UNIVERSITÄT AUGSBURG

Interactive Verification of Statecharts

Andreas Thums, Michael Balser

Report 2002-11 Juni 2002

INSTITUT FÜR INFORMATIK
D-86135 AUGSBURG

Interactive Verification of Statecharts

Andreas Thums and Michael Balser
Lehrstuhl Softwaretechnik,
Universität Augsburg, 86135 Augsburg, Germany
{thums,balser}@informatik.uni-augsburg.de

Abstract

This paper presents an approach to the integration of statecharts, temporal logic and algebraic specification within an interactive verification environment. Currently some integrated formalisms exist [13, 7], but there is no proof support for theses approaches. Also model checkers are able to prove temporal properties of statecharts [3, 10], but they can only be used to verify properties based on a small, finite data domain.

Our goal is to provide a uniform, interactive proof support for verifying temporal properties of statecharts with algebraic data types and functions over infinite data domains. As an implementation platform the KIV system [2] is used. The semantics of statecharts is based on [6], which formalizes the STATEMATE semantics of statecharts [12].

1 Introduction

We present an approach which aims to support the interactive verification of (safety) properties for concurrent, reactive systems. For this, we use (i) statecharts to describe the operational system behavior, (ii) temporal logic to express properties of the complete execution trace, and (iii) algebraic specifications to formalize complex and possibly infinite data domains. Furthermore (iv) sequential programs are used as action language within stateqcharts.

We tightly integrate the different formalisms on the level of the semantics, interpreting statecharts as temporal formulas. Also, we provide a uniform proof method based on symbolic execution and induction. Symbolic execution is an intuitive proof method widely used for the interactive verification of sequential programs. We adapt this technique to the verification of temporal logic and statecharts.

In this paper, we focus on statecharts, explaining how they can be interpreted as temporal formulas and how to symbolically execute statechart formulas. Details on executing temporal formulas can be found in [1]. Sequential programs are executed using Dynamic Logic (DL) [8]. Execution