\theta \;\text{ if } X = \mathcal{C} \text{ for sets of clauses } \mathcal{C}, \\
(X \oplus Y)\theta &= X\theta \oplus Y\theta, \\
(X \otimes Y)\theta &= X\theta \times Y\theta.
\end{aligned}
$$

Definition 10
Let X, Y be C-terms. We define

$X \subseteq Y$ iff $|X| \subseteq |Y|$,

$X \sqsubseteq Y$ iff for all $C \in |Y|$ there exists a $D \in |X|$ s.t. $D \sqsubseteq C$,

$X \leq_s Y$ iff there exists a substitution θ with $X\theta = Y$,

$X \leq_{ss} Y$ iff $|X| \leq_{ss} |Y|$.

Remark:
$\sqsubseteq$ is the subclause-relation:
$C \sqsubseteq D$ iff there exists an E s.t. $C \circ E = D$.
$\leq_{ss}$ is the *subsumption* relation.

Lemma 2 *Let X, Y, Z be C-terms and $X \subseteq Y$. Then*

(1) $X \oplus Z \subseteq Y \oplus Z$,

(2) $Z \oplus X \subseteq Z \oplus Y$,

(3) $X \otimes Z \subseteq Y \otimes Z$,

(4) $Z \otimes X \subseteq Z \otimes Y$.

Lemma 3 *Let X, Y, Z be C-terms and $X \sqsubseteq Y$. Then*

(1) $X \oplus Z \sqsubseteq Y \oplus Z$,

(2) $Z \oplus X \sqsubseteq Z \oplus Y$,

(3) $X \otimes Z \sqsubseteq Y \otimes Z$,

(4) $Z \otimes X \sqsubseteq Z \otimes Y$.

Replacing subterms in a clause term preserves the relations $\subseteq$ and $\sqsubseteq$:

Lemma 4 *Let λ be an occurrence in a C-term X and $Y \preceq X.\lambda$ for $\preceq \in \{\subseteq, \sqsubseteq\}$. Then $X[Y]_\lambda \preceq X$.*

The point is:
$\subseteq, \sqsubseteq$ and $\leq_s$ are preserved under cut-reduction steps.

Together the define a relation $\triangleright$:

Definition 11 Let X and Y two C-terms. We define $X \triangleright Y$ if (at least) one of the following properties is fulfilled:

(a) $Y \subseteq X$ or

(b) $X \sqsubseteq Y$ or

(c) $X \leq_s Y$. $\sharp$

Remark: In general $Y \leq_s Z$ does not imply $X[Y]_\lambda \leq_s X[Z]_\lambda$, i.e. $\leq_s$ is not compatible with $\oplus$ and $\otimes$. Consider, for example, the terms

$$
\begin{aligned}
&Y = \{\vdash P(x)\},\ Z = \{\vdash P(f(x))\} \text{ and} \\
&X = \{\vdash Q(x)\} \otimes \{\vdash R(x)\}, \\
&X.\lambda = \{\vdash Q(x)\}.
\end{aligned}
$$

Clearly $Y \leq_s Z$. By replacement we obtain

$$
\begin{aligned}
X[Y]_\lambda &= \{\vdash P(x)\} \otimes \{\vdash R(x)\}, \\
X[Z]\lambda &= \{\vdash P(f(x))\} \otimes \{\vdash R(x)\}.
\end{aligned}
$$

Obviously $X[Y]_\lambda \not\leq_s X[Z]_\lambda$. $\sharp$

The reflexive transitive closure $\rhd^*$ of $\rhd$ can be considered as a
weak form of subsumption:

Proposition 3
Let X and Y be C-terms s.t.
$X \rhd^* Y$. Then $X \leq_{ss} Y$.

Note: The subsumption relation $\leq_{ss}$ is defined on sets of clauses by

$\mathcal{C} \leq_{ss} \mathcal{D} \leftrightarrow$
for all $D \in \mathcal{D}$ there is a $C \in \mathcal{C}$: $C \leq_{ss} D$.

$\Gamma \vdash \Delta \leq_{ss} \Pi \vdash \Lambda \leftrightarrow$
there exists a substitution θ s.t.
set($\Gamma\theta$) $\subseteq$ set(Π), set($\Delta\theta$) $\subseteq$ set(Λ).

Lemma 5 (main lemma)
Let φ, φ' be **LK***-derivations with $\varphi > \varphi'$ for a cut reduction relation $>$ based on $\mathcal{R}$. Then $\Theta(\varphi) \rhd \Theta(\varphi')$.*

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

$\mathcal{R} =$ set of cut-reduction rules extracted from Gentzen's proof (possibly extended by cut-projection rules).

Theorem 1
Let φ be an **LK***-deduction and ψ be a normal form of φ under a cut reduction relation $>$ based on $\mathcal{R}$. Then*

$$\Theta(\varphi) \ \leq_{ss} \ \Theta(\psi).$$

Proof: Use Lemma 5 and the facts

- $\rhd \subseteq \leq_{ss}$,
- $\leq_{ss}$ is transitive.

$\diamond$

Theorem 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 resolution refutation γ of* $\mathrm{CL}(\varphi)$ *s.t.*

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

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

Proof: $\Theta(\varphi) \leq_{ss} \Theta(\psi)$ and thus

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

By the subsumption principle, for every resolution refutation δ of $\mathrm{CL}(\psi)$ there exists a resolution refutation γ of $\mathrm{CL}(\varphi)$ with

$$\gamma \leq_{ss} \delta.$$

$\diamond$

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* CL(φ) *s.t.*

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

Proof: By Theorem 2 and the fact that $l(\mathrm{RES}(\psi))$ is at most exponential in $l(\psi)$. $\diamond$

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* χ *obtained from* φ *by CERES 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 CL(φ). $\diamond$

Corollary 3
Let φ *be an* **LK**-*derivation and* ψ *be a normal form of* φ *under Gentzen's or Tait's method (possibly extended by cut-projection rules). Then there exists a proof* χ *obtained from* φ *by CERES s.t.*

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

Proof: Gentzens and Tait's methods are based on $\mathcal{R}$. $\diamond$

Extensions of CERES:

(I) CERES-m.

For cut-elimination in Gentzen calculi for many-valued logics.

easy:
– generalization of clause terms.
– many-valued resolution.
– proof projections.

delicate:
skolemization and re-skolemization.

crucial: full contraction and weakening.

(II) CERES-e.

For cut-elimination in proofs with equality.

approach:

axioms include $A \vdash A$ and $\vdash s = s$.

extend **LK** to $\mathbf{LK}_{=}$ by paramodulation-type rules

$$\frac{\Gamma \vdash \Delta, s = t \quad A[s], \Gamma' \vdash \Delta'}{\Gamma, \Gamma', A[t] \vdash \Delta, \Delta'} =: l$$

example:

$$\dfrac{\dfrac{\vdash a = f(a,e) \quad \dfrac{P(a) \vdash P(a) \quad Q(a) \vdash Q(a)}{P(a) \to Q(a), P(a) \vdash Q(a)} \to: l}{\dfrac{P(f(a,e)) \to Q(a), P(a) \vdash Q(a)}{(\forall y)(P(f(a,y)) \to Q(a)), P(a) \vdash Q(a)} \forall : l} =: l}{(\forall x)(\forall y)(P(f(x,y)) \to Q(x)), P(a) \vdash Q(a)} \forall : l$$

CERES-e:

– characteristic term: analogous

– projections: analogous

– skolemization: unproblematic.

– resolution $\Rightarrow$ resolution $+$ paramodulation.

very useful in handling mathematical proofs!

main goal:

- Cut-elimination in real mathematical proofs.
Experiments with proof transformations.

Cut-elimination in classical logic is
– *not confluent:*
construct different elementary proofs
corresponding to a proof with lemmas.

Experiments: to be presented on Friday.

Cut Reduction Rules:

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

$$\psi > \psi'$$

where $\psi =$

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

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.

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

transforms to

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

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

3.113.33.

$$\dfrac{\dfrac{\begin{matrix}(\rho'[\alpha])\\ \Gamma \vdash \Delta, B^x_\alpha\end{matrix}}{\Gamma \vdash \Delta, (\forall x)B}\,\forall : r \qquad \dfrac{\begin{matrix}(\sigma')\\ B^x_t, \Pi \vdash \Lambda\end{matrix}}{(\forall x)B, \Pi \vdash \Lambda}\,\forall : l}{\Gamma, \Pi \vdash \Delta, \Lambda}\,cut((\forall x)B)$$

transforms to

$$\dfrac{\dfrac{\begin{matrix}(\rho'[t])\\ \Gamma \vdash \Delta, B^x_t\end{matrix} \qquad \begin{matrix}(\sigma')\\ B^x_t, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\,cut(B^x_t)}{\Gamma, \Pi \vdash \Delta, \Lambda}\,w :^*$$

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

$$\dfrac{\begin{array}{c}(\rho)\\ \Pi \vdash \Lambda\end{array} \qquad \dfrac{\begin{array}{c}(\sigma_1)\\ \Gamma \vdash \Delta, B\end{array} \quad \begin{array}{c}(\sigma_2)\\ \Gamma \vdash \Delta, C\end{array}}{\Gamma \vdash \Delta, B \wedge C}\wedge : r}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, B \wedge C}\, cut(A)$$

transforms to

$$\dfrac{\dfrac{\begin{array}{c}(\rho)\\ \Pi \vdash \Lambda\end{array} \quad \begin{array}{c}(\sigma_1)\\ \Gamma \vdash \Delta, B\end{array}}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, B}\, cut(A) \qquad \dfrac{\begin{array}{c}(\rho)\\ \Pi \vdash \Lambda\end{array} \quad \begin{array}{c}(\sigma_2)\\ \Gamma \vdash \Delta, C\end{array}}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta, C}\, cut(A)}{\Pi, \Gamma^*, \vdash \Lambda^*, \Delta, B \wedge C}\wedge : r$$

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

$$\dfrac{\overset{(\rho)}{\Pi \vdash \Lambda} \quad \dfrac{\overset{(\sigma_1)}{B, \Gamma \vdash \Delta} \quad \overset{(\sigma_2)}{C, \Gamma \vdash \Delta}}{B \vee C, \Gamma \vdash \Delta}\,\vee : l}{\Pi, (B \vee C)^*, \Gamma^* \vdash \Lambda^*, \Delta}\,cut(A)$$

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

We first define the proof τ:

$$\dfrac{\dfrac{\dfrac{\overset{(\rho)}{\Pi \vdash \Lambda} \quad \overset{(\sigma_1)}{B, \Gamma \vdash \Delta}}{B^*, \Pi, \Gamma^* \vdash \Lambda^*, \Delta}\,cut(A)}{B, \Pi, \Gamma^* \vdash \Lambda^*, \Delta}\,x \qquad \dfrac{\dfrac{\overset{(\rho)}{\Pi \vdash \Lambda} \quad \overset{(\sigma_2)}{C, \Gamma \vdash \Delta}}{C^*, \Pi, \Gamma^* \vdash \Lambda^*, \Delta}\,cut(A)}{C, \Pi, \Gamma^* \vdash \Lambda^*, \Delta}\,x}{B \vee C, \Pi, \Gamma^* \vdash \Lambda^*, \Delta}\,\vee : l$$

Note that, in case $A = B$ or $A = C$, the inference x is $w : l$; 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

$$\dfrac{\dfrac{\begin{matrix}(\rho) \\ \Pi \vdash \Lambda\end{matrix} \qquad \tau}{\Pi, \Pi^*, \Gamma^* \vdash \Lambda^*, \Lambda^*, \Delta}\, cut(A)}{\Pi, \Gamma^* \vdash \Lambda^*, \Delta}\, c :^*$$

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

$$\dfrac{\begin{matrix}(\psi_1)\\ \Pi \vdash \Sigma\end{matrix} \qquad \dfrac{\begin{matrix}(\chi_1)\\ \Gamma \vdash \Theta, B\end{matrix} \qquad \begin{matrix}(\chi_2)\\ C, \Delta \vdash \Lambda\end{matrix}}{B \rightarrow C, \Gamma, \Delta \vdash \Theta, \Lambda} \rightarrow: l}{\Pi, (B \rightarrow C)^*, \Gamma^*, \Delta^* \vdash \Sigma^*, \Theta, \Lambda}\, cut(A)$$

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:

$$\dfrac{\dfrac{\begin{matrix}(\psi_1)\\ \Pi \vdash \Sigma\end{matrix} \qquad \begin{matrix}(\chi_1)\\ \Gamma \vdash \Theta, B\end{matrix}}{\Pi, \Gamma^* \vdash \Sigma^*, \Theta, B}\, cut(A) \qquad \dfrac{\dfrac{\begin{matrix}(\psi_1)\\ \Pi \vdash \Sigma\end{matrix} \qquad \begin{matrix}(\chi_2)\\ C, \Delta \vdash \Lambda\end{matrix}}{C^*, \Pi, \Delta^* \vdash \Sigma^*, \Lambda}\, cut(A)}{C, \Pi, \Delta^* \vdash \Sigma^*, \Lambda}\, x}{B \rightarrow C, \Pi, \Gamma^*, \Pi, \Delta^* \vdash \Sigma^*, \Theta, \Sigma^*, \Lambda} \rightarrow: l$$

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:

$$
\dfrac{\begin{matrix}(\chi_1)\\ \Gamma \vdash \Theta, B\end{matrix} \qquad \dfrac{\dfrac{\begin{matrix}(\psi_1)\\ \Pi \vdash \Sigma\end{matrix} \qquad \begin{matrix}(\chi_2)\\ C, \Delta \vdash \Lambda\end{matrix}}{C^*, \Pi, \Delta^* \vdash \Sigma^*, \Lambda}\, cut(A)}{C, \Pi, \Delta^* \vdash \Sigma^*, \Lambda}\, x}{B \to C, \Gamma, \Pi, \Delta^* \vdash \Theta, \Sigma^*, \Lambda} \to: l
$$

Again we distinguish the cases $B \to C = A$ and $B \to C \neq A$ 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, vol. 29, 149–176 (2000).

M. Baaz, A. Leitsch: Towards a Clausal Analysis of Cut-elimination. Journal of Symbolic Computation (to appear).

M. Baaz, A. Leitsch: CERES in Many-valued Logics. Proc. LPAR 2004.

M. Baaz, S. Hetzl, A. Leitsch, C. Richter, H. Spohr: Cut-elimination: Experiments with CERES. LPAR 2004.

M. Baaz, A. Leitsch, G. Moser: System Description: CutRes 01, cut-elimination by resolution. CADE-16, LNAI vol. 1632, 212-216 (1999).

C. Richter: System demonstration: CERES. V.A. Steklov Mathematical Institute, Russian Academy of Sciences, Moscow 2004.

web site: http://www.logic.at/ceres/