J Autom Reasoning (2013) 51:431–451
DOI 10.1007/s10817-013-9274-9

Finite Reasons for Safety

Parameterized Verification by Finite Model Finding

Alexei Lisitsa

Received: 31 May 2011 / Accepted: 27 January 2013 / Published online: 23 February 2013

Abstract In this paper we investigate to what extent a very simple and natural "reachability as deducibility" approach, originating in research on formal methods for security, is applicable to the automated verification of large classes of infinite state and parameterized systems. In this approach the verification of a safety property is reduced to the purely logical problem of finding a countermodel for a first-order formula. This task is delegated then to generic automated finite model building procedures. A finite countermodel, if found, provides with a concise representation for a system invariant sufficient to establish the safety. In this paper we first present a detailed case study on the verification of a parameterized mutual exclusion protocol. Further we establish the relative completeness of the finite countermodel finding method (FCM) for a class of parameterized linear arrays of finite automata with respect to known methods based on monotonic abstraction and symbolic backward reachability. The practical efficiency of the method is illustrated on a set of verification problems taken from the literature using Mace4 model finding procedure.

Keywords Finite model finding · Parameterized verification · Mutual exclusion · Monotonic abstraction · Regular invariants

1 Introduction

The verification of infinite state systems and parameterized systems is, in general, an undecidable algorithmic problem. That means the search for efficient procedures to tackle larger and larger subclasses of verification tasks will never end. In this paper

A. Lisitsa (✉)
Department of Computer Science,
University of Liverpool, Liverpool, UK
e-mail: A.Lisitsa@liverpool.ac.uk