Parameter Synthesis with IC3

Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta

Fondazione Bruno Kessler
Trento, Italy
{cimatti,griggio,mover,tonettas}@fbk.eu

Abstract

Parametric systems arise in many application domains, from real-time systems to software to cyber-physical systems. Parameters are fundamental to model unknown quantities at design time and allow a designer to explore different instantiation of the system (i.e. every parameter valuation induces a different system), during the early development phases.

A key challenge is to automatically synthesize all the parameter valuations for which the system satisfies some properties. In this talk we focus on the parameter synthesis problem for infinite-state transition systems and invariant properties. We describe the synthesis algorithm ParamIC3 [1], which is based on IC3, one of the major recent breakthroughs in SAT-based model checking, and lately extended to the SMT case.

The algorithm follows a general approach that first builds the set of "bad" parameter valuations and then obtain the set of "good" valuations by complement. The approach enumerates the counterexamples that violate the property, extracting from each counterexample a region of bad parameter valuations, existentially quantifying the state variables.

ParamIC3 follows the same principles, but it overcomes some limitations of the previous approach by exploiting the IC3 features. First, IC3 may find a set of counterexamples $s_o, \ldots, s_k$, where each state in s_i is guaranteed to reach some of the bad states in s_k in $k - i$ steps; this is exploited to apply the expensive quantifier elimination on shortest, and thus more amenable, counterexamples. Second, the internal structure of IC3 allows our extension to be integrated in a fully incremental fashion, never restarting the search from scratch to find a new counterexample.

While various approaches already solve the parameter synthesis problem for several kind of systems, like infinite-state transition systems, timed and hybrid automata, the advantages ParamIC3 are that: it synthesizes an optimal region of parameters, it avoids computing the whole set of the reachable states, it is incremental and applies quantifier elimination only to small formulas.

We present the results of an experimental evaluation performed on benchmarks from the timed and hybrid systems domain. We compared the approach with similar SMT-based techniques and with techniques based on the computation of the reachable states. The results show the potential of our approach.

1998 ACM Subject Classification D.2.4 Software/Program Verification

Keywords and phrases parameter synthesis, infinite-state transition systems, satisfiability modulo theories, IC3

Digital Object Identifier 10.4230/OASIcs.SynCoP.2015.106

Category Informal Presentation

2nd International Workshop on Synthesis of Complex Parameters (SynCoP'15).
Editors: Étienne André and Goran Frehse; pp. 106–107

OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

References

1 Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Parameter synthesis with IC3. In *Formal Methods in Computer-Aided Design, FMCAD 2013, Portland, OR, USA, October 20-23, 2013*, pages 165–168, 2013.