Merz, Stephan

Model checking: A tutorial overview. (English) Zbl 0986.68063


Summary: We survey principles of model checking techniques for the automatic analysis of reactive systems. The use of model checking is exemplified by an analysis of the Needham-Schroeder public key protocol. We then formally define transition systems, temporal logic, $\omega$-automata, and their relationship. Basic model checking algorithms for linear- and branching-time temporal logics are defined, followed by an introduction to symbolic model checking and partial-order reduction techniques. The paper ends with a list of references to some more advanced topics.

For the entire collection see [Zbl 0974.00044].

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.)
- 94A62 Authentication, digital signatures and secret sharing
- 68Q45 Formal languages and automata
- 03D05 Automata and formal grammars in connection with logical questions
- 03B44 Temporal logic

Software:

Uppaal; HyTech