Translation of Resolution Proofs into Short First-Order Proofs without Choice Axioms

Hans de Nivelle

Max Planck Institut für Informatik, Saarbrücken

25.04.2003

Abstract

I present a way of generating proofs from resolution proofs containing Skolemization. The resulting proofs are purely first-order, i.e. do not make use of 'choice axioms', 'satisfiability preserving proof steps', etc.

The resulting firts-order proofs are short, i.e. polynomial in the output of the theorem prover.

Motivation 1

Theorem provers are complicated pieces of software. Complicated software can be incorrect. Theorem provers are used for verification of critical software. One needs a way of being able to trust theorem provers without any hesitation. There are 3 approaches:

1. Verify the prover as it is. Difficult, because the prover is big and changing (being tuned to applications)

2. Make sure that the prover uses a 'trusted code base'. Only the trusted code base needs to be verified.

3. Let the prover produce explicit proofs which can be checked independently.

Approach 2 and 3 are closely related. For 2, one has to generate the proof 'procedurally'. For 3, one has to store it.

Motivation 2

I confess, the previous slide only partially motivates this work.

As far as Motivation 1 is concerned, it does not matter whether one uses choice axioms or not.

Using choice axioms for proving first-order formulas is ugly.
Resolution is disliked by many people because of Skolemization.

Main Idea:

The problem with choice functions is that they choose, which is not sound in first-order logic.
Therefore, do not choose. Use Skolem relations.
Let $\forall x \; p(x, f(x))$, be a clause with f a Skolem function.

Replace it by

$$\forall x \; \forall \alpha \; F(x, \alpha) \rightarrow p(\alpha).$$

Similarly, $p(x, f(f(x)) \;)$ can be replaced by

$$\forall x \; \forall \alpha\beta \; F(x, \alpha) \rightarrow F(\alpha, \beta) \rightarrow p(\beta).$$

Surprising Fact:

It is possible to replace functions by relations in resolution proofs on the conditions that

1. The relations introduced are serial.
2. Paramodulation is simultaneous.

Seriality means: $\forall x_1 \cdots x_n \; \exists y \; F(x_1, \ldots, x_n, y)$ is provable.
Simultaneous Paramodulation means the following:
If $t_1 \approx t_2 \vee R_1$ paramodulates with $A[t_1] \vee R_2$, then all occurrences of t_1 in A and R_2 have to be replaced by t_2.

This restriction of paramodulation is complete, and commonly implemented because it is more efficient.

Definition We assume a global function $[\ ]$, which

- assigns to each n-ary function symbol an $n+1$-ary relation.
- assigns to each functional term t a new variable.

Definition For a literal/quantifier free formula A, $[A]$ is obtained by replacing all terms t in A by their corresponding $[t]$.

For a term/literal/quantifier free formula, $\mathrm{Var}(A)$ is the set of variables introduced by $[A]$.

For a term/literal/quantifier free formula, $\mathrm{Def}(A)$ is the set of definitions characterizing the variables introduced by $[A]$.

Example

Assume that $[f] = F, \quad [f(x)] = \alpha,\ [f(f(x))] = \beta.$

Then:

$[p(f(x))] = p(\alpha),$

$[q(f(x), f(f(x)))\ ] = q(\alpha, \beta),$

$\mathrm{Var}(p(f(x))\ ) = \{\alpha\},$

$\mathrm{Var}(q(f(x), f(f(x)))\ ) = \{\alpha, \beta\}.$

$\mathrm{Def}(p(f(x))\ ) = \{F(x, \alpha)\}.$
$\mathrm{Def}(q(f(x), f(f(x)))\ ) = \{F(x, \alpha),\ F(\alpha, \beta)\}.$

For sake of simplicity, we assume that all functions are replaced by relations. One can always replace an n-ary non-Skolem function $f(t_1, \ldots, t_n)$ by the $(n+1)$-ary relation $\alpha \approx f(t_1, \ldots, t_n)$.

Using the previous definitions, a clause $\forall \overline{x}\ A_1 \vee \cdots \vee A_p$ can be replaced by
$\forall \overline{x}\ \forall\ \mathrm{Var}(A_1, \ldots, A_p)\ \ \mathrm{Def}(A_1, \ldots, A_p) \rightarrow [A_1] \vee \cdots \vee [A_p]$.

Theorem

Let $\forall \overline{x}\ C$ be a clause. Let $\forall \overline{y}\ D$ be obtained by factoring/equality factoring/equality reflexivity.

Then $\forall \overline{y}\ \ \forall\ \mathrm{Var}(D)\ \ \mathrm{Def}(D) \rightarrow [D]$ can be proven from $\forall \overline{x}\ \ \forall\ \mathrm{Var}(C)\ \ \mathrm{Def}(C) \rightarrow [C]$.

Let $\forall \overline{x}_1\ C_1$ and $\forall \overline{x}_2\ C_2$ be clauses. Let $\forall \overline{y}\ D$ be derived by resolution/simultaneous paramodulation. Then $\forall \overline{y}\ \ \forall\ \mathrm{Var}(D)\ \ \mathrm{Def}(D) \rightarrow [D]$ can be proven from

$\forall \overline{x}_1\ \ \forall\ \mathrm{Var}(C_1)\ \ \mathrm{Def}(C_1) \rightarrow [C_1]$, and

$\forall \overline{x}_2\ \ \forall\ \mathrm{Var}(C_2)\ \ \mathrm{Def}(C_2) \rightarrow [C_2]$.

Some highlights of the proof follow:

Proof (Instantiation)

Assume that $\forall \overline{x}\ C$ has instance $\forall \overline{y}\ D$. Then

$C' = \forall \overline{x}\ \ \forall\ \mathrm{Var}(C)\ \ \mathrm{Def}(C) \rightarrow [C]$ subsumes

$D' = \forall \overline{y}\ \ \forall\ \mathrm{Var}(D)\ \ \mathrm{Def}(D) \rightarrow [D]$.

We show this for simple instantiations.

- If $\forall \overline{y}\ D$ is obtained by merging two variables in $\overline{x}$, one can merge the same variables in C', together with the variables in $\mathrm{Var}(C)$ corrresponding to terms that become equal after the merging.

- If $\forall \overline{y}\ D$ is obtained by assigning a term $f(z_1, \ldots, z_n)$ to a variable x, then D' has form $\forall z_1 \cdots z_n\ \forall (\overline{x} \backslash \{x\})\ \forall\ \mathrm{Var}(C), x\ \ F(z_1, \ldots, z_n, x) \rightarrow \mathrm{Def}(C) \rightarrow [C]$.

More complicated instantiations can be obtained by iteration.

Proof (Equality Reflexivity)

Assume that $\forall \overline{x}\ C$ is obtained from $\forall \overline{x}\ \ t \not\approx t \vee C$ by equality reflexivity.

We need to show that
$\forall \overline{x}\ \forall\ \mathrm{Var}(t \not\approx t, C)\ \ \mathrm{Def}(t \not\approx t, C) \rightarrow [t \not\approx t \vee C]$ implies
$\forall \overline{x}\ \forall\ \mathrm{Var}(C)\ \ \mathrm{Def}(C) \rightarrow [C]$.

If $\mathrm{Def}(C) \subset \mathrm{Def}(t \not\approx t, C)$, then there are terms in t that do not occur in C. Let u be an outermost such term. Let $[u] = \alpha$. Then $\mathrm{Def}(t \not\approx t, C) \backslash \mathrm{Def}(C)$ contains an atom $F(\beta_1, \ldots, \beta_n, \alpha)$, defining α. This atom can be removed through the seriality axiom for F.

Repeating this procedure, all atoms $\mathrm{Def}(t \not\approx t, C) \backslash \mathrm{Def}(C)$ can be removed.

This is the only point where seriality is used.

Proof (Paramodulation)

Assume that $\forall \overline{x}\ t_1 \approx t_2$ rewrites $\forall \overline{x}\ A[t_1]$ into $\forall \overline{x}\ t_1 \not\approx t_1 \vee t_2 \not\approx t_2 \vee A[t_2]$.

For sake of simplicity, the disjunctional part in the equality is omitted, and it is ensured that there are no disappearing terms.

One needs to prove

$$\forall \overline{x}\ \ \forall\ \mathrm{Var}(t_1 \not\approx t_1, t_2 \not\approx t_2, A[t_2])\ \mathrm{Def}(t_1 \not\approx t_1, t_2 \not\approx t_2, A[t_2])$$

$$\rightarrow [t_1 \not\approx t_1 \vee t_2 \not\approx t_2 \vee A[t_2]\ ]$$

from

$\forall \overline{x}\ \ \forall\ \mathrm{Var}(A[t_1])\ \mathrm{Def}(A[t_1]) \rightarrow [A[t_1]\ ]$.

$\forall \overline{x}\ \ \forall\ \mathrm{Var}(t_1, t_2)\ \mathrm{Def}(t_1, t_2) \rightarrow [t_1 \approx t_2]$

Failure in the case of non-simultaneous paramodulation

The method fails in the case of non-simultaneous paramodulation:

Suppose that $a \approx b$ is applied on $s(a) \approx s(a)$ to obtain $s(a) \approx s(b)$.

The translation of $s(a) \approx s(a)$ equals $\forall \alpha \; S(a, \alpha) \rightarrow \alpha \approx \alpha$, which is a tautology.

The translation of $s(a) \approx s(b)$ equals
$\forall \alpha \beta \; S(a, \alpha) \rightarrow S(b, \beta) \rightarrow \alpha = \beta$, which is a choice axiom for S on $a (\approx b)$

Skolemization

We have shown that it is possible to replace functions by serial relations in resolution proofs. It remains to obtain the relations. The relations must have two properties:

1. The translated clauses must follow from the original formula.
2. Seriality of the relation must follow from the original formula.

A Skolem function f originates from Skolemizing some formula $\forall x_1 \cdots x_n \; \exists y \; A(x_1, \dots, x_n, y)$.

Simply take A as the serial relation for f :

1. $\forall x_1 \cdots x_n \forall y \; A(x_1, \dots, x_n, y) \rightarrow A(x_1, \dots, x_n, y)$ is a tautology.
2. $\forall x_1 \cdots x_n \exists y \; A(x_1, \dots, x_n, y)$ is the original formula.

Using this approach, there are two problems:

Small Problem: Skolemization in a context

Consider the formula
$\forall x_1 \cdots x_n \; A(x_1, \ldots, x_n) \to \exists y \; B(x_1, \ldots, x_n, y)$, which Skolemizes into $\forall x_1 \cdots x_n \; A(x_1, \ldots, x_n) \to B(x_1, \ldots, x_n, f(x_1, \ldots, x_n))$.

Here the existential quantifiers occurs in a conditional context.

Simply encode the context into the relation:
$F(x_1, \ldots, x_n, y) := A(x_1, \ldots, x_n) \to B(x_1, \ldots, x_n, y)$.

Then the translation
$\forall x_1 \cdots x_n \; A(x_1, \ldots, x_n) \to \forall y \; F(x_1, \ldots, x_n, y) \to B(x_1, \ldots, x_n, y)$
is a tautology, and $\forall x_1 \cdots x_n \; \exists y \; F(x_1, \ldots, x_n, y)$ is equivalent to the original formula.

Big Problem: Parallel Skolemization:

Consider the formula $\forall x \ \exists y_1 y_2 \ p(x, y_1, y_2)$,

Its Skolemization equals $\forall x \ p(x, f_1(x), f_2(x) \ )$.

This would translate into
$\forall x \ \forall y_1 y_2 \ F_1(x, y_1) \rightarrow F_2(x, y_2) \rightarrow p(x, y_1, y_2)$.

In the original formula, y_2 is chosen after y_1. In the Skolemization, f_1 and f_2 have to choose in parallel.

As a consequence, in the translation, F_1 and F_2 do not know about each other's choice. There seems to be no way to define F_1 and F_2 independently, such that they are serial and the translation of the Skolemization becomes provable.

Solution: Inner Skolemization

Skolemization is usually performed outside-inside, because this results in smaller Skolem terms. If one Skolemizes inside-outside, the 'lack-of-knowledge' problem disappears, because each Skolem-term receives all variables on which it depends.

$\forall x \; \exists y_1 y_2 \; p(x, y_1, y_2)$ Skolemizes into $\forall x \; \exists y_1 \; p(x, y_1, f_2(x, y_1) \;)$, which in turn Skolemizes into $\forall x \; p(x, f_1(x), f_2(x, f_1(x)) \;)$.

Inside-outside Skolemization results in bigger Skolem terms. In the example $f_2(x, f_1(x))$ is bigger than $f_2(x)$.

Theorem: Let F be some first-order formula. Let F_1 be its inner Skolemization. Let F_2 be its outer Skolemization. Let y be an existential variable in F. Let t_1 be its Skolem term in F_1. Let t_2 be its Skolem term in F_2. Then t_1 and t_2 contain exactly the same variables.

proof: (very sketchy)

For both F_1, F_2, a variable x, belonging to subformula $\forall x\ A$ of F, is in the Skolem term for y iff
there is a sequence of existentially quantified subformulas $\exists y_1\ B_1,\ \exists y_2\ B_2, \ldots, \exists y_n\ B_n$ of F, such that **(1)** $\exists y_1\ B_1$ is in the scope of A, and x occurs in B_1, **(2)** each $\exists y_{i+1}\ B_{i+1}$ is in the scope of B_i, and y_i occurs in B_{i+1}, **(3)** $y_n = y$.

It remains to observe the following: A resolution proof remains valid if one replaces some function symbol f by a complex term depending on the same subterms, as follows:

$$f(x_1, \ldots, x_n) \Rightarrow t[x_1, \ldots, x_n].$$

As a consequence, a proof remains valid if one replaces all outermost Skolemizations by innermost Skolemizations. Innermost Skolemization is bad for proof search, but it does not increase the proof length.

This completes the procedure: On constructs the outer Skolemization and lets the prover run. If it finds a proof, one first replaces it by the proof of the outer Skolemization. After that, one replaces the Skolem functions in it by serial relations, and the result is a purely first-order proof.

Conclusions, Future Work

- I presented a way of removing Skolem functions from resolution proofs, without increasing their size significantly.
- The method can be adapted to handle the splitting rule as well.
- Can this be used in the presence of theories, for example AC? (What does 'simultaneous paramodulation' actually mean in the context of AC?)