Symbolic Model Checking of Real-Time Systems
Using Difference Decision Diagrams

Jesper B. Møller
April 2002

Abstract

This dissertation describes:

- A uniform notation for modeling real-time systems called timed guarded commands where discrete state changes and progression of time are expressed as conditional nondeterministic value assignments.

- A symbolic technique for verification of real-time systems where sets of states are represented as formulae in a simple first-order logic over difference inequalities of the form x-y <= d, and where all basic verification operations are performed as operations within this logic; the progression of time, for example, is expressed as an existential quantification.

- A data structure called difference decision diagrams for representing formulae over difference inequalities as directed acyclic graphs with associated algorithms for combining formulae with Boolean operators, eliminating quantifiers, and determining satisfiability.

The dissertation establishes that timed guarded commands using difference decision diagrams are feasible and useful for symbolic model checking of real-time systems.