Model Checking of Array-Based Systems: from Foundations to Implementation

Silvio Ghilardi

Dipartimento di Scienze dell'Informazione,
Università degli Studi di Milano (Italy)

Abstract. We are interested in automatically proving safety properties of infinite state systems, by combining the classical algebraic approach of [4] with deductive techniques exploiting, off-the-shelf, SMT solvers. After briefly recalling the main contributions in [4] leading to the use of backward reachability analysis to prove safety properties and overviewing the long line of works stemming from that seminal paper (such as [9, 8, 5–7]), we present the notion of *array based systems* [10]. Such systems are declarative abstractions of several classes of parametrised systems and (sequential) programs manipulating arrays. In the framework of array based systems, key notions from [4] (such as configuration, configuration ordering, and monotonic transition) can be adapted and reused in a uniform and simple way. A by-product of this approach is to make readily available deductive techniques (like the synthesis and the use of invariants [11]) in the context of the algorithmic verification technique of backward reachability. This is so because the framework retains the modularity and the flexibility typical of logic-based approaches to model-checking (in the same spirit of, e.g., [14]).

The key feature of array-based systems is that a suitable format for initial/unsafe states and transition formulae can be designed: this format is sufficiently expressive to cover interesting classes of infinite state systems and, at the same time, generates proof obligations (during backward analysis) that can be discharged by instantiation and SMT solving techniques for quantifier-free formulae.

To make the theoretical framework useful in practice, powerful heuristics are required to obtain adequate performances: these heuristics concern optimization of the computation of the pre-image [13], (static and dynamic) filtration of the instantiations that current SMT solvers cannot yet handle efficiently, as well as forward/backward simplification routines [12].

In the last part of the talk, we report our experimental experience with a prototype tool called MCMT [1], currently under development: we discuss its architecture (especially the interplay between the generation of proof obligations, the computation of pre-images, and the various heuristics) and its integration with the SMT solver YICES [3]; finally we compare MCMT with some state-of-the-art model checkers based on dedicated techniques like PFS [2].

This is joint work with Silvio Ranise (Università di Verona).

References

1. MCMT. http://homes.dsi.unimi.it/∼ghilardi/mcmt.
2. PFS. http://www.it.uu.se/research/docs/fm/apv/tools/pfs.
3. YICES. http://yices.csl.sri.com.
4. P. A. Abdulla, K. Cerans, B. Jonsson, and Y.-K. Tsay. General decidability theorems for infinite-state systems. In *Proc. of LICS*, pages 313–321, 1996.
5. P. A. Abdulla, G. Delzanno, N. B. Henda, and A. Rezine. Regular model checking without transducers. In *TACAS*, volume 4424 of *LNCS*, pages 721–736, 2007.
6. P. A. Abdulla, G. Delzanno, and A. Rezine. Parameterized verification of infinite-state processes with global conditions. In *CAV*, volume 4590 of *LNCS*, pages 145–157, 2007.
7. P. A. Abdulla, N. B. Henda, G. Delzanno, and A. Rezine. Handling parameterized systems with non-atomic global conditions. In *Proc. of VMCAI*, volume 4905 of *LNCS*, pages 22–36, 2008.
8. G. Delzanno, J. Esparza, and A. Podelski. Constraint-based analysis of broadcast protocols. In *Proc. of CSL*, volume 1683 of *LNCS*, pages 50–66, 1999.
9. J. Esparza, A. Finkel, and R. Mayr. On the verification of broadcast protocols. In *Proc. of LICS*, pages 352–359. IEEE Computer Society, 1999.
10. S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Towards SMT Model-Checking of Array-based Systems. In *Proc. of IJCAR*, LNCS, 2008. Full version available as a Technical Report at http://homes.dsi.unimi.it/∼ghilardi/allegati/GhiNiRaZu-RI318-08.pdf.
11. S. Ghilardi and S. Ranise. Goal-Directed Invariant Synthesis in Model Checking Modulo Thoeries. In *Proc. of TABLEAUX 09*, LNCS, 2009. Full version available as a Technical Report at http://homes.dsi.unimi.it/∼ghilardi/allegati/GhRa-RI325-09.pdf.
12. S. Ghilardi and S. Ranise. Model Checking Modulo Theories at work: the integration of Yices with MCMT. In *Proc. of AFM 09*, 2009. Available from MCMT web page.
13. S. Ghilardi, S. Ranise, and T. Valsecchi. Light-Weight SMT-based Model-Checking. In *Proc. of AVOCS 07-08*, ENTCS, 2008. Available from MCMT web page.
14. T. Rybina and A. Voronkov. A logical reconstruction of reachability. In *Revised Papers of the 5th Int. A. Ershov Mem. Conf. on Perspectives of Systems Informatics (PSI 2003)*, volume 2890 of *LNCS*, pages 222–237, 2003.