Advances in Space and Time Efficient Model Checking of Finite State Systems

Atanas Nikolaev Parashkevov

Thesis submitted for the degree of
Doctor of Philosophy
in
The University of Adelaide
(Faculty of Engineering, Computer and Mathematical Sciences)

November 2002

Contents

Abstract

The complexity of today's computer and electronic systems has reached a point where traditional approaches for design verification—simulation, testing, and reviews—are no longer sufficient. The cost of design defects slipping into production has also sharply increased.

Formal verification holds the promise of a more robust, complete and hopefully automated approach to ensuring that these systems implement their desired behaviour. However, a phenomenon known as state space explosion limits the size of systems that can be handled successfully. This thesis studies automated formal verification techniques and their associated space and time implementation complexity when applied to finite state concurrent systems. In particular, the focus is on concurrent systems expressed in the Communicating Sequential Processes (CSP) framework. The large body of work on CSP includes a process description language, a set of semantic models—traces, failures, and failures-divergences, as well as formal notions of process refinement and equivalence.

An approach to the compilation of CSP system descriptions into boolean formulae in the form of Ordered Binary Decision Diagrams (OBDD) is presented. This representation of CSP semantics is further utilised by a basic algorithm that checks a refinement or equivalence relation between a pair of processes in any of the three CSP semantic models. The performance of this algorithm is studied on a set of benchmark examples and a comparative analysis of its strengths and weaknesses in relation to explicit on-the-fly model checking is performed. This analysis identifies the major factors affecting the performance of OBDD-based refinement checking.

The performance bottlenecks of the basic refinement checking algorithms are identified and addressed with the introduction of a number of novel techniques and algorithms. Hierarchical partitioned transition relations provide an alternative to monolithic transition relations which may grow too large for certain problems. A pseudo-root state approach is developed to reduce the number of states that need to be stored during reachability analysis. A partial order technique—the sleep set method—is applied to OBDD-based refinement checking, which significantly reduces the verification run-time. The pseudo-root state

and sleep set methods are synergistically combined to obtain lower space and time requirements for reachability analysis than either of these techniques alone can provide. We utilise the full abstraction property of the CSP semantics to reduce a CSP refinement checking problem into a reachability problem that can be solved efficiently using OBDDs and enables the application of SAT-based and semi-formal verification techniques.

The algorithms described in this thesis are implemented in the Adelaide Refinement Checking tool.