Available online at www.sciencedirect.com
SCIENCE DIRECT®
Information and Computation 199 (2005) 24–54
Information and Computation
www.elsevier.com/locate/ic

Translation of resolution proofs into short first-order proofs without choice axioms

Hans de Nivelle *

Max-Planck Institut für Informatik, Stuhlsatzenhausweg 85, 66123 Saarbrücken, Germany

Received 8 December 2003; revised 31 August 2004
Available online 7 April 2005

Abstract

We present a way of transforming a resolution-style proof containing Skolemization into a natural deduction proof without Skolemization. The size of the proof increases only moderately (polynomially). This makes it possible to translate the output of a resolution theorem prover into a purely first-order proof that is moderate in size.

MSC: 68T15; 03F20; 03F05

Keywords: Theorem proving; Proof theory; Skolemization

1. Introduction

If one wants a resolution based theorem prover to generate explicit proofs, one has to decide what to do with Skolemization. One possibility is to allow Skolemization (or equivalently the axiom of choice) as a proof principle. In that case, the resolution proof can be translated more or less one-to-one into a natural deduction proof. In [10] it is described how to do this efficiently

* Fax: +49 681 9325 299.
E-mail address: nivelle@mpi-sb.mpg.de.
URL: www.mpi-sb.mpg.de/∼nivelle.

0890-5401/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ic.2004.10.011

for the clausal normal form (CNF) transformation. In [6,7], a hybrid method was developed. For resolution on the clause level, explicit proofs were generated. For the CNF-transformation, an algorithm was developed inside COQ and proven correct. Using this approach, explicit generation of proofs for the CNF-transformation could be avoided. (Although strictly seen, inside COQ, the term defining the algorithm also defines a proof principle.) A related approach was taken in [14], using the Boyer–Moore theorem prover instead of COQ. Both approaches use the axiom of choice. In [6], the axiom of choice was used for proving the clausification algorithm correct. In [14], it is assumed that domains are finite, which implies the axiom of choice.

Another possibility is to completely eliminate the Skolemization steps from the proof. If one is interested in correctness only, the axiom of choice is certainly acceptable, but it is much more elegant to avoid using the axiom of choice at all in proofs of first-order formulas. Until recently, the only known way of eliminating applications of Skolemization from a proof made use of cut elimination. Because of this, these methods can cause a hyperexponential increase in proof size in the worst case, see [21] or [18], or also [4]. In [19], such an algorithm is described in detail. In [13], an improved method is given, which is optimized towards readability of the resulting proof. This method has been implemented in Ωmega by Andreas Meijer (see [20]).

In [1], a method for eliminating Skolem functions from first-order proofs was presented, which results in proofs of polynomial size. The method works only in the context of a theory that is strong enough to encode finite functions. This is a weak requirement, because for example axiomatizations of common data structures, like lists or arrays would suffice. The finite functions are used to approximate the Skolem functions through an internalized forcing argument. We think that the method could be implemented, but it would not work in the general first-order case.

The general problem whether Skolem functions can be efficiently eliminated from every first-order logic proof seems to be open, see the table in [8, p. 9].

In this paper, we give a general method for eliminating Skolem functions from *resolution proofs*, which can be implemented and expected to be efficient. In addition, it is *structure preserving*, by which we mean that it does almost not change the structure of the proof. The main idea is the following: Assume that f is a Skolem function in the clausal formula $\forall x\ p(x) \vee q(f(x))$.[1] Then f can be replaced by a binary relation F as follows: $\forall x \alpha\ F(x,\alpha) \rightarrow p(x) \vee q(\alpha)$. It turns out that if one replaces Skolem functions by relations in a resolution proof, and for each relation one can show *seriality*, then the result will still be a valid first-order proof. The surprising fact is that resolution does not make use of the functionality of F, only of its seriality. Because f is a Skolem function, it originates from a formula of form $\forall x \exists y\ F(x,y)$. Hence, F can be taken as serial relation. Proofs containing paramodulation steps can also be handled. There is only one restriction on the use of paramodulation, namely that it has to be *simultaneous in the Skolem functions*. Simultaneous in the Skolem functions means that whenever an equality $t_1 \approx t_2$ is applied inside a Skolem term, *all* instances of t_1 that are inside some Skolem term have to be replaced by t_2. The completeness of this restriction follows from the fact that one does not have to paramodulate at all into Skolem terms for completeness. This was proven in [5], and generally accepted as an efficient restriction of resolution.

We will give an example of a complete transformation. Consider the set of first-order formulas, given in Fig. 1. The set is unsatisfiable, because the first formula requires that there exists a chain of

[1] When writing a first-order formula, we assume that the scope of a quantifier extends as far to the right as possible.