Verification of State/Event Systems with Acyclic Dependencies by Quotienting

Nicky O. Bodentien   Jacob Vestergaard   Jakob Friis
Kåre J. Kristoffersen   Kim G. Larsen

September 6, 1999

Abstract

A rather new approach towards compositional verification of concurrent systems is the quotient technique, where components are gradually removed from the concurrent system while transforming the specification accordingly. When the intermediate specifications can be kept small, the state explosion problem is avoided and there are already promising experimental results for systems with an interleaving semantics, including real-time systems. This paper extends the quotienting approach to deal with a synchronous framework in the shape of state/event systems with acyclic dependencies. A state/event system is a concurrent system with a set of interdependent components operating synchronously according to stimuli provided by an environment. We introduce Left Restricting state/event systems as a key notion for state/event systems with acyclic dependencies. Two families of modal logics, $\mathcal{L}$ and $\mathcal{M}$, specifically designed for expressing reachability properties of dependency closed and not dependency closed subsystems are introduced. Two quotient constructions for moving components from dependency closed and not dependency closed subsystems into the specification are presented and their correctness are justified in a formal proof. Furthermore, heuristics for minimizing formulae are proposed and the techniques are demonstrated on a Duplo train example.