Shankar, Natarajan
Combining theorem proving and model checking through symbolic analysis. (English)

Zbl 0999.68523

Summary: Automated verification of concurrent systems is hindered by the fact that the state spaces are either infinite or too large for model checking, and the case analysis usually defeats theorem proving. Combinations of the two techniques have been tried with varying degrees of success. We argue for a specific combination where theorem proving is used to reduce verification problems to finite-state form, and model checking is used to explore properties of these reductions. This decomposition of the verification task forms the basis of the Symbolic Analysis Laboratory (SAL), a framework for combining different analysis tools for transition systems via a common intermediate language. We demonstrate how symbolic analysis can be an effective methodology for combining deduction and exploration.

For the entire collection see [Zbl 0944.00069].

MSC:

68Q60 Specification and verification (program logics, model checking, etc.)
68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)
68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)

Software:
PVS; Cadence SMV; HOL