Available online at www.sciencedirect.com
SCIENCE DIRECT®

Electronic Notes in Theoretical Computer Science

ELSEVIER Electronic Notes in Theoretical Computer Science 117 (2005) 153–182
www.elsevier.com/locate/entcs

Symbolic Reachability Analysis Using Narrowing and its Application to Verification of Cryptographic Protocols*

José Meseguer and Prasanna Thati

Department of Computer Science, UIUC, Urbana-Champaign, USA

Abstract

Narrowing was introduced, and has traditionally been used, to solve equations in initial and free algebras *modulo* a set of equations E. This paper proposes a generalization of narrowing which can be used to solve *reachability goals* in initial and free models of a rewrite theory $\mathcal{R}$. We show that narrowing is sound and weakly complete (i.e., complete for normalized solutions) under reasonable executability assumptions about $\mathcal{R}$. We also show that in general narrowing is not strongly complete, that is, not complete when some solutions can be further rewritten by $\mathcal{R}$. We then identify several large classes of rewrite theories, covering many practical applications, for which narrowing is strongly complete. Finally, we illustrate an application of narrowing to analysis of cryptographic protocols.

Keywords: Rewriting logic, narrowing, reachability, security protocols.

1 Introduction

This paper addresses the following technical question. Given a rewrite theory $\mathcal{R}$ satisfying reasonable assumptions, is there a general deductive procedure to solve *reachability problems* for $\mathcal{R}$? By a "reachability problem" we mean the obvious, that is, an existential formula

$$(\exists \overrightarrow{x})\ t \rightarrow^* t'$$

or, more generally, an existentially quantified conjunction of such reachability goals. Since $\mathcal{R}$ typically specifies either a concurrent system or an inference

* Research supported by ONR Grant N00014-02-1-0715 and NSF Grant CCR-0234524

1571-0661/$ – see front matter
doi:10.1016/j.entcs.2004.06.024

system, the meaning and interest of solving such goals is quite obvious. The terms t and t' denote sets of states in the initial model of $\mathcal{R}$, and we want to know for what subset of the states denoted by t we can reach the set denoted by t'. Under finite state assumptions, questions of this kind can be answered by model checking techniques [9]. Our interest, however, is in general methods that do not require finiteness assumptions and can complement such model checking techniques. In this paper, we generalize *narrowing* from a technique for solving equality goals [16,21,23] to one for solving reachability goals; indeed equational narrowing goals can be viewed as a special case of reachability goals.

That narrowing in this more general sense should be developed as a method for analyzing concurrent systems and should fit within a wider spectrum of analysis capabilities, was first proposed in [12]. One can view narrowing as a new form of "symbolic model checking", available also for infinite state systems, where the word "symbolic", instead of having the more restricted sense of representing finite sets of states by Boolean propositions, is widened to mean the representation of possibly infinite sets of states by terms with logical variables. These methods could even have useful applications in the case of finite-state systems that are too large to analyze by standard model checking techniques.

There are indeed a number of techniques actively investigated to analyze infinite state systems, including model checking for suitable subclasses, e.g. [4,5,15,17], abstraction techniques, e.g. [10,26,19,25,40], tree-automata based reachability analyses, e.g. [18,35], and theorem proving, e.g. [37,36]. We think that narrowing is a promising additional technique to be further explored. Indeed, narrowing like techniques have already been shown useful in the analysis of cryptographic protocols [2,22,29].

We formally define narrowing for *order-sorted unconditional* rewrite theories of the form $\mathcal{R} = (\Sigma, E, R)$ where $E = \Delta \cup B$, with Δ confluent and terminating modulo B. We prove soundness of solutions found for reachability problems using narrowing, and also show that the narrowing procedure is *weakly* complete in the following sense: if ρ is a solution of a given reachability problem and ρ is normalized with respect to rewriting with the rules R modulo E, then the narrowing procedure finds a solution η that subsumes ρ modulo E. This weak completeness result holds under reasonable executability assumptions about the given rewrite theory.

We also show that in general, narrowing is *not* complete in the following stronger sense: if ρ is a (not necessarily normalized) solution of a reachability goal, then the narrowing procedure finds a solution η that subsumes ρ modulo E. Hence the "weakness" in completeness of narrowing. This does not hold in general, as we show by several examples. The point is that in equational