Skolemization of Sequent Calculus Proofs in Higher-Order Logic (Work in Progress)

Daniel Weller

Structural Proof Theory
Paris, 20 November 2008

Outline

Skolemization in FOL

- Operation sk on formulas
- Focus on proofs: consider validity-preserving sk
- $\mathrm{sk}(F)$ valid iff F valid
- $\mathrm{sk}(F)$ contains no strong quantifiers

Skolemization in FOL

- Operation sk on formulas
- Focus on proofs: consider validity-preserving sk
- $\mathrm{sk}(F)$ valid iff F valid
- $\mathrm{sk}(F)$ contains no strong quantifiers

Example

$$\mathrm{sk}(\neg(\forall x)P(x) \vee (\forall x)P(x)) = \neg(\forall x)P(x) \vee P(s)$$

where s is a skolem symbol.

Skolemization in FOL

- Operation sk on formulas
- Focus on proofs: consider validity-preserving sk
- $\mathrm{sk}(F)$ valid iff F valid
- $\mathrm{sk}(F)$ contains no strong quantifiers
- Can be extended to proofs

Proof skolemization

Example

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

Proof skolemization

Example

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

Proof skolemization

Example

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

where s is a skolem symbol.

Properties of Proof Skolemization

- All strong quantifiers are cut-ancestors.
- For cut-free proofs:
  - No strong quantifier rules, hence no eigenvariable conditions!
  - Proofs are closed under substitution.
  - More flexible rule permutations possible.

Applications of Proof Skolemization

- Extremely useful in CERES (cut-elimination by resolution) (Baaz, Leitsch 2000)
- cut-free proof π' obtained from π by
    1. extraction of cut-free proofs $P_1, \ldots, P_n$ from π
    2. computation of resolution refutation γ
    3. composition of instances of the P_i and γ into π'

CERES projection example

Example

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

CERES projection example

Example

$$\dfrac{\dfrac{\dfrac{P(\alpha) \vdash P(\alpha)}{(\forall x)P(x) \vdash P(\alpha)}\ \forall : l}{(\forall x)P(x) \vdash (\forall x)P(x)}\ \forall : r \qquad \dfrac{P(s) \vdash {\color{red}P(s)}}{(\forall x)P(x) \vdash {\color{red}P(s)}}\ \forall : l}{(\forall x)P(x) \vdash {\color{red}P(s)}}\ cut$$

CERES projection example

Example

Projection to $P(s)$:

$$P(s) \vdash P(s)$$

CERES - projection without skolemization?

Example

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

CERES - projection without skolemization?

Example

$$\dfrac{\dfrac{\dfrac{P(\alpha) \vdash P(\alpha)}{(\forall x)P(x) \vdash P(\alpha)}\ \forall : l}{(\forall x)P(x) \vdash (\forall x)P(x)}\ \forall : r \qquad \dfrac{\dfrac{P(\beta) \vdash \color{red}{P(\beta)}}{(\forall x)P(x) \vdash \color{red}{P(\beta)}}\ \forall : l}{(\forall x)P(x) \vdash \color{red}{(\forall x)P(x)}}\ \color{red}{\forall : r}}{(\forall x)P(x) \vdash \color{red}{(\forall x)P(x)}}\ cut$$

CERES - projection without skolemization?

Example

Projection to $P(\beta)$:

$$\frac{P(\beta) \vdash P(\beta)}{P(\beta) \vdash (\forall x)P(x)} \forall : r$$

Not a proof!

Motivation - Skolemization for higher-order **LK**

- Useful to defining CERES for HOL
- Motivation:
  - Regularity theorem: proof with atomic cuts is composition of instances of projections of proof with cuts
  - Tool for applied proof analysis

Skolemization in HOL - History

- Used in an unsound way in P.B. Andrews, *Resolution in Type Theory* (1971)
- Sound higher order skolemization introduced by D. Miller, *A Compact Representation of Proofs* (1987)

Naive approach

- Approach as in FOL:
  1. remove strong quantifiers
  2. insert skolem terms
  3. propagate changes upwards

Naive approach

Example

Consider

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(\beta,a) \vdash P(\beta,a)}{(\forall x)P(x,a) \vdash P(\beta,a)}\ \forall : l}{(\forall x)P(x,a) \vdash (\forall z)P(z,a)}\ \forall : r \qquad \dfrac{\dfrac{P(\alpha,b) \vdash P(\alpha,b)}{(\forall z)P(z,b) \vdash P(\alpha,b)}\ \forall : l}{(\forall z)P(z,b) \vdash (\forall x)P(x,b)}\ \forall : r}{(\forall x)P(x,a), (\forall z)P(z,a) \to (\forall z)P(z,b) \vdash (\forall x)P(x,b)}\ \to : l}{(\forall x)P(x,a), (\forall X)(X(a) \to X(b)) \vdash (\forall x)P(x,b)}\ \forall^2 : l}{(\forall X)(X(a) \to X(b)) \vdash (\forall x)P(x,a) \to (\forall x)P(x,b)}\ \to : r$$

with substitution term $\lambda x.(\forall z)P(z,x)$.

Naive approach

Example

The naive approach fails:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(s_2, a) \vdash P(s_2, a)}{(\forall x)P(x, a) \vdash P(s_2, a)}\ \forall : l \qquad \dfrac{P(s_1, b) \vdash P(s_1, b)}{(\forall z)P(z, b) \vdash P(s_1, b)}\ \forall : l}{(\forall x)P(x, a), P(s_2, a) \rightarrow (\forall z)P(z, b) \vdash P(s_1, b)}\ \rightarrow : l}{(\forall x)P(x, a), (\forall X)(X(a) \rightarrow X(b)) \vdash P(s_1, b)}\ \forall^2 : l}{(\forall X)(X(a) \rightarrow X(b)) \vdash (\forall x)P(x, a) \rightarrow P(s_1, b)}\ \rightarrow : r$$

where the $\forall^2 : l$ rule application is violated.

New approach

- Like Miller — introduce strong quantifier from skolem term
- *Labelled* quantifiers to keep track of skolem term parameters
- Labelled quantifier rules update label and introduce skolem terms

New approach (first-order)

Definition

Labelled quantifier: $(\forall x)^l$, where l is a list of terms

$$\frac{F^t[x \leftarrow t], \Gamma \vdash \Delta}{(\forall x)F, \Gamma \vdash \Delta} \; \forall_{sk} : l$$

F^t is F where t is appended to the label of all strong quantifiers in F.

$$\frac{\Gamma \vdash \Delta, F[x \leftarrow f(t_1 \ldots t_n)]}{\Gamma \vdash \Delta, (\forall x)^{t_1,\ldots,t_n} F} \; \forall_{sk} : r$$

f is a skolem symbol, $f(t_1, \ldots, t_n)$ is the skolem term of the rule.

New approach (first-order)

$$\frac{\Gamma \vdash \Delta, F[x \leftarrow f(t_1 \ldots t_n)]}{\Gamma \vdash \Delta, (\forall x)^{t_1,\ldots,t_n} F} \; \forall_{sk} : r$$

- Rule sound if we have eigensymbol condition (i.e. f does not occur in $\Gamma \cup \Delta$ and F).
- What if we drop this local condition?

New approach (first-order)

$$\frac{\Gamma \vdash \Delta, F[x \leftarrow f(t_1 \ldots t_n)]}{\Gamma \vdash \Delta, (\forall x)^{t_1,\ldots,t_n} F} \; \forall_{sk} : r$$

Definition ($\mathbf{LK}_{\mathrm{sk}}$-tree)

1. $\forall_{sk} : r$, $\forall_{sk} : l$ used for end-sequent ancestors
2. $\forall : r$, $\forall : l$ used for cut ancestors
3. propositional, structural rules of **LK**

New approach (first-order)

Example ($\mathbf{LK}_{\mathrm{sk}}$-tree)

$$\dfrac{\dfrac{\dfrac{\dfrac{P(s) \vdash P(s)}{\vdash P(s), \neg P(s)}\ \neg : r}{\vdash P(s), \forall x \neg P(x)}\ \forall_{sk} : r}{\neg \forall x \neg P(x) \vdash P(s)}\ \neg : l}{\neg \forall x \neg P(x) \vdash \forall x P(x)}\ \forall_{sk} : r$$

$\mathbf{LK}_{\mathrm{sk}}$-trees not sound!

New approach (first-order)

Definition ($\mathbf{LK}_{\mathrm{sk}}$-preproof)

$\mathbf{LK}_{\mathrm{sk}}$-tree with end-sequent S s.t.

1. S contains neither skolem symbols nor labelled quantifiers and
2. for every two distinct strong labelled quantifier rules with common skolem term t, they are homomorphous.

New approach (first-order)

Definition ($\mathbf{LK}_{\mathrm{sk}}$-preproof)

$\mathbf{LK}_{\mathrm{sk}}$-tree with end-sequent S s.t.

1. S contains neither skolem symbols nor labelled quantifiers and
2. for every two distinct strong labelled quantifier rules with common skolem term t, they are homomorphous.

Definition (Homomorphous rules)

ρ_1, ρ_2 rule applications of the same type with auxiliary occurrences α_1 and α_2. ρ_1, ρ_2 *homomorphous* if there is an application of contraction with auxiliary occurrences γ_1, γ_2 and the sequences of main formulas on the paths from α_1 to γ_1 and α_2 to γ_2 exist and are equal.

Showing soundness

Theorem (Soundness of cut-free $\mathbf{LK}_{\mathrm{sk}}$)

Let π be a cut-free $\mathbf{LK}_{\mathrm{sk}}$*-preproof of S. Then there exists a cut-free* **LK***-proof of S.*

Proof.

By permuting $\forall_{sk} : r$ rules down s.t. there are no eigenterm violations. Then, we replace skolem terms by eigenvariables and $\forall_{sk} : r$ rules by $\forall : r$ rules. □

Showing soundness

Theorem (Soundness of cut-free $\mathbf{LK}_{\mathrm{sk}}$)

Let π be a cut-free $\mathbf{LK}_{\mathrm{sk}}$-preproof of S. Then there exists a cut-free **LK***-proof of S.*

Theorem (Cut-elimination)

Let π be an $\mathbf{LK}_{\mathrm{sk}}$-preproof of S. Then there exists a cut-free $\mathbf{LK}_{\mathrm{sk}}$-preproof of S.

Proof.

Using the CERES method and elimination of atomic cuts. □

Showing soundness

Theorem (Soundness of cut-free $\mathbf{LK}_{\mathrm{sk}}$)

Let π be a cut-free $\mathbf{LK}_{\mathrm{sk}}$-preproof of S. Then there exists a cut-free $\mathbf{LK}$-proof of S.

Theorem (Cut-elimination)

Let π be an $\mathbf{LK}_{\mathrm{sk}}$-preproof of S. Then there exists a cut-free $\mathbf{LK}_{\mathrm{sk}}$-preproof of S.

Theorem (Soundness)

Let π be an $\mathbf{LK}_{\mathrm{sk}}$-preproof of S. Then there exists an $\mathbf{LK}$-proof of S.

Example revisited

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{P(s_2, a) \vdash P(s_2, a)}{(\forall x)P(x, a) \vdash P(s_2, a)}\ \forall : l
}{(\forall x)P(x, a) \vdash (\forall z)P(z, a)}\ \forall_{sk} : r
\qquad
\dfrac{
\dfrac{P(s_1, b) \vdash P(s_1, b)}{(\forall z)P(z, b) \vdash P(s_1, b)}\ \forall : l
}{(\forall z)P(z, b) \vdash (\forall x)P(x, b)}\ \forall_{sk} : r
}{(\forall x)P(x, a), (\forall z)P(z, a) \to (\forall z)P(z, b) \vdash (\forall x)P(x, b)}\ \to : l
}{(\forall x)P(x, a), (\forall X)(X(a) \to X(b)) \vdash (\forall x)P(x, b)}\ \forall^2 : l
}{(\forall X)(X(a) \to X(b)) \vdash (\forall x)P(x, a) \to (\forall x)P(x, b)}\ \to : r
$$

Possible Applications

- First-order CERES (elimination of single cuts)
  - May avoid deskolemization step when combining proofs
- Higher-order CERES
- Other applications involving rule permutations

Second-order CERES example

- $\mathbf{LK}^2_{\mathrm{sk}}$
  - Cut ancestors: $\mathbf{LK^2}$ rules
  - End-sequent ancestors: $\mathbf{LK}_{\mathrm{sk}} + \forall^2_{sk} : r + \forall^2_{sk} : l$ quantifier rules

$\pi =$

$$\frac{\pi_1 \qquad \pi_2}{(\forall X)(X(a) \to X(b)) \vdash (\exists x)\neg P(x,a) \lor P(c,b)}\; cut$$

Second-order CERES example

$\pi_1 =$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(s_2, a) \vdash P(s_2, a)}{(\forall x)P(x, a) \vdash P(s_2, a)}\ \forall : l}{(\forall x)P(x, a) \vdash (\forall z)P(z, a)}\ \forall_{sk} : r \qquad \dfrac{\dfrac{P(\alpha, b) \vdash P(\alpha, b)}{(\forall z)P(z, b) \vdash P(\alpha, b)}\ \forall : l}{(\forall z)P(z, b) \vdash (\forall x)P(x, b)}\ \forall : r}{(\forall x)P(x, a), (\forall z)P(z, a) \to (\forall z)P(z, b) \vdash (\forall x)P(x, b)}\ \to: l}{(\forall x)P(x, a), (\forall X)(X(a) \to X(b)) \vdash (\forall x)P(x, b)}\ \forall^2 : l}{(\forall X)(X(a) \to X(b)) \vdash (\forall x)P(x, a) \to (\forall x)P(x, b)}\ \to: r
$$

Second-order CERES example

$\pi_2 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{P(\beta, a) \vdash P(\beta, a)}{\vdash P(\beta, a), \neg P(\beta, a)}\ \neg : r}{\vdash P(\beta, a), (\exists x)\neg P(x, a)}\ \exists : r}{\vdash (\forall x)P(x, a), (\exists x)\neg P(x, a)}\ \forall : r \quad \dfrac{P(c, b) \vdash P(c, b)}{(\forall x)P(x, b) \vdash P(c, b)}\ \forall : l}{\dfrac{(\forall x)P(x, a) \to (\forall x)P(x, b) \vdash (\exists x)\neg P(x, a), P(c, b)}{(\forall x)P(x, a) \to (\forall x)P(x, b) \vdash (\exists x)\neg P(x, a) \lor P(c, b)}\ \lor : r}\ \to : l$$

Second-order CERES example

$$CL(\pi) = \{\vdash P(\beta, a); \quad P(c, b) \vdash; \quad P(s_2, a) \vdash P(\alpha, b)\}$$

$\gamma =$

$$\dfrac{\dfrac{\vdash P(s_2, a) \qquad P(s_2, a) \vdash P(c, b)}{\vdash P(c, b)} \qquad P(c, b) \vdash}{\vdash}$$

$$\sigma = [\beta \leftarrow s_2, \alpha \leftarrow c]$$

Second-order CERES example - ACNF

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(s_2,a) \vdash P(s_2,a)}{\vdash P(s_2,a), \neg P(s_2,a)}\ \neg : r}{\vdash P(s_2,a), (\exists x)\neg P(x,a)}\ \exists : r}{\vdash P(s_2,a), (\exists x)\neg P(x,a), P(c,b)}\ w : r}{\vdash (\exists x)\neg P(x,a) \lor P(c,b), P(s_2,a)}\ \lor : r
\quad
\dfrac{\dfrac{\dfrac{P(s_2,a) \vdash P(s_2,a)}{P(s_2,a) \vdash (\forall z)P(z,a)}\ \forall_{sk} : r \quad \dfrac{P(c,b) \vdash P(c,b)}{(\forall z)P(z,b) \vdash P(c,b)}\ \forall : l}{P(s_2,a), (\forall z)P(z,a) \to (\forall z)P(z,b) \vdash P(c,b)}\ \to : l}{P(s_2,a), (\forall X)(X(a) \to X(b)) \vdash P(c,b)}\ \forall^2 : l}{(\forall X)(X(a) \to X(b)) \vdash P(c,b), (\exists x)\neg P(x,a) \lor P(c,b)}\ cut
$$

Second-order CERES example - rank reduced

$$\dfrac{P(s_2,a) \vdash P(s_2,a) \qquad P(s_2,a) \vdash P(s_2,a)}{P(s_2,a) \vdash P(s_2,a)}\ cut$$

$$\dfrac{P(s_2,a) \vdash P(s_2,a)}{P(s_2,a) \vdash (\forall z)P(z,a)}\ \forall_{sk} : r$$

$$\dfrac{P(s_2,a) \vdash (\forall z)P(z,a)}{\vdash (\forall z)P(z,a), \neg P(s_2,a)}\ \neg : r$$

$$\dfrac{\vdash (\forall z)P(z,a), \neg P(s_2,a)}{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a)}\ \exists : r$$

$$\dfrac{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a)}{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a), P(c,b)}\ w : r$$

$$\dfrac{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a), P(c,b)}{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a) \vee P(c,b)}\ \vee : r \qquad \dfrac{P(c,b) \vdash P(c,b)}{(\forall z)P(z,b) \vdash P(c,b)}\ \forall : l$$

$$\dfrac{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a) \vee P(c,b) \qquad (\forall z)P(z,b) \vdash P(c,b)}{(\forall z)P(z,a) \rightarrow (\forall z)P(z,b) \vdash P(c,b), (\exists x)\neg P(x,a) \vee P(c,b)}\ \rightarrow : l$$

$$\dfrac{(\forall z)P(z,a) \rightarrow (\forall z)P(z,b) \vdash P(c,b), (\exists x)\neg P(x,a) \vee P(c,b)}{(\forall X)(X(a) \rightarrow X(b)) \vdash P(c,b), (\exists x)\neg P(x,a) \vee P(c,b)}\ \forall^2 : l$$

Second-order CERES example - deskolemized

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{P(s_2,a) \vdash P(s_2,a) \qquad P(s_2,a) \vdash P(s_2,a)}{P(s_2,a) \vdash P(s_2,a)}\; cut
}{\vdash P(s_2,a), \neg P(s_2,a)}\; \neg : r
}{\vdash P(s_2,a), (\exists x)\neg P(x,a)}\; \exists : r
}{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a)}\; {\color{green}\forall_{sk} : r}
}{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a), P(c,b)}\; w : r
}{\vdash (\forall z)P(z,a), (\exists x)\neg P(x,a) \vee P(c,b)}\; \vee : r
\qquad
\dfrac{P(c,b) \vdash P(c,b)}{(\forall z)P(z,b) \vdash P(c,b)}\; \forall : l
}{(\forall z)P(z,a) \rightarrow (\forall z)P(z,b) \vdash P(c,b), (\exists x)\neg P(x,a) \vee P(c,b)}\; \rightarrow : l
}{(\forall X)(X(a) \rightarrow X(b)) \vdash P(c,b), (\exists x)\neg P(x,a) \vee P(c,b)}\; \forall^2 : l
$$

Conclusion

- Skolemization integral to first-order CERES method
- Labelled quantifier rules hopefully suitable higher-order generalization
- Preliminary results in first-order logic and working examples in higher-order logic

Peter B. Andrews.
Resolution in Type Theory.
Journal of Symbolic Logic, 36(3):414–432, September 1971.

Matthias Baaz and Alexander Leitsch.
Cut-elimination and Redundancy-elimination by Resolution.
Journal of Symbolic Computation, 29(2):149–176, 2000.

Dale A. Miller.
A compact representation of proofs.
Studia Logica, 46(4):347–370, December 1987.