On the complexity of proof deskolemization

M. Baaz, S. Hetzl, D. Weller

Collegium Logicum: proof & structures 2010

Motivation

- Investigate the influence of Skolem functions on length of classical first-order proofs.

Motivation

- Investigate the influence of Skolem functions on length of classical first-order proofs.
- Of practical interest:
  - Skolemization used by resolution provers and the CERES method.
  - Give an (efficient?) algorithm to remove Skolem functions.

Motivation

- Investigate the influence of Skolem functions on length of classical first-order proofs.
- Of practical interest:
  - Skolemization used by resolution provers and the CERES method.
  - Give an (efficient?) algorithm to remove Skolem functions.
- Of theoretical interest:
  - How much expressivity is gained by using Skolem functions?

Motivation

Problem

Given: a proof of the Skolemization of a formula F.
Wanted: a proof of F.

Aim: Find upper and lower bounds for this problem.

Motivation

A related question was asked in [P. Clote and J. Krajíček 1993]:

Question (Pudlák)

Assume that $(\forall x)(\exists y)\phi(x, y)$ is provable in predicate logic. Introduce a new function symbol f and an axiom A_ϕ which states

$$(\forall x)\phi(x, f(x)).$$

Does there exist formula ϕ such that the extended system gives a superexponential speed-up over predicate calculus, with respect to number of symbols in proofs?

Remark

- A positive answer seems to require the construction of a lower bound for a proof system with cut.
- A negative answer for a large class was given by (Avigad 2003):
  - From proofs in theories strong enough to code finite functions, Skolem functions can be eliminated in polynomial time.
- Here, we concentrate on cut-free systems.

More Related Work

- Maehara 1955: Remove Skolem functions from proofs (uses cut-elimination).
- de Nivelle 2003: Remove Skolem functions from resolution proofs (introduces new predicate symbols).

Sequent calculus

- We use cut-free **G3c** $+ \top$:
  - Two-sided sequents.
  - **Contraction** and **weakening** absorbed into logical rules and axioms.
  - Connectives $\top, \bot, \neg, \vee, \wedge, \rightarrow, \exists, \forall$.
- Length of proof $|\pi|$ = number of sequents in π.

Skolemization

- Different forms of Skolemization are known:
  - Prefix Skolemization.
  - Structural Skolemization.
  - ...

Skolemization

- Different forms of Skolemization are known:
  - Prefix Skolemization.
  - Structural Skolemization.
  - ...
- Know from (Baaz, Leitsch 1994):
  - Prefix may be non-elementarily worse than Structural w.r.t. Herbrand complexity.
- We concentrate on structural Skolemization.

Structural Skolemization

Definition (Structural Skolemization)

The structural Skolemization $\mathrm{sk}(F)$ is obtained from F by iterating: Take a leftmost strong quantifier (Qx), remove it and replace x by $f(y_1, \ldots, y_n)$, where $(Q_1 y_1), \ldots (Q_n y_n)$ are the weak quantifiers dominating (Qx) and f is fresh.

Structural Skolemization

Example (Structural Skolemization)

Let $F = (\exists x)((\forall y)G(y) \wedge (\exists z)H(z))$ where G, H are quantifier-free. Then

$$\mathrm{sk}(F) = (\exists x)(G(f(x)) \wedge (\exists z)H(z))$$

A prefix Skolemization of F is

$$(\exists x)(\exists z)(G(f(x, z)) \wedge H(z)).$$

Outline

An upper bound

Theorem

Let π *be a cut-free proof of* $\mathrm{sk}(S)$*. Then there exists a cut-free proof* ψ *of* S *such that* $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$*.*

An upper bound

Theorem

Let π be a cut-free proof of $\mathrm{sk}(S)$. Then there exists a cut-free proof ψ of S such that $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$.

Proof sketch.

We will use a variant of expansion trees from (Miller 1983).

1. Extract a small expansion E from π.
2. Construct a proof φ of E in a calculus $\mathbf{LK}^{\mathbf{E}}$. φ has small depth. φ has to be constructed according to a specific strategy.
3. Transform φ into ψ by replacing Skolem terms by eigenvariables.

□

Expansions

- Idea: For a formula F, store instantiation and Skolem term information such that a valid Herbrand disjunction can "easily" be computed.

Lemma

Let π be a cut-free proof of a sequent S which does not contain any strong quantifiers. Then there is a tautological expansion E of S s.t. $|E| \leq |\pi|$.

Expansions

- Tautological expansions are not quantifier-free, but contain all instantiation information necessary to prove them.
- So: define a calculus on expansions to be able to use the usual bottom-up proof search for propositional logic.

$\mathbf{LK}^{\mathbf{E}}$

Axioms (A is an atom):

$$A, \Pi \vdash \Lambda, A, \quad \Pi \vdash \Lambda, \top, \text{ or } \quad \bot, \Pi \vdash \Lambda$$

Propositional rules:

$$\frac{E_1, \Pi \vdash \Lambda \quad E_2, \Pi \vdash \Lambda}{E_1 \vee E_2, \Pi \vdash \Lambda} \vee_l \qquad \frac{\Pi \vdash \Lambda, E_1, E_2}{\Pi \vdash \Lambda, E_1 \vee E_2} \vee_r$$

$$\frac{\Pi \vdash \Lambda, E}{\neg E, \Pi \vdash \Lambda} \neg_l \qquad \frac{E, \Pi \vdash \Lambda}{\Pi \vdash \Lambda, \neg E} \neg_r$$

and analogously for $\wedge$ and $\rightarrow$.

$\mathbf{LK^E}$

Quantifier rules:

$$\frac{\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_{i-1}} E_{i-1} +^{t_{i+1}} E_{i+1} \ldots +^{t_n} E_n, E_i}{\Pi \vdash \Lambda, \exists x\, A +^{t_1} E_1 \ldots +^{t_n} E_n}\ \exists_r$$

$$\frac{E, \Pi \vdash \Lambda}{\exists x\, A +^{t} E, \Pi \vdash \Lambda}\ \exists_l$$

and analogously for $\forall_r$ and $\forall_l$.
Note: No eigenvariable condition. Will be recovered later.

$\mathbf{LK}^{\mathbf{E}}$

Lemma

Let π *be an* $\mathbf{LK}^{\mathbf{E}}$*-proof of an expansion* E*, then* $\mathrm{depth}(\pi) \leq |E|$.

Skolem term ordering

Definition

For an expansion E we define the Skolem term ordering $\prec_E$ as $s \prec_E t$ if

1. s is a proper subterm of t, or
2. E contains a strong quantifier $Qx\, A' +^s E'$ and E' contains a strong quantifier $Qy\, A'' +^t E''$.

- Analogous relations have been used in the literature when removing Skolem terms.

Skolem term ordering

- The following condition will ensure that the $\mathbf{LK}^{\mathbf{E}}$-proofs we construct can be transformed to **LK**-proofs obeying the eigenvariable conditions.

Definition

An $\mathbf{LK}^{\mathbf{E}}$-proof is called compatible with a term ordering $\preceq$ if for all quantifier inferences ι_1 and ι_2 where ι_1 is strong and is above ι_2 we have $\mathrm{t}(\iota_1) \npreceq \mathrm{t}(\iota_2)$.

Proof search

Lemma

Every tautological expansion E has an $\mathbf{LK^E}$*-proof that is compatible with* $\preceq_E$*.*

Proof sketch.

By propositional proof search with the following strategy for selecting main formulas:

- Take a $\preceq_E$-minimal element $f(\bar{s}, \bar{t})$. By definition it has a unique strong quantifier (Qy) in E.
- Select the formula containing (Qy) as the main formula.

□

Transforming to **LK**

Lemma

Let E be an expansion of a sequent S and let π be an $\mathbf{LK^E}$-proof of E which is compatible with $\preceq_E$. Then there is a cut-free proof ψ of S with $\mathrm{depth}(\psi) = \mathrm{depth}(\pi)$.

Upper bound — cut-free case

Theorem

Let π be a cut-free proof of $\mathrm{sk}(S)$, then there is a cut-free proof ψ of S with $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$ and hence $|\psi| \leq 2^{|\pi|\mathrm{qocc}(S)+|\pi|+\mathrm{qocc}(S)}$.

Upper bound — cut-free case

Theorem

Let π *be a cut-free proof of* $\mathrm{sk}(S)$*, then there is a cut-free proof* ψ *of* S *with* $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$ *and hence* $|\psi| \leq 2^{|\pi|\mathrm{qocc}(S)+|\pi|+\mathrm{qocc}(S)}$.

Corollary (Quantifier-free cut-elimination)

Let π *be a proof of* S *with quantifier-free cuts only, then there is a cut-free proof* ψ *of* S *with* $\mathrm{depth}(\psi) \leq |\pi|\mathrm{qocc}(S) + |\pi| + \mathrm{qocc}(S)$ *and hence* $|\psi| \leq 2^{|\pi|\mathrm{qocc}(S)+|\pi|+\mathrm{qocc}(S)}$.

The case with cut

Definition

A proof π has *essentially Skolem-free cuts* if every term that starts with a Skolem symbol and appears in a cut formula of π does not contain a bound variable.

The case with cut

Theorem

Let π be a proof of $\mathrm{sk}(S)$ with essentially Skolem-free cuts. Let c be the number of quantifiers in the cut-formulas of π. Then there is a proof ψ of S
s.t. $\mathrm{depth}(\psi) \leq (|\pi|^2 \mathrm{qocc}(S) + |\pi| + 1)(c + \mathrm{qocc}(S) + 1)$.

The case with cut

Proof sketch.

Let $S = \Gamma \vdash \Delta$ and $\mathrm{sk}(S) = \Gamma' \vdash \Delta'$.

1. Construct a "Skolem-term overbinding T-extension" of π, obtain cut-free proof of $\Sigma, \Gamma' \vdash \Delta'$.
2. Skolemize, obtain cut-free proof of $\Sigma', \Gamma' \vdash \Delta'$.
3. Apply deskolemization theorem, obtain cut-free proof of $\Sigma, \Gamma \vdash \Delta$ with exponential blow-up.
4. Reverse T-extension, obtain proof (with cuts) of $\Gamma \vdash \Delta$.

□

Outline

Lower bound for cut-free case

Theorem

There exists a sequence of sequents (R_n) such that

- *For all cut-free proofs π of R_N, $|\pi| \geq 2^N$, and*
- *there exists a cut-free proof π of $\mathrm{sk}(R_N)$ such that $|\pi| \leq k * N + c$ for some constants c, k.*

Lower bound for cut-free case

Proof.

Take

$$R_0 = \quad G_0 \to G_0$$
$$R_n = \quad ((\exists x_n)P_n(x_n) \vee G_n) \to (\exists y_n)((P_n(y_n) \vee G_n) \wedge R_{n-1}).$$

Quantifier placement forces R_{n-1} to be proved twice. The tree structure of proofs is used. □

An optimized Skolemization

Definition

We define a rewrite relation $\rightarrow_{sm}$ on formulas that "pushes quantifiers down":

$$(\forall x)\neg F \rightarrow_{sm} \neg(\exists x)F, \quad (\forall x)(F \vee G) \rightarrow_{sm} (\forall x)F \vee G$$

provided that x is not free in G, and so on for the other cases and connectives. If $F \rightarrow^*_{sm} G$ then $\mathrm{sk}(G)$ is an *sm-Skolemization* of F.

Lower bound for *sm*-Skolemization

Theorem

There exist sequences of sequents $(S_n), (M_n)$

1. M_n *is an sm-Skolemization of* S_n*, and*
2. *there exists a cut-free proof of* M_n *of elementary length, and*
3. *all cut-free proofs of* S_n*, have non-elementary length.*

Lower bound for *sm*-Skolemization

Theorem

There exist sequences of sequents $(S_n), (M_n)$

1. M_n *is an sm-Skolemization of* S_n*, and*
2. *there exists a cut-free proof of* M_n *of elementary length, and*
3. *all cut-free proofs of* S_n*, have non-elementary length.*

Proof sketch.

Consider Statman's sequence T_n and short proofs with cut π_n of T_n. Consider the end-sequent T'_n of the T-extension of π_n. Take $\mathrm{sk}(T'_n)$ for M_n. For S_n we take a certain "bad prefixation" of T'_n, constructed as the witness for e) in Theorem 4.1 in (Baaz1994). The result then follows from that Theorem. □

Open questions

- The case of proofs with cuts which are not essentially Skolem-free.
- The cut-free DAG case (our lower bound uses the fact that proofs are trees).