Cut-Elimination

Matthias Baaz

Vienna University of Technology

the language of predicate logic: syntactic material

- infinite set of predicate symbols for every arity (notation P, Q, R, H, M),
- infinite set of function symbols for every arity (notation f, g, h),
- infinite set of constant symbols (notation a, b, c).
- variables:
  - infinite set of free variables V_f,
  - infinite set of bound variables V_b.
- logical connectives: $\wedge$, $\vee$, $\neg$, $\rightarrow$.
- quantifiers: $\forall$, $\exists$

the language of predicate logic: syntactic material

Notation:

- α, β for free variables,
- x, y, z for bound variables.

$$(\forall x)(H(x) \to M(x))$$

x: bound variable, H, M: unary predicate symbols.

the language of predicate logic: terms

terms and semi-terms:

We define the set of semi-terms inductively:

- bound and free variables are semi-terms,
- constants are semi-terms,
- if $t_1, \ldots, t_n$ are semi-terms and f is an n-place function symbol then $f(t_1, \ldots, t_n)$ is a semi-term.

Semi-terms which do not contain bound variables are called terms.

the language of predicate logic: terms

α, β: free variables,
x, y: bound variables,
f: two-place function symbol.
a: constant symbol.

- $f(\alpha, \beta)$ is a term,
- $f(x, \beta)$ is a semi-term,
- α, β, c are terms,
- x is a semi-term.

the language of predicate logic: formulas

If $t_1, \ldots, t_n$ are terms and P is an n-place predicate symbol then $P(t_1, \ldots, t_n)$ is a an (atomic) formula.

- If A is a formula then $\neg A$ is a formula.
- If A, B are formulas then $(A \to B)$, $(A \wedge B)$ and $(A \vee B)$ are formulas.
- If $A\{x \leftarrow \alpha\}$ is a formula then $(\forall x)A, (\exists x)A$ are formulas.
- Semi-formulas differ from formulas in containing free variables in V_b.

the language of predicate logic: formulas

P: one-place predicate symbol.
f: two-place function symbol.

$P(f(\alpha, \beta))$ is a formula, and so are

$$(\forall x)P(f(x, \beta)), \; (\exists y)(\forall x)P(f(x, y)).$$

$P(f(x, \beta))$ is a semi-formula.

sequents

Let Γ and Δ be finite (possibly empty) multisets of formulas.
$S : \Gamma \vdash \Delta$ is called a sequent.

$S : \Gamma \vdash \Delta$ is satisfied by ν_I iff there is a $A \in \Gamma$ with $\nu_I(A) = 0$ or if there is a $B \in \Delta$ with $\nu_I(B) = 1$.
(for classical logic)

$S : \Gamma \vdash \Delta$ is satisfied by ν_I iff $\nu_I(\bigwedge_{A \in \Gamma} A \rightarrow \bigvee_{B \in \Delta} B) = 1$
For $\Gamma = \emptyset$ the right side is identified with true, for $\Delta = \emptyset$ the left side is identified with false.
(classical logic and intuitionistic logic)

sequents

A sequent $A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ is called atomic if the A_i, B_j are atomic formulas.

If $S = \Gamma \vdash \Delta$ and $S' = \Pi \vdash \Lambda$ we define the composition of S and S' by $S \circ S'$, where

$$S \circ S' = \Gamma, \Pi \vdash \Delta, \Lambda.$$

where Γ, Π stands for the multiset union of Γ and Π.

Let Γ be a multiset of formulas.
Then we write $\Gamma - A$ for Γ after deletion of all occurrences of A.

Let S, S' be sequents. We define $S' \sqsubseteq S$ if there exists a sequent S'' s.t. $S' \circ S'' = S$ and call S' a subsequent of S.

the sequent calculus **LK**: axiom sets

A (possibly infinite) set $\mathcal{A}$ of sequents is called an axiom set if it is

- closed under substitution, i.e., for all $S \in \mathcal{A}$ and for all substitutions θ we have $S\theta \in \mathcal{A}$.
- If $\mathcal{A}$ consists only of atomic sequents we speak about an atomic axiom set.
- Let $\mathcal{A}_T$ be the smallest axiom set containing all sequents of the form $A \vdash A$ for arbitrary atomic formulas A. A_T is called the standard axiom set.

the sequent calculus **LK**: the rules

- inference rules of **LK** work on sequents.
- logical rules
- structural rules

A and B denote formulas, $\Gamma, \Delta, \Pi, \Lambda$ multisets of formulas.

In the rules we distinguish

- introducing or auxiliary formulas (in the premises) and
- introduced or principal formulas in the conclusion.
- notation: mark the auxiliary formulas occurrences by $+$ and the principal ones by $\star$.

the sequent calculus **LK**: the logical rules

- $\wedge$-introduction:

$$\frac{A^{+}, \Gamma \vdash \Delta}{(A \wedge B)^{\star}, \Gamma \vdash \Delta}\ \wedge\colon l_1 \quad \frac{B^{+}, \Gamma \vdash \Delta}{(A \wedge B)^{\star}, \Gamma \vdash \Delta}\ \wedge\colon l_2 \quad \frac{\Gamma \vdash \Delta, A^{+} \quad \Gamma \vdash \Delta, B^{+}}{\Gamma \vdash \Delta, (A \wedge B)^{\star}}\ \wedge\colon r$$

- $\vee$-introduction:

$$\frac{A^{+}, \Gamma \vdash \Delta \quad B^{+}, \Gamma \vdash \Delta}{(A \vee B)^{\star}, \Gamma \vdash \Delta}\ \vee\colon l \quad \frac{\Gamma \vdash \Delta, A^{+}}{\Gamma \vdash \Delta, (A \vee B)^{\star}}\ \vee\colon r_1 \quad \frac{\Gamma \vdash \Delta, B^{+}}{\Gamma \vdash \Delta, (A \vee B)^{\star}}\ \vee\colon r_2$$

- $\rightarrow$-introduction:

$$\frac{\Gamma \vdash \Delta, A^{+} \quad B^{+}, \Pi \vdash \Lambda}{(A \rightarrow B)^{\star}, \Gamma, \Pi \vdash \Delta, \Lambda}\ \rightarrow\colon l \qquad \frac{A^{+}, \Gamma \vdash \Delta, B^{+}}{\Gamma \vdash \Delta, (A \rightarrow B)^{\star}}\ \rightarrow\colon r$$

- $\neg$-introduction:

$$\frac{\Gamma \vdash \Delta, A^{+}}{\neg A^{\star}, \Gamma \vdash \Delta}\ \neg\colon l \qquad \frac{A^{+}, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A^{\star}}\ \neg\colon r$$

the sequent calculus **LK**: the logical rules

- $\forall$-introduction:

$$\frac{A\{x \leftarrow t\}^{+}, \Gamma \vdash \Delta}{(\forall x)A^{\star}, \Gamma \vdash \Delta}\ \forall\colon l$$

where t is an arbitrary term.

$$\frac{\Gamma \vdash \Delta, A\{x \leftarrow \alpha\}^{+}}{\Gamma \vdash \Delta, (\forall x)A^{\star}}\ \forall\colon r$$

where α is a free variable which may not occur in Γ, Δ, A. α is called an eigenvariable.

- The logical rules for $\exists$-introduction (variable conditions for $\exists : l$ as for $\forall\colon r$, similarly for $\exists : r$ and $\forall\colon l$):

$$\frac{A\{x \leftarrow \alpha\}^{+}, \Gamma \vdash \Delta}{(\exists x)A^{\star}, \Gamma \vdash \Delta}\ \exists\colon l \qquad \frac{\Gamma \vdash \Delta, A\{x \leftarrow t\}^{+}}{\Gamma \vdash \Delta, (\exists x)A^{\star}}\ \exists\colon r$$

the sequent calculus **LK**: the structural rules

- weakening:

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A^{\star}}\ w\colon r \qquad \frac{\Gamma \vdash \Delta}{A^{\star}, \Gamma \vdash \Delta}\ w\colon l$$

- contraction:

$$\frac{A^{+}, A^{+}, \Gamma \vdash \Delta}{A^{\star}, \Gamma \vdash \Delta}\ c\colon l \qquad \frac{\Gamma \vdash \Delta, A^{+}, A^{+}}{\Gamma \vdash \Delta, A^{\star}}\ c\colon r$$

the sequent calculus **LK**: the structural rules

- The **cut rule:**

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

  where $k, l \geq 1$ and A^k denotes $A, \ldots, A$ k-times.

- the mix rule: Π and Δ do not contain A.

LK-proofs

An **LK**-derivation is defined as a

- finite directed labeled tree,
- nodes are labeled by sequents (via the function *Seq*),
- edges labeled by the corresponding rule applications.
- label of the root is called the end-sequent.
- Sequents occurring at the leaves are called initial sequents or axioms.
- An **LK**-proof φ of S is an **LK**-derivation with end-sequent S from the set of standard axioms. If S is of the form $\vdash A$ for a formula A we also say that φ is a proof of A.

LK-proofs

Let φ be the **LK**-derivation

$$\dfrac{\dfrac{\nu_1 : P(a) \vdash P(a)}{\nu_2 : (\forall x)P(x) \vdash P(a)}\ \forall : l \qquad \dfrac{\nu_3 : P(a) \vdash Q(a)}{\nu_4 : P(a) \vdash (\exists x)Q(x)}\ \exists : r}{\dfrac{\nu_5 : (\forall x)P(x) \vdash (\exists x)Q(x)}{\nu_6 : \quad \vdash (\forall x)P(x) \to (\exists x)Q(x)}\ \to : r}\ \mathit{cut}$$

- The ν_i denote the nodes in φ.
- The leaf nodes are ν_1 and ν_3,
- the root is ν_6.
- $\mathit{Seq}(\nu_2) = (\forall x)P(x) \vdash P(a)$.

LK-proofs

prove the sentence

$$(H(s) \wedge (\forall x)(H(x) \to M(x))) \to M(s) \text{ in } \mathbf{LK}.$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{H(s) \vdash H(s) \quad M(s) \vdash M(s)}{H(s) \to M(s), H(s) \vdash M(s)}\ \to: l}{(\forall x)(H(x) \to M(x)), H(s) \vdash M(s)}\ \forall: l}{H(s) \wedge (\forall x)(H(x) \to M(x)), H(s) \vdash M(s)}\ \wedge: l_2}{H(s) \wedge (\forall x)(H(x) \to M(x)), H(s) \wedge (\forall x)(H(x) \to M(x)) \vdash M(s)}\ \wedge: l_1}{H(s) \wedge (\forall x)(H(x) \to M(x)) \vdash M(s)}\ c: l}{\vdash (H(s) \wedge (\forall x)(H(x) \to M(x))) \to M(s)}\ \to: r$$

on the role of contraction

In the proof of

$$(P(a) \wedge (\forall x)(P(x) \to P(f(x)))) \to P(f(f(a)))$$

we need two copies of the formula $(\forall x)(P(x) \to P(f(x)))$:

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

the role of cut

proof with cut:

$$\dfrac{\dfrac{\dfrac{\dfrac{Pa \vdash Pa \qquad Qa \vdash Qa}{Pa, Pa \to Qa \vdash Qa}\ \to : l}{Pa, Pa \to Qa \vdash \exists x.Qx}\ \exists : r}{Pa, \forall x(Px \to Qx) \vdash \exists x.Qx}\ \forall : l \qquad \dfrac{\dfrac{\dfrac{\dfrac{Q\alpha \vdash Q\alpha \qquad R\alpha \vdash R\alpha}{Q\alpha, Q\alpha \to R\alpha \vdash R\alpha}\ \to : l}{Q\alpha, Q\alpha \to R\alpha \vdash \exists x.Rx}\ \exists : r}{Q\alpha, \forall x(Qx \to Rx) \vdash \exists x.Rx}\ \forall : l}{\exists x.Qx, \forall x(Qx \to Rx) \vdash \exists x.Rx}\ \exists : l}{Pa, \forall x(Px \to Qx), \forall x(Qx \to Rx) \vdash \exists x.Rx}\ cut$$

proof without cut:

$$\dfrac{\dfrac{\dfrac{\dfrac{etc.}{Pa, Pa \to Qa, Qa \to Ra \vdash Ra}}{Pa, Pa \to Qa, Qa \to Ra \vdash\vdash \exists x.Rx}\ \exists : r}{Pa, Pa \to Qa, \forall x(Qx \to Rx) \vdash \exists x.Rx}\ \forall : l}{Pa, \forall x(Px \to Qx), \forall x(Qx \to Rx) \vdash \exists x.Rx}\ \forall : l$$

cut-elimination: the Hauptsatz

Gerhard Gentzen, 1935:

Every sequent provable in **LK** is also provable without the cut rule.

- proof by double induction on rank and grade.
- stricly speaking the method eliminates mix.
- Proofs with cut-rules and proofs with mix rules polynomially simulate each other.

grade of a cut

Let ψ be a cut-derivation of the form

$$\dfrac{\begin{matrix}(\psi_1)\\ \Gamma_1 \vdash \Delta_1\end{matrix} \quad \begin{matrix}(\psi_2)\\ \Gamma_2 \vdash \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2^* \vdash \Delta_1^*, \Delta_2}\ cut(A)$$

- then we define the grade of ψ as $comp(A)$ - the logical complexity of A.
- We write $cut(A)$ for the mix on A: Δ_1^*, Γ_2^* do not contain A.

rank of a cut

Let ψ be a cut-derivation of the form

$$\dfrac{\overset{(\psi_1)}{\Gamma_1 \vdash \Delta_1} \quad \overset{(\psi_2)}{\Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2^* \vdash \Delta_1^*, \Delta_2}\ cut(A)$$

- μ be the root node of ψ_1,
- ν be the root node of ψ_2.
- An A-right path in ψ_1 is a path in ψ_1 of the form $\mu, \mu_1, \ldots, \mu_n$ s.t. A occurs in the consequents of all $Seq(\mu_i)$ (note that A clearly occurs in Δ_1).
- an A-left path in ψ_2 is a path in ψ_2 of the form $\nu, \nu_1, \ldots, \nu_m$ s.t. A occurs in the antecedents of all $Seq(\nu_j)$.

rank of a cut

Let ψ be a cut-derivation of the form

$$\dfrac{\begin{matrix}(\psi_1)\\ \Gamma_1 \vdash \Delta_1\end{matrix} \quad \begin{matrix}(\psi_2)\\ \Gamma_2 \vdash \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2^* \vdash \Delta_1^*, \Delta_2}\ cut(A)$$

- Let P_1 be the set of all A-right paths in ψ_1 and
- P_2 be the set of all A-left paths in ψ_2.

Then we define the left-rank of ψ $(\mathrm{rank}_l(\psi))$
and the right-rank of ψ $(\mathrm{rank}_r(\psi))$ as

$$\begin{aligned}\mathrm{rank}_l(\psi) &= \max\{lp(\pi) \mid \pi \in P_1\} + 1,\\ \mathrm{rank}_r(\psi) &= \max\{lp(\pi) \mid \pi \in P_2\} + 1.\end{aligned}$$

The rank of ψ is the sum of right-rank and left-rank, i.e.

$$\mathrm{rank}(\psi) = \mathrm{rank}_l(\psi) + \mathrm{rank}_r(\psi).$$

principle of Gentzen's proof

given proof φ.

- select an uppermost cut-derivation ψ in φ;
- if $\mathrm{rank}(\psi) = 2$ select a grade reduction rule;
- if $\mathrm{rank}(\psi) > 2$ select a rank reduction rule;
- after this reduction either
  - the grade is reduced, but the rank may increase,
  - the rank is reduced, but the grade does not increase.

induction on tupel odering on $\mathbb{N} \times \mathbb{N}$ s.t.

$$(i, j) < (k, l) \text{ iff either } i < k \text{ or } i = k \text{ and } j < l.$$

Cut Reduction Rules

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

$$\psi > \psi'$$

where $\psi =$

$$\dfrac{\begin{matrix}(\rho) \\ \Gamma \vdash \Delta\end{matrix} \qquad \begin{matrix}(\sigma) \\ \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\ \mathit{cut}$$

Cut Reduction Rules

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.

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

transforms to

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

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

Cut Reduction Rules

3.113.33.

$$\dfrac{\dfrac{\overset{(\rho'[\alpha])}{\Gamma \vdash \Delta, B\{x \leftarrow \alpha\}}}{\Gamma \vdash \Delta, (\forall x)B}\ \forall\colon r \qquad \dfrac{\overset{(\sigma')}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{(\forall x)B, \Pi \vdash \Lambda}\ \forall\colon l}{\Gamma, \Pi \vdash \Delta, \Lambda}\ cut((\forall x)B)$$

transforms to

$$\dfrac{\dfrac{\overset{(\rho'[t])}{\Gamma \vdash \Delta, B\{x \leftarrow t\}} \qquad \overset{(\sigma')}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\ cut(B\{x \leftarrow t\})}{\Gamma, \Pi \vdash \Delta, \Lambda}\ w:^*$$

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

Cut Reduction Rules: rank reduction

3.12. rank > 2:

3.121. right-rank > 1:

Cut Reduction Rules: rank reduction

3.121.1. The cut formula occurs in Γ.

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

transforms to

$$\dfrac{\begin{array}{c}(\sigma)\\ \Pi \vdash \Lambda\end{array}}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\ s^*$$

Cut Reduction Rules: rank reduction

3.121.2. The cut formula does not occur in Γ.

3.121.21. Let ξ be one of the rules $w\colon l$ or $c\colon l$; then

$$\dfrac{\begin{matrix}(\rho)\\ \Gamma \vdash \Delta\end{matrix} \qquad \dfrac{\begin{matrix}(\sigma')\\ \Sigma \vdash \Lambda\end{matrix}}{\Pi \vdash \Lambda}\,\xi}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\,cut(A)$$

transforms to

$$\dfrac{\dfrac{\begin{matrix}(\rho)\\ \Gamma \vdash \Delta\end{matrix} \qquad \begin{matrix}(\sigma')\\ \Sigma \vdash \Lambda\end{matrix}}{\Gamma, \Sigma^* \vdash \Delta^*, \Lambda}\,cut(A)}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\,s^*$$

Note that the sequence of structural rules s^* may be empty, i.e. it can be skipped if the sequent does not change.

Cut Reduction Rules: rank reduction

3.121.22. Let ξ be an arbitrary unary rule (different from $c\colon l, w\colon l$) and let C^* be empty if $C = A$ and C otherwise. The formulas B and C may be equal or different or simply nonexisting (in case ξ is a right rule). Let us assume that ψ is of the form

$$\dfrac{\begin{array}{c}(\rho)\\ \Gamma \vdash \Delta\end{array} \quad \dfrac{\begin{array}{c}(\sigma')\\ B, \Pi \vdash \Sigma\end{array}}{C, \Pi \vdash \Lambda}\,\xi}{\Gamma, C^*, \Pi^* \vdash \Delta^*, \Lambda}\,cut(A)$$

Let τ be the proof

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}(\rho)\\ \Gamma \vdash \Delta\end{array} \quad \begin{array}{c}(\sigma')\\ B, \Pi \vdash \Sigma\end{array}}{\Gamma, B^*, \Pi^* \vdash \Delta^*, \Sigma}\,cut(A)}{\Gamma, B, \Pi^* \vdash \Delta^*, \Sigma}\,s^*}{\Gamma, C, \Pi^* \vdash \Delta^*, \Lambda}\,\xi + s^*$$

Cut Reduction Rules: rank reduction

3.121.221. $A \neq C$, including the case that ξ is a right rule and B, C do not exist at all: then ψ transforms to τ.

3.121.222. $A = C$ and $A \neq B$: in this case C is the principal formula of ξ. Then ψ transforms to

$$\dfrac{\dfrac{\overset{(\rho)}{\Gamma \vdash \Delta} \qquad \overset{(\tau)}{\Gamma, A, \Pi^* \vdash \Delta^*, \Lambda}}{\Gamma, \Gamma^*, \Pi^* \vdash \Delta^*, \Delta^*, \Lambda}\ cut(A)}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\ s^*$$

3.121.223. $A = B = C$. Then $\Sigma \neq \Lambda$ and ψ transforms to

$$\dfrac{\dfrac{\overset{(\rho)}{\Gamma \vdash \Delta} \qquad \overset{(\sigma')}{A, \Pi \vdash \Sigma}}{\Gamma, \Pi^* \vdash \Delta^*, \Sigma}\ cut(A)}{\Gamma, \Pi^* \vdash \Delta^*, \Lambda}\ \xi$$

Cut Reduction Rules: rank reduction, a special case

$$\dfrac{\overset{(\rho)}{\Gamma \vdash \Delta, (\forall x)A(x)} \qquad \dfrac{\overset{(\sigma')}{A(t), (\forall x)A(x), \Pi \vdash \Lambda}}{(\forall x)A(x), (\forall x)A(x), \Pi \vdash \Lambda}\ \forall\colon l}{\Gamma, \Pi \vdash \Delta, \Lambda}\ cut$$

$$\dfrac{\overset{(\rho)}{\Gamma \vdash \Delta, (\forall x)A(x)} \qquad \dfrac{\dfrac{\overset{(\rho)}{\Gamma \vdash \Delta, (\forall x)A(x)} \qquad \overset{(\sigma')}{A(t), (\forall x)A(x), \Pi \vdash \Lambda}}{\Gamma, A(t), \Pi \vdash \Delta, \Lambda}\ cut}{(\forall x)A(x), \Gamma, \Pi \vdash \Delta, \Lambda}\ \forall\colon l + *}{\Gamma, \Pi \vdash \Delta, \Lambda}\ cut + *$$

Cut Reduction Rules: rank reduction

3.121.23. The last inference in σ is binary:

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

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

transforms to

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

Cut Reduction Rules: rank reduction

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

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

$(B \vee C)^*$ is empty if $A = B \vee C$ and $B \vee C$ otherwise.
We first define the proof τ:

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

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.

Cut Reduction Rules: rank reduction

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

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

Cut Reduction Rules: rank reduction

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

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

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

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

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

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

Cut Reduction Rules: rank reduction

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

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

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.

Example of a Gentzen reduction

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

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

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

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

Example of a Gentzen reduction

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

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

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

Example of a Gentzen reduction

$\mathrm{grade} = 0, \;\; \mathrm{rank} = 3$:

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

eliminate cut with axiom:

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

An application of cut-elimination: Herbrand's theorem

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 $(\forall x_{1,i}) \ldots (\forall x_{k_i,i})$ and F_i, G_j are quantifier-free. 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 $(\forall x_{1,i}) \ldots (\forall x_{k_i,i})$ and F_i, G_j are quantifier-free. 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 these instances.
- then S^* is a Herbrand sequent.

construction of a Herbrand sequent: example

proof:

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

extracted Herbrand sequent:

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

an application of cut-elimination: interpolation

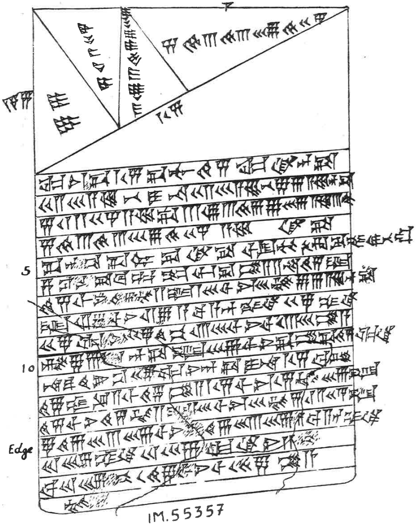
Theorem.

Let $\Pi_1, \Pi_2 \vdash \Gamma_1, \Gamma_2$ be any partition of the derivable sequent $\Pi \vdash \Gamma$. There is an interpolant I containing only function symbols and predicate symbols both in P_1, Γ_1 (P_2, Γ_2).

Proof.

Lemma of Maehara.

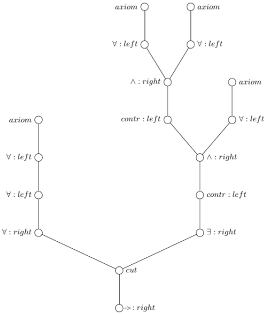
an application of cut-elimination: generalization of proofs



an application of cut-elimination: generalization of proofs

Definition

The skeleton of an LK-proof is a tree of names of rule applications.



$\vdash \forall x \forall y P(x,y) \rightarrow \exists z (P(0,z) \wedge P(z,a) \wedge P(Sz,Sa))$.

There is a proof underlying this representation by name iff a is replaced by $S^{2n}(0)$.

an application of cut-elimination: generalization of proofs

Theorem.
For every skeleton S and every parametrized end-sequent $\lambda\vec{x}S(\vec{x})$ there is a most general term-minimal proof of $S(\vec{t})$ if there is any proof of the same skeleton of $S(\vec{t'}$ for some $\vec{t'}$.

Corollary.
If $\vdash A(s(n(0)))$ is shortly derivable for sufficiently big n then $\vdash \forall x A(s(n(x)))$ is derivable.

the calculus LJ

LJ is defined exactly as LK, only that $|\Delta| \leq 1$ in $\Gamma \vdash \Delta$.

Same Hauptsatz, same proof.

Proposition

$\vdash A$ is derivable in LJ if A is derivable in intuitionistic logic.

Corollary

Intuitionistic propositional logic is decidable.

the calculus LJ

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A \vee \neg A}\ \vee : r1}{\neg(A \vee \neg A), A}\ \neg : l}{\neg(A \vee \neg A) \vdash \neg A}\ \neg : r}{\neg(A \vee \neg A) \vdash A \vee \neg A}\ \vee : r2}{\neg(A \vee \neg A), \neg(A \vee \neg A) \vdash}\ \neg : l}{\neg(A \vee \neg A) \vdash}\ c : l}{\vdash \neg\neg(A \vee \neg A)}\ \neg : r
$$

n-valued logics

Represented by *n*-sided sequents.

Example: 3-valued Gödel logic implication

$\to$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	1	1
1	0	$\frac{1}{2}$	1

$$\nu_I(A \to B) = 0 \quad (\nu_I(A) = 1 \vee \nu_I(A) = \frac{1}{2}) \text{ and } \nu_I(B) = 0$$

$$\frac{\Pi | \Gamma, A | \Delta, A \qquad \Pi, B | \Gamma | \Delta}{\Pi, A \to B | \Gamma | \Delta} \to : 0$$

$$\nu_I(A \to B) = \frac{1}{2} \quad \nu_I(A) = 1 \text{ and } \nu_I(B) = \frac{1}{2}$$

$$\frac{\Pi | \Gamma | \Delta, A \qquad \Pi | \Gamma, B | \Delta}{\Pi | \Gamma, A \to B | \Delta} \to : \tfrac{1}{2}$$

n-valued logics

$$\nu_I(A \to B) = 1 \quad \mathit{not}(((\nu_I(A) = 1 \text{ or } \nu_I(A) = \frac{1}{2}) \text{ or}$$

$$((\nu_I(A) = 1 \text{ and } \nu_I(B) = \frac{1}{2}) \text{ or } \nu_I(B) = 0$$

$$\Downarrow$$

$$\nu_I(A) = 0 \text{ or } \nu_I(B) = \frac{1}{2} \text{ or } \nu_I(B) = 1$$

and

$$\nu_I(A) = 0 \text{ or } \nu_I(A) = \frac{1}{2} \text{ or } \nu_I(B) = 1$$

$$\frac{\Pi, A|\Gamma, B|\Delta, B \qquad \Pi, A|\Gamma, A|\Delta, B}{\Pi|\Gamma|\Delta, A \to B}\; 1 : A \to B$$

structural rules

axioms $A|A|A \vdash A|A|A$

weakening, contraction obvious.

$$\frac{\Pi, A|\Gamma|\Delta \qquad \Pi'|\Gamma', A|\Delta'}{\Pi, \Pi'|\Gamma, \Gamma'|\Delta, \Delta'} \text{cut}$$

$$\frac{\Pi, A|\Gamma|\Delta \qquad \Pi'|\Gamma'|\Delta', A}{\Pi, \Pi'|\Gamma, \Gamma'|\Delta, \Delta'} \text{cut}$$

$$\frac{\Pi|\Gamma|\Delta, A \qquad \Pi', A|\Gamma'|\Delta'}{\Pi, \Pi'|\Gamma, \Gamma'|\Delta, \Delta'} \text{cut}$$

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:

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

  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.

the origin of complexity

$$
\cfrac{\cfrac{\cfrac{\cfrac{\overline{P(a) \to P(f^n(a)), P(f^n(a)) \to P(f^{2n}(a)) \vdash P(a) \to P(f^{2n}(a))}}{P(a) \to P(f^n(a)), \forall x(P(x) \to P(f^n(x))) \vdash P(a) \to P(f^{2n}(a))}}{\forall x(P(x) \to P(f^n(x))), \forall x(P(x) \to P(f^n(x))) \vdash P(a) \to P(f^{2n}(a))}}{\forall x(P(x) \to P(f^n(x))) \vdash P(a) \to P(f^{2n}(a))}}{\forall x(P(x) \to P(f^n(x))) \vdash \forall x(P(x) \to P(f^{2n}(x)))}
$$

derive $\forall x(P(x) \to P(f(x))) \vdash \forall x(P(x) \to P(f^{2n}(x)))$

limits of complexity

Theorem

For fixed k there is an elementary procedure that eliminates cuts from proofs with $\leq k$ iterated quantifiers in the cuts.

Cut-Elimination

Matthias Baaz

Vienna University of Technology

skolemization of formulas

- idea of skolemization: eliminate quantifiers with eigenvariable conditions, so-called strong quantifiers.
- strong quantifier: $\forall$ in positive, $\exists$ in negative occurrence,
- weak quantifier: $\forall$ in negative, $\exists$ in positive occurrence.

Examples:

- $(\forall x)(\exists y)P(x,y)$: $\forall x$ strong, $\exists y$ weak.
- $\neg(\forall x)(\exists y)P(x,y)$: $\forall x$ weak, $\exists y$ strong.
- $(\forall z)((\forall x)Q(x,z) \to (\forall y)R(y,z))$: $\forall z$, $\forall y$: strong, $\forall x$: weak.

skolemization of formulas

sk: closed formulas → closed formulas; eliminates strong quantifiers. it is defined in the following way:

$$sk(F) \;=\; F \quad \text{if } F \text{ does not contain strong quantifiers.}$$

Otherwise take (Qy) - the first strong quantifier in F which is in the scope of the weak quantifiers $(Q_1x_1), \ldots, (Q_nx_n)$. Let f be an n-ary function symbol not occurring in F (f is a constant symbol for $n = 0$). Then $sk(F)$ is defined inductively as

$$sk(F) \;=\; sk(F_{(Qy)}\{y \leftarrow f(x_1, \ldots, x_n)\}).$$

where $F_{(Qy)}$ is F after omission of (Qy). $sk(F)$ is called the (structural) Skolemization of F.

skolemization of formulas: examples

- $sk((\forall x)(\exists y)P(x,y)) = (\exists y)P(c,y)$,
- $sk(\neg(\forall x)(\exists y)P(x,y)) = \neg(\forall x)P(x,f(x))$,
- $sk((\forall z)((\forall x)Q(x,z) \rightarrow (\forall y)R(y,z))) =$
  $((\forall x)Q(x,c) \rightarrow R(d,c))$.
- $sk(\neg((\exists x)P(x) \wedge (\exists y)\neg P(y))) = \neg(P(c) \wedge P(d))$.

skolemization of sequents

Let S be the sequent
$A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ consisting of closed formulas only and

$$sk((A_1 \wedge \ldots \wedge A_n) \rightarrow (B_1 \vee \ldots \vee B_m)) =$$
$$(A'_1 \wedge \ldots \wedge A'_n) \rightarrow (B'_1 \vee \ldots \vee B'_m).$$

Then the sequent

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

is called the Skolemization of S.

example:

$S = (\forall x)(\exists y)P(x, y) \vdash (\forall x)(\exists y)P(x, y)$. Then the Skolemization of S is

$$S' : \; (\forall x)P(x, f(x)) \vdash (\exists y)P(c, y).$$

skolemization of proofs

- Skolemized proof: proof of the Skolemized end sequent.
- construction by ommitting strong quantifier introductions and by replacing eigenvariables.
- also proofs with cuts can be Skolemized, but the cut formulas themselves cannot!
- Only the strong quantifiers which are ancestors of the end sequent are eliminated.
- skolemization does not increase the number of inferences.

skolemization of proofs: example

$$
\begin{prooftree}
\AxiomC{$P(a,\alpha) \vdash P(a,\alpha)$}
\AxiomC{$Q(\alpha) \vdash Q(\alpha)$}
\RightLabel{$\to\colon l$}
\BinaryInfC{$P(a,\alpha), P(a,\alpha) \to Q(\alpha)) \vdash Q(\alpha)$}
\RightLabel{$\exists\colon r$}
\UnaryInfC{$P(a,\alpha), P(a,\alpha) \to Q(\alpha)) \vdash (\exists z)Q(z)$}
\RightLabel{$\forall\colon l$}
\UnaryInfC{$P(a,\alpha), (\forall v)(P(a,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\RightLabel{$\forall\colon l$}
\UnaryInfC{$P(a,\alpha), (\forall u)(\forall v)(P(u,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\RightLabel{$\exists\colon l$}
\UnaryInfC{$(\exists y)P(a,y), (\forall u)(\forall v)(P(u,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\RightLabel{$\forall\colon l$}
\UnaryInfC{$(\forall x)(\exists y)P(x,y), (\forall u)(\forall v)(P(u,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\end{prooftree}
$$

$$
\begin{prooftree}
\AxiomC{$P(a,f(a)) \vdash P(a,f(a))$}
\AxiomC{$Q(f(a)) \vdash Q(f(a))$}
\RightLabel{$\to\colon l$}
\BinaryInfC{$P(a,f(a)), P(a,f(a)) \to Q(f(a))) \vdash Q(f(a))$}
\RightLabel{$\exists\colon r$}
\UnaryInfC{$P(a,f(a)), P(a,f(a)) \to Q(f(a))) \vdash (\exists z)Q(z)$}
\RightLabel{$\forall\colon l$}
\UnaryInfC{$P(a,f(a)), (\forall v)(P(a,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\RightLabel{$\forall\colon l$}
\UnaryInfC{$P(a,f(a)), (\forall u)(\forall v)(P(u,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\RightLabel{$\forall\colon l$}
\UnaryInfC{$(\forall x)P(x,f(x)), (\forall u)(\forall v)(P(u,v) \to Q(v)) \vdash (\exists z)Q(z)$}
\end{prooftree}
$$

clause form transformations

- clause: atomic sequent.
- provability of $\vdash F$ can be reduced to refutability of sets of clauses $\mathcal{C}(F)$.
- clause form transformation: transformation of $\neg F$ to $\mathcal{C}(F)$.
- refutation of sets of clauses: by resolution

clause form transformations: example

$$F = (H(s) \land (\forall x)(H(x) \to M(x))) \to M(s).$$

transform $\neg F$ to

$$(H(s) \land (\forall x)(H(x) \to M(x))) \land \neg M(s).$$

clause form:

$$\{\vdash H(s),\ H(x) \vdash M(x),\ M(s) \vdash\}.$$

the resolution calculus

- resolution works on sets of clauses.
- resolution consists of substitution (most general unification) + cut.

The resolution rule (A_i, B_j atoms):

- $C = \Gamma \vdash \Delta, A_1, \ldots, A_n$,
- $D = B_1, \ldots, B_m, \Pi \vdash \Lambda$,
- assume $A_i\theta = B_j\theta = A'$ for all i, j so θ "unifies" all the A_i, B_j.
- then apply θ, cut out the A_i, B_j and get the resolvent of C and D:

$$\Gamma\theta, \Pi\theta \vdash \Delta\theta, \Lambda\theta.$$

resolution deductions

- binary proof trees with resolution as the only rule.
- resolution refutation: resolution deduction of $\vdash$ (the empty sequent).

example:

$$\mathcal{C} = \{\vdash H(s),\ H(x) \vdash M(x),\ M(s) \vdash\}.$$

resolution refutation of $\mathcal{C}$:

$$\dfrac{\dfrac{\vdash H(s) \quad H(x) \vdash M(x)}{\vdash M(s)}\ x \leftarrow s \qquad M(s) \vdash}{\vdash}$$

the resolution calculus

- resolution is complete, i.e. $\vdash A$ is provable in **LK** iff the clause form of $\neg A$ is refutable by resolution.
- resolution is the basic calculus for the most efficient automated theorem provers.
- (without unification) resolution represents the "logic-free" structural part of **LK** on atomic sequents.

The Method CERES: cut-elimination by resolution

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

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

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:

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

$\varphi(C_1) =$

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

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 γ $\Rightarrow$ 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 $\mathrm{CL}(\varphi)$:

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

ground projection γ of δ:

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

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

Example

end sequent S of φ, $S = B \vdash C$.

$\gamma =$

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\overset{(\chi_2)}{B \vdash C, P(a)} \qquad \overset{(\chi_1)}{P(a), B \vdash C, Q(a)}}{B, B \vdash C, C, Q(a)}\,cut}{B \vdash C, Q(a)}\,c^* \qquad \overset{(\chi_3)}{Q(a), B \vdash C}}{B, B \vdash C, C}\,cut}{S}\,c^*$$

skolemized proofs

- SK = set of all **LK**-derivations with skolemized end-sequents.
- $\mathrm{SK}_\emptyset$ = 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 $\varphi \in \mathrm{SK}$ into $\psi \in \mathrm{SK}^0$.
- Proof skolemization needed for soundness of projections!

first step: construction of the characteristic clause set

characteristic clause set

- φ: an **LK**-derivation of S,
- Ω be the set of all occurrences of cut formulas in φ.

We define the set of clauses $\mathrm{CL}(\varphi)$ inductively:

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

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

where $\mathrm{sq}(\nu, \Omega)$ is the subsequent of sq_ν containing the ancestors of Ω.

Assume: S/ν already constructed for $\mathrm{depth}(\nu) \leq k$.
$\mathrm{depth}(\nu) = k + 1$:

(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 $\mathrm{sq}(\mu_1, \Omega), \mathrm{sq}(\mu_2, \Omega)$:

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

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

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

$\mathrm{CL}(\varphi) = S/\nu_0$ 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 $\mathrm{CL}(\varphi) = \{\vdash\}$.

Proposition:

Let φ be an **LK**-derivation. Then $\mathrm{CL}(\varphi)$ is refutable by resolution.

projection

Lemma:

Let φ be a deduction in 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.

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

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

- $\varphi(C)$ is sound: no strong quantifier inferences in $\varphi(C)$!

the remaining steps of CERES

- Construct a resolution refutation γ of $\mathrm{CL}(\varphi)$,
- insert the projections of φ into γ.
- add some contractions and obtain a proof with (only) atomic cuts, the CERES normal form.

(elimination of the atomic cuts optional)

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 $C \in \mathrm{CL}(\varphi)$:

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

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

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

- **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 w.r.t. the length of cut-free proofs:

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 $\mathcal{R}$!

1903

David Hilbert, Grundlagen der Geometrie

$\Downarrow$

the axiomatic method

the Hilbertian revolution

And before?

Euler became famous by deriving

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \tag{1}$$

Let us consider Eulers reasoning. Consider the polynomial of even degree

$$b_0 - b_1 x^2 + b_2 x^4 - \ldots + (-1)^n b_n x^{2n} \tag{2}$$

If $b_n = 1$ it has the $2n$ roots $\pm\beta_1, \ldots, \beta_n \neq 0$ then (2) can be written as

$$(x - \beta_1)(x + \beta_1) \ldots (x - \beta_n)(x + \beta_n) \tag{3}$$

$$(-1)^n(\beta_1 - x)(\beta_1 + x) \ldots (\beta_n - x)(\beta_n + x) \tag{4}$$

$$(-1)^n(\beta_1^2 - x^2) \ldots (\beta_n^2 - x^2) \tag{5}$$

where $b_0 = (-1)^n \beta_1^2 \ldots \beta_n^2$

$$b_0 \left(1 - \frac{x^2}{\beta_1^2}\right)\left(1 - \frac{x^2}{\beta_2^2}\right) \ldots \left(1 - \frac{x^2}{\beta_n^2}\right) \tag{6}$$

By comparing coefficients in (2) and (6) one obtains that

$$b_1 = b_0 \left(\frac{1}{\beta_1^2} + \frac{1}{\beta_2^2} + \ldots + \frac{1}{\beta_n^2}\right). \tag{7}$$

Next Euler considers the Taylor series for $sin(x)$ divided by x

$$\frac{\sin x}{x} = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n+1)!} \tag{8}$$

which has as roots $\pm\pi, \pm 2\pi, \pm 3\pi, \ldots$ Now by way of analogy Euler assumes that the infinite degree polynomial (8) behaves in the same way as the finite polynomial (2). Hence in analogy to (6) he obtains

$$\frac{\sin x}{x} = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\ldots \tag{9}$$

and in analogy to (7) he obtains

$$\frac{1}{3!} = \left(\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \ldots\right) \tag{10}$$

which immediately gives

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \tag{11}$$

(1) That Kurt Gödel is Austrian entails that Kurt Gödel is Austrian.
(2) Hence, that Kurt Gödel is Austrian entails that everyone is Austrian.
(3) That is, if Kurt Gödel is Austrian, then all people are Austrian.
(4) Therefore, there exists a person such that, if that person is Austrian, then all people are Austrian.

$$\dfrac{\dfrac{\dfrac{A(a) \vdash A(a)}{A(a) \vdash \forall y A(y)}}{\vdash A(a) \to \forall y A(y)}}{\vdash \exists x (A(x) \to \forall y A(y))}$$

The traditional way to ensure soundness

- Inferences are sound, i.e. only true conclusions result from true premises.
- Derivations are hereditary, i.e. initial segments of proofs are proofs themselves.

Weak regularity

$$\dfrac{\dfrac{\dfrac{\dfrac{A(a) \vdash A(a)}{A(a) \vdash \forall x A(x)} \qquad \dfrac{A(f(a)) \vdash A(f(a))}{\forall x A(x) \vdash A(f(a))}}{A(a) \vdash A(f(a))}}{\vdash A(a) \to A(f(a))}}{\vdash \exists x (A(x) \to A(f(x)))}$$

Side variables

b is a side variable of a in π (written $a <_\pi b$) if π contains a strong-quantifier inference of the form

$$\frac{\Gamma \vdash \Delta, A(a, b, \vec{c})}{\Gamma \vdash \Delta, \forall x A(x, b, \vec{c})}$$

or of the form

$$\frac{A(a, b, \vec{c}), \Gamma \vdash \Delta}{\exists x A(x, b, \vec{c}), \Gamma \vdash \Delta}$$

Skolemization sk(A)

The Skolemization of a first-order formula is defined by replacing every strongly quantified variable y with a new function symbol $f_y(x_1, \ldots, x_n)$, where $x_1, \ldots, x_n$ are the weakly quantified variables such that Q_y appears in the scope of their quantifiers, and removing the quantifier Q_y.

$$\begin{array}{c}
A(b) \vdash A(b) \\
\hline
A(a), A(b) \vdash A(b) \\
\hline
A(b) \vdash A(a) \to A(b) \\
\hline
A(b) \vdash A(a) \to A(b), A(c) \\
\hline
\vdash A(a) \to A(b), A(b) \to A(c) \\
\hline
\vdash A(a) \to A(b), \forall y(A(b) \to A(y)) \\
\hline
\vdash A(a) \to A(b), \exists x \forall y(A(x) \to A(y)) \\
\hline
\vdash \forall y(A(a) \to A(y)), \exists x \forall y(A(x) \to A(y)) \\
\hline
\vdash \exists x \forall y(A(x) \to A(y)), \exists x \forall y(A(x) \to A(y)) \\
\hline
\vdash \exists x \forall y(A(x) \to A(y))
\end{array}$$

Skolemization:

$$\begin{array}{c}
A(f(a)) \vdash A(f(a)) \\ \hline
A(a), A(f(a)) \vdash A(f(a)) \\ \hline
A(f(a)) \vdash A(a) \to A(f(a)) \\ \hline
A(f(a)) \vdash A(a) \to A(f(a)), A(f(f(a))) \\ \hline
\vdash A(a) \to A(f(a)), A(f(a)) \to A(f(f(a))) \\ \hline
\vdash A(a) \to A(f(a)), \exists x(A(x) \to A(f(x))) \\ \hline
\vdash \exists x(A(x) \to A(f(x))), \exists x(A(x) \to A(f(x))) \\ \hline
\vdash \exists x(A(x) \to A(f(x)))
\end{array}$$

Suitable quantifier inferences

A quantifier inference is suitable for a proof π if either it is a weak-quantifier inference, or the following three conditions are satisfied:

- (substitutability) the characteristic variable does not appear in the conclusion of π.
- (side-variable condition) the relation $<_\pi$ is acyclic.
- (weak regularity) the characteristic variable is not the characteristic variable of another strong-quantifier inference in π.

(LK^+)

The calculus LK^+ is defined like LK, except that we instead allow all weak and strong quantifier inferences with the proviso that they be suitable for the proof.

Weakly suitable quantifier inference

A quantifier inference is weakly suitable for a proof π if either it is a weak-quantifier inference or it satisfies substitutability, the side-variable condition, and

- (very weak regularity) whenever the characteristic variable is also the characteristic variable of another strong-quantifier inference in π, then it has the same critical formula.

LK^{++}

The calculus LK^{++} is the extension of LK^{+} that results from allowing all weakly suitable quantifier inferences.

Soundness

Theorem.
If a sequent is LK^{++}-derivable, then it is already LK-derivable.

Proof. Let π be an LK^{++}-proof. Replace every unsound universal quantifier inference by an $\to L$ inference:

$$\frac{\Gamma \vdash \Delta, A(a) \qquad \forall x A(x) \vdash \forall x A(x)}{\Gamma, A(a) \to \forall x A(x) \vdash \Delta, \forall x A(x)}$$

Similarly replace every unsound existential quantifier by an $\to L$ inference

$$\frac{\exists x A(x) \vdash \exists x A(x) \qquad A(a), \Gamma \vdash \Delta}{\Gamma, \exists x A(x), \exists x A(x) \to A(a) \vdash \Delta}$$

By doing this, we obtain a proof of the desired sequent, together with many formulae of the form $A(a) \to \forall x A(x)$ or $\exists x A(x) \to A(a)$ on the left-hand side. Introduce existential quantifiers left. This is sound in LK by properties of $<_\pi$.

Corollary.

If a sequent is derivable in LK^{+} or LK^{++}, then it is already derivable in LK.

$$\dfrac{\dfrac{\dfrac{\dfrac{A(a,b) \vdash A(a,b)}{A(a,b) \vdash \forall y A(a,y)}}{A(a,b) \vdash \exists x \forall y A(x,y)}}{\exists x A(x,b) \vdash \exists x \forall y A(x,y)}}{\forall y \exists x A(x,y) \vdash \exists x \forall y A(x,y)}$$

$$a <_\pi b \quad b <_\pi a\ !$$

LK

$$
\begin{prooftree}
\AxiomC{$A(a) \vdash A(a)$}
\UnaryInfC{$A(a) \vdash A(a), B$}
\UnaryInfC{$\vdash A(a), A(a) \to B$}
\UnaryInfC{$\vdash A(a), \exists x\,(A(x) \to B)$}
\UnaryInfC{$\vdash \exists x\,(A(x) \to B), A(a)$}
\UnaryInfC{$\vdash \exists x\,(A(x) \to B), \forall x\, A(x)$}
\AxiomC{$B \vdash B$}
\BinaryInfC{$\forall x\, A(x) \to B \vdash \exists x\,(A(x) \to B), B$}
\UnaryInfC{$\forall x\, A(x) \to B, A(b) \vdash \exists x\,(A(x) \to B), B$}
\UnaryInfC{$\forall x\, A(x) \to B \vdash \exists x\,(A(x) \to B), A(b) \to B$}
\UnaryInfC{$\forall x\, A(x) \to B \vdash \exists x\,(A(x) \to B), \exists x\,(A(x) \to B)$}
\UnaryInfC{$\forall x\, A(x) \to B \vdash \exists x\,(A(x) \to B)$}
\end{prooftree}
$$

LK$^+$

$$\begin{prooftree}
\AxiomC{$A(a) \vdash A(a)$}
\UnaryInfC{$A(a) \vdash \forall x\, A(x)$}
\AxiomC{$B \vdash B$}
\BinaryInfC{$A(a), \forall x\, A(x) \to B \vdash B$}
\UnaryInfC{$\forall x\, A(x) \to B, A(a) \vdash B$}
\UnaryInfC{$\forall x\, A(x) \to B \vdash A(a) \to B$}
\UnaryInfC{$\forall x\, A(x) \to B \vdash \exists x\, (A(x) \to B)$}
\end{prooftree}$$

Theorem.

There is no elementary function bounding the length of the shortest cut-free LK-proof of a formula in terms of its shortest cut-free LK^{+}-proof.

An immediate consequence is the following:

Corollary.

There is no elementary function bounding the length of the shortest cut-free LK-proof of a formula in terms of its shortest cut-free LK^{++}-proof.

The calculus $\mathsf{LK}_{\mathsf{shift}}$ is obtained by extending LK with the following rules:

$$\frac{\Gamma, \kappa[Qx\, A \lhd B] \vdash \Delta}{\Gamma, \kappa[Q'x\,(A \lhd B)] \vdash \Delta} \qquad \frac{\Gamma, \kappa[A \lhd Qx\, B] \vdash \Delta}{\Gamma, \kappa[Q'x\,(A \lhd B)] \vdash \Delta}$$

$$\frac{\Gamma \vdash \Delta, \kappa[Qx\, A \lhd B]}{\Gamma \vdash \Delta, \kappa[Q'x\,(A \lhd B)]} \qquad \frac{\Gamma \vdash \Delta, \kappa[A \lhd Qx\, B]}{\Gamma \vdash \Delta, \kappa[Q'x\,(A \lhd B)]}$$

where $\kappa[\cdot]$ is a context, $\lhd \in \{\wedge, \vee, \rightarrow\}$ and $Q' = Q$, except if $\lhd$ is $\rightarrow$ and Q is taken from the antecedent, in which case Q' is opposite. We refer to these rules as *deep quantifier shifts*.

Proposition.

Cut-free LK^+ simulates cut-free $\mathsf{LK}_{\mathsf{shift}}$ double-exponentially, i.e., every $\mathsf{LK}_{\mathsf{shift}}$-provable sequent is LK^+-provable and there is a double exponential function that bounds the length of the least cut-free LK^+-proof of a LK^+-provable sequent in terms of its least cut-free $\mathsf{LK}_{\mathsf{shift}}$-proof.

In $\mathrm{LK}_{\mathrm{shift}}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{A(a) \vdash A(a)}{\forall x A(x) \vdash A(a)}}{\forall x A(x) \vdash \forall y A(y)}}{\vdash \forall x A(x) \to \forall y A(y)}}{\vdash \exists x (A(x) \to \forall y A(y))}$$

In LK^{+}:

$$\dfrac{\dfrac{\dfrac{A(a) \vdash A(a)}{A(a) \vdash \forall y A(y)}}{\vdash A(a) \to \forall y A(y)}}{\vdash \exists x (A(x) \to \forall y A(y))}$$

In LK:

$$
\begin{array}{r@{\;}l}
A(a) & \vdash A(a) \\
\hline
A(a) & \vdash A(a), \forall y A(y) \\
\hline
 & \vdash A(a), A(a) \to \forall y A(y) \\
\hline
 & \vdash A(a), \exists x (A(x) \to \forall y A(y)) \\
\hline
 & \vdash \forall y A(y), \exists x (A(x) \to \forall y A(y)) \\
\hline
A(a) & \vdash \forall y A(y), \exists x (A(x) \to \forall y A(y)) \\
\hline
 & \vdash A(a) \to \forall y A(y), \exists x (A(x) \to \forall y A(y)) \\
\hline
 & \vdash \exists x (A(x) \to \forall y A(y)), \exists x (A(x) \to \forall y A(y)) \\
\hline
 & \vdash \exists x (A(x) \to \forall y A(y))
\end{array}
$$

Theorem.

There is no elementary function bounding the length of the shortest cut-free LK-proof of a formula in terms of its shortest cut-free $\mathrm{LK}_{\mathrm{shift}}$-proof.

e.g. Statman's sequence $\{s_j\}_{j<\omega}$

1. the size of S_i is polynomial in i;
2. there is no bound on the size of their smallest cut-free LK-proofs that is elementary in i;
3. the size of these proofs (with cuts), however, is polynomially bounded in i;
4. all cut formulae are closed; we can also assume they are prenex by, e.g., Theorem 3.3 in [BaazLeitsch94][1].

---

[1] M. Baaz and A. Leitsch, On Skolemization and Proof Complexity, Fund. Inform., 20 (1994), 353-379.

Transform this proof in $\mathrm{LK}_{\mathrm{shift}}$

$$\frac{\Gamma \vdash \Delta, A \qquad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}$$

$$\Downarrow$$

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma, A \vdash \Delta}{\Gamma, A \to A \vdash \Delta} \to L$$

obtaining

$$A_0 \to A_0, \ldots, A_m \to A_m, \Gamma_i \vdash \Delta_i$$

cut-free.

And by $\mathrm{LK}_{\mathrm{shift}}$-rules cut-free

$$\forall x_0^0 \exists x_1^0 \ldots (\hat{A}_0 \to \hat{A}_0), \ldots, \forall x_0^m \exists x_1^m (\hat{A}_m \to \hat{A}_m), \Gamma_i \vdash \Delta_i.$$

Claim.

There is no elementary function bounding the size of the smallest cut-free LK-proofs of

$$\forall x_0^0 \exists x_1^0 \ldots (\hat{A}_0 \to \hat{A}_0), \ldots, \forall x_0^m \exists x_1^m (\hat{A_m} \to \hat{A_m}), \Gamma_i \vdash \Delta_i.$$

Skolemize, extract a Herbrand sequent and replace all Skolem terms stepwise by $f(t_1, \ldots, t_n) \to t_i$ sucht that the instances of

$$\forall x_0^0 \exists x_1^0 \ldots (\hat{A}_0 \to \hat{A}_0), \ldots, \forall x_0^m \exists x_1^m$$

Skolemized become of the form $c \to c$.

LJ^+ and LJ^{++}

Proposition

LJ^+ and LJ^{++} do not admit cut elimination.

$$\dfrac{\dfrac{\dfrac{\dfrac{A(a) \vdash A(a)}{A(a) \vdash \forall x A(x)} \qquad \dfrac{A(f(a)) \vdash A(f(a))}{\forall x A(x) \vdash A(f(a))}}{A(a) \vdash A(f(a))}}{\vdash A(a) \to A(f(a))}}{\vdash \exists x (A(x) \to A(f(x)))}$$

Consequently, there is no Gentzen-style cut-elimination for LK^+ and LK^{++}.

Quantifier shifts not valid intuitionistically

1. $\forall x\,(A \vee B(x)) \vdash A \vee \forall x\, B(x)$;
2. $(\forall x\, A(x) \to B) \vdash \exists x\,(A(x) \to B)$;
3. $(A \to \exists x\, B(x)) \vdash \exists x\,(A \to B(x))$.

Proposition.

A sequent is provable in LJ^{++} if and only if it is provable in LJ with all quantifier shifts added as axioms.

No elementary Skolemization for cut-free LK^{+} and LK^{++} proofs.
(But quadratic Skolemization using additional cuts.)

No elementary extraction of Skolemized Herbrand disjunctions from cut-free LK^{+} and LK^{++} proofs.

Andrew's Skolemization

$\mathcal{A}(\exists x B(x, \overline{y}))$
B negative in $\mathcal{A}$

$\mathcal{A}(\forall x B(x, \overline{y}))$
B positive in $\mathcal{A}$

$$\Downarrow$$

$$\mathcal{A}(B(f(\overline{y}), \overline{y}))$$

where f depends only on the weakly bound variables of the scope that occur in B.

Proposition.

Andrew's Skolemization projects a cut-free LK^{++}-proof into a cut-free proof of the Skolemized end-sequent. Conversely, any cut-free proof of Andrew's Skolemization of a sequent can be easily retransformed into a cut-free proof in LK.

Andrew's Skolemization

Consequently, there is a sequence of refutable formulas $A_1, A_2, \ldots$ such that the lenght of the shortest refutations of the clause forms of the usual Skolemization cannot not be elementarily bounded in the length of the shortest refutations of the clause forms of Andrews's Skolemizations.

(Note that this holds for any elementary transformation to clause form of the Skolemized formulas!)

Relation to the ε-calculus

$$\exists x A(x) \sim A(\varepsilon_x A(x))$$

$$\forall x A(x) \sim A(\varepsilon_x \neg A(x)) \sim A(\tau_x A(x))$$

LK_ε

$$\frac{\Gamma, A(t) \vdash \Delta}{\Gamma, A(\tau_x A(x)) \vdash \Delta}\ \tau$$

$$\frac{\Gamma \vdash \Delta, A(t)}{\Gamma \vdash \Delta, A(\varepsilon_x A(x))}\ \varepsilon$$

Consider the following proof of a sequent whose only occurrence of τ is weak:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A(\tau_x(A(x) \to B)) \vdash A(\tau_x(A(x) \to B))}{A(\tau_x A(x)) \vdash A(\tau_x(A(x) \to B))}}{A(\tau_x A(x)) \vdash B,\ A(\tau_x(A(x) \to B))}}{\vdash A(\tau_x A(x)) \to B,\ A(\tau_x(A(x) \to B))} \qquad B \vdash B}{A(\tau_x(A(x) \to B)) \to B \vdash A(\tau_x A(x)) \to B,\ B}}{A(\tau_x(A(x) \to B)) \to B,\ A(\tau_x A(x)) \vdash A(\tau_x A(x)) \to B,\ B}}{A(\tau_x(A(x) \to B)) \to B \vdash A(\tau_x A(x)) \to B,\ A(\tau_x A(x)) \to B}}{A(\tau_x(A(x) \to B)) \to B \vdash A(\tau_x A(x)) \to B}$$

The corresponding Herbrand sequent is

$$A(a) \to B \vdash \big(A(a) \to B\big) \vee \big(A(b) \to B\big), \qquad\qquad (D)$$

which is a propositional tautology.

Moreover, the result of shifting the disjunction to where the ε-term originally appeared, namely,

$$A(a) \to B \vdash A(a) \land A(b) \to B,$$

is also a propositional tautology. Here, the disjunction is replaced by a conjunction, as the ε-term appeared in the antecedent of an implication. The conclusion of the proof is the translation of the Skolemized sequent

$$\forall x \, \bigl(A(x) \to B\bigr) \vdash \forall x \, A(x) \to B,$$

and so this is LK-provable. Compare this with

$$\forall x \, \bigl(A(x) \to B\bigr) \vdash \exists x \, \bigl(A(x) \to B\bigr),$$

which is the Skolemized sequent suggested by (D).

Proposition

If a sequent is has an LK^{++}-proof of length k, then its standard translation has an $\mathrm{LK}^{\varepsilon}$-proof of length $\leq k$.

Proposition

A sequent is LJ^{++}-provable if and only if its standard translation is $\mathrm{LJ}^{\varepsilon}$-provable.

Relation to the ε-calculus

Another soundness proof for LK^{+} and LK^{++}
But e.g.

$$\begin{array}{c}
(\varphi) \\
\Gamma \vdash \Delta, A(s(t)) \\
\hline
\Gamma \vdash \Delta, A(s(\varepsilon_x A(s(x)))) \\
\hline\hline
\Gamma' \vdash \Delta', A(s(\varepsilon_x A(s(x)))) \\
\hline
\Gamma' \vdash \Delta', A(\varepsilon_x A(x))
\end{array}$$

not represented in LK^{+} and LK^{++}.

All cuts in LK$^{\varepsilon}$ can be immediately reduced to translations of universal cuts.

$$\Downarrow$$

No Schütte-Tait-style cut-elimination.

Also Gentzen-style cut-elimination is impossible.

$$\dfrac{\dfrac{\Pi \vdash \Gamma, A(e, f(e)) \qquad A(e, f(e)), \Pi \vdash \Gamma}{\Pi, \Pi \vdash \Gamma, \Gamma}}{\Pi \vdash \Gamma}$$

$$f(x) \sim \tau_y A(x, y), \quad e \sim \varepsilon_x A(x, f(x)), \quad A(e, f(e)) \sim [\exists x \forall y A(x, y)]^{\varepsilon}$$

can be easily transformed into

$$\dfrac{\dfrac{\dfrac{\dfrac{\Pi \vdash \Gamma, A(e, f(e)) \qquad A(e, f(e)), \Pi \vdash \Gamma}{A(e, f(e)) \to A(e, f(e)), \Pi \vdash \Gamma}}{A(e, h(e)) \to A(e, h(e)), \Pi \vdash \Gamma}}{A(g, h(g)) \to A(g, h(g)), \Pi \vdash \Gamma}}{\Pi \vdash \Gamma}$$

cut with

$$\dfrac{A(g, h(g)) \vdash A(g, h(g))}{\vdash A(g, h(g)) \to A(g, h(g))}$$

$h(x) \sim \tau_y(A(x, y) \to A(x, y)), g \sim \tau_x(A(x, h(x)) \to A(x, h(x)))$
$A(g, h(g)) \to A(g, h(g)) \sim [\forall x \forall y(A(x, y) \to A(x, y))]^{\varepsilon}$

We have to suppress inner inferences (no first ε-theorem for the logic captured by $\mathsf{LJ}^{\varepsilon}$!)

Inner inferences

$$\frac{\Pi \vdash \Gamma, A(t)}{\Pi \vdash \Gamma, A(\varepsilon_x A(x))}$$

$$\frac{A(t), \Pi \vdash \Gamma}{A(\tau_x A(x)), \Pi \vdash \Gamma}$$

are eliminated by inferring

$$A(\overline{s}, t) \to A(\overline{s}, f_i(\overline{s})) \qquad A(\overline{s}, f_j(\overline{s})) \to A(\overline{s}, t)$$

on the left side, where $\overline{s}$ are terms substituted in the matrix.

We reconstruct an LK^{++} proof of

$$\ldots \forall \overline{x} \forall y (A(\overline{x}, y) \rightarrow A(\overline{x}, f_i(\overline{x}))) \ldots \forall \overline{x} \forall y (A(\overline{x}, f(\overline{x})) \rightarrow A(\overline{x}, y)),$$

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

from a proof of $[A_1]^\tau, \ldots, [A_n]^\tau \vdash [B_1]^\tau, \ldots, [B_m]^\tau$ in LJ$^\varepsilon$.

Translate this proof to a proof of

$$\forall \overline{x} \exists z \forall y (A(\overline{x}, y) \rightarrow A(\overline{x}, z)) \ldots \forall \overline{x} \exists z \forall y (A(\overline{x}, z) \rightarrow A(\overline{x}, y)),$$

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

Derive the additional formulas using shifts and apply cuts.

complexity of the ε-notation

ε-translation of $\exists x \exists y \exists z\ A(x, y, z)$:

$$\begin{array}{l}
A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)),\ \varepsilon_z A(x, \varepsilon_y\ A(x, y, \varepsilon_z \\
A(x, y, z)), z)),\ \varepsilon_y\ A(\varepsilon_x\ A(x, \varepsilon_y \\
A(x, y, \varepsilon_z A(x, y, z)), \varepsilon_z A(x, \varepsilon_y A(x, y, \varepsilon_z A(x, y, z)), z)),\ y, \varepsilon_z A(\varepsilon_x \\
A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z \\
A(x, y, z)), z)), y, z)),\ \varepsilon_z A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z \\
A(x, y, z)), \varepsilon_z A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)),\ \varepsilon_y A(\varepsilon_x\ A(x, \varepsilon_y \\
A(x, y, \varepsilon_z\ A(x, y, z)), \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)),\ y, \varepsilon_z \\
A(\varepsilon_x\ A(x, \varepsilon_y\ A(x,\ y,\ \varepsilon_z\ A(x,\ y,\ z)), \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z \\
A(x, y, z)), z)), y, z)), z)).
\end{array}$$

Lemma (Hilbert's Ansatz)

If $A(t_1) \to A(\varepsilon_x A(x)), \ldots, A(t_n) \to A(\varepsilon_x\ A(x)), \Pi \vdash \Delta$ *is valid then* $\Pi\{\varepsilon_x A(x) \to t_1\}, \ldots, \Pi\{\varepsilon_x A(x) \to t_n\}, \Pi \vdash \Delta\{\varepsilon_x\ A(x) \to t_1\}, \ldots, \Delta\{\varepsilon_x\ A(x) \to t_n\}, \Delta$ *is valid (*$\varepsilon_x A(x)$ *can then be substituted by a fixed constant).*

Proof.

Note that $A(t_i), \Pi\{\varepsilon_x A(x) \to t_i\} \vdash \Delta\{\varepsilon_x A(x) \to t_i\}$ and $\neg A(t_1), \ldots, \neg A(t_n), \Pi \vdash \Delta$ are valid. $\square$

Definition

An ε-term e is *nested* in an ε-term e' if e is a proper subterm of e'. An ε-term e is *subordinate* to an ε-term $e' = \varepsilon_x A(x)$ if e occurs in e' and x is free in e.

The *rank* counts the subordination levels and the *degree* the length of the maximal inclusion chain.

Theorem (Extended first ε-theorem)

Given a proof $C_1, \ldots, C_r, \Pi \vdash \Delta$ *we obtain a valid sequent* $\Pi\sigma_1, \ldots, \Pi\sigma_n \vdash \Delta\sigma_1, \ldots, \Delta\sigma_n$ *containing no* ε*-terms, where the* σ_i *are substituting* ε*-terms by closed terms.*

Proof.

(Sketch) Hilbert's Ansatz is repeatedly applied to ε-terms of maximal rank and maximal degree and to the remaining critical formulas to obtain an expansion both of the other critical formulas and of the rest of the sequent. The condition of maximal rank is necessary to guarantee that critical formulas are transformed into critical formulas by these substitutions. The maximal degree is necessary for termination. ☐

Literature

- Juan P. Aguilera and Matthias Baaz. Unsound inferences make proofs shorter. To appear in the Journal of Symbolic Logic.
- Matthias Baaz and Alexander Leitsch. Methods of cut-elimination. Vol. 34. Springer Science & Business Media, 2011.
- David Hilbert and Paul Bernays. Grundlagen der Mathematik. 2, 1939.
- Georg Moser and Richard Zach. The epsilon calculus and Herbrand complexity. Studia Logica, 82(1) : 133 – 155, 2006.
- Helmut Schwichtenberg. Proof theory: Some applications of cut-elimination. Studies in Logic and the Foundations of Mathematics. Vol. 90. Elsevier, 1977. 867-895.
- Gaisi Takeuti. Proof theory. Volume 81 of Studies in Logic and the Foundations of Mathematics, 1975.