Symbolic Execution for the Derivation of Meaningful Properties of Hybrid Systems [1]

Angelo E. M. Ciarlini
The Laboratory of Formal Methods, Departamento de Informática
Pontifícia Universidade Católica do R.J.
Rua Marquês de S.Vicente 225, 22.453-900 - Rio de Janeiro, Brazil
angelo@inf.puc-rio.br

Thom Frühwirth
Computer Science Institute
University of Munich
Oettingenstr. 67, D-80538 München, Germany
fruehwir@informatik.uni-muenchen.de

Abstract

Several authors have recently suggested the use of constraint logic programming (CLP) for the verification of hybrid systems. The results of our research offer evidence that CLP can also be used for the derivation of essential properties of software specified by hybrid systems. The derived properties can be used to find meaningful test cases. In our approach, hybrid automata are automatically translated into a CLP program. The user can then study the behaviour of his system by specifying conditions under which the execution should be performed. The conditions are specified declaratively in a fragment of first order temporal logic relating variables' values at different times. Such a specification is translated automatically into conjunctions and disjunctions of constraints, which are taken into account during the symbolic execution of the CLP program. As a result, all possible paths that satisfy the conditions given initially are obtained, together with the corresponding necessary and sufficient constraints. Such constraints are translated and informed to the user who can then create reliable test plans by extracting good input values for testing the final code of his system. In order to avoid non-termination problems we use a depth-first iterative deepening search.

Our ideas have been used to implement the DExVal tool (Derivation of Meaningful Experiments for Validation). We have tried to incorporate the following features: independence between the specification of the system and the testing task; support for continuous variables; expressiveness of the query language; projection of the remaining constraints on the values of specific variables at specific times; and support for linear and non-linear expressions.

[1] This work is partially supported by the CNPq/BMBF Brazilian-German Programme on Scientific and Technological Cooperation