Instantiation-Based Automated Reasoning From Theory to Practice

Konstantin Korovin*

University of Manchester, UK
korovin@cs.man.ac.uk

Instantiation-based automated reasoning aims at combining the efficiency of propositional SAT and SMT technologies with the expressiveness of first-order logic. Propositional SAT and SMT solvers are probably the most successful reasoners applied to real-world problems, due to extremely efficient propositional methods and optimized implementations. However, the expressiveness of first-order logic is essential in many applications ranging from formal verification of software and hardware to knowledge representation and querying. Therefore, there is a growing demand to integrate efficient propositional and more generally ground reasoning modulo theories into first-order reasoning.

The basic idea behind instantiation-based reasoning is to interleave smart generation of instances of first-order formulae with propositional type reasoning. Instantiation-based methods can be divided into two major categories: (i) fine-grained interleaving of instantiation with efficient propositional inference rules, and (ii) modular combination of instantiation and propositional reasoning. Examples from the first category include the disconnection calculus (DCTP) [8, 24], which combines instance generation with an efficient tableau data structure, and the model evolution calculus (ME) [6], which interleaves instance generation with DPLL style reasoning. Both DCTP and ME methods have advanced implementations DCTP [33] and Darwin [3], respectively.

Our approach to instantiation-based reasoning [15, 21] falls into the second category, where propositional reasoning is integrated in a modular fashion and was inspired by work on hyper-linking and its extensions (see [23, 31, 18]). The main advantage of the modular combination is that it allows one to use off-the-shelf SAT/SMT solvers in the context of first-order reasoning. One of our main goals was to develop a flexible theoretical framework, called Inst-Gen, for modular combination of instantiation with propositional reasoning and more generally with ground reasoning modulo theories. This framework provides methods for proving completeness of instantiation calculi, powerful redundancy elimination criteria and flexible saturation strategies. All these ingredients are crucial for developing reasoning systems which can be used in practical applications. We also show that most of the powerful machinery developed in the resolution-based framework can be suitably adapted for the Inst-Gen method.

Based on these theoretical results we have developed and implemented an automated reasoning system, called iProver [22]. iProver features state-of-the-art implementation techniques such as unification and simplification indexes;

* Supported by The Royal Society

semantically-guided inferences based on propositional models; redundancy elimination based on dismatching constraints, blocking of non-proper instantiations and global subsumption. For propositional reasoning iProver uses an optimised SAT solver MiniSat [12]. For efficient equational and theory reasoning, we are currently integrating (joint work with C. Sticksel) state-of-the-art SMT solvers CVC3 [1] and Z3 [11] into iProver.

One of the major success stories of instantiation-based methods is in reasoning with the effectively propositional (EPR) fragment of first-order logic, also called the Bernays-Schönfinkel class. All known instantiation-based methods are decision procedures for the EPR fragment. Recently it was shown that the EPR fragment has a number of applications in areas such as bounded model checking, planning, logic programming and knowledge representation [28, 30, 19, 13]. As witnessed by the CASC competition [34] instantiation-based methods considerably outperform other methods in the EPR division. The importance of the EPR fragment triggered the development of a number of dedicated methods [10, 29, 5], but they have not yet been extensively evaluated and compared with general-purpose instantiation-based methods.

There are many challenges remaining in the area of instantiation-based reasoning. Let me just mention some of them. The first challenge is the integration of theory reasoning and, in particular, reasoning with real and integer arithmetic. There are results on the integration of equational reasoning [25, 16, 7] and some initial results on the integration of theory reasoning [17, 4], but these should be considerably extended to cover more problems coming from applications.

The second challenge is combining instantiation-based methods with other reasoning methods such as resolution. Refinements of resolution are decision procedures for many important fragments of first-order logic including the guarded fragment and fragments corresponding to translations of various modal and description logics (see e.g., [14, 32, 20]). It is a natural progression to combine instantiation-based methods with resolution in order to obtain efficient reasoning methods for combinations of the EPR fragment and fragments decidable by resolution (note that in general, the resulting fragments can be undecidable).

The third challenge is in applying instantiation-based methods in reasoning with large theories. There is growing interest using first-order reasoning systems in problems involving large theories and, in particular, large knowledge-bases [26]. Initial experiments show that the performance of instantiation-based methods on such problems is promising but more research is needed in this area.

The fourth challenge is in applying instantiation-based methods to model finding. Instantiation-based methods are designed mainly to prove validity of first-order formulae. In many applications the dual problem of proving satisfiability of first-order formulae, or model finding, is equally important. Recently it was shown that the problem of finite model finding for first-order logic can be reduced to the satisfiability problem in the EPR fragment [2, 27]. Therefore, instantiation-based methods can be naturally used for finite model finding and such capabilities are incorporated into Darwin and iProver. Already finding models with small domain sizes is a challenging problem due to enormous search

spaces. Symmetry reduction is one of the main methods used to reduce redundant computations in model finders (see e.g., [9, 2]). More research is required to develop powerful symmetry reductions in the context of instantiation-based methods. Finally, little is known about model finding in the case of very large models or infinite models.

To conclude, instantiation-based reasoning is a rapidly developing area with high potential and exciting research challenges.

References

1. C. Barrett and C. Tinelli. CVC3. In W. Damm and H. Hermanns, editors, *CAV'07*, volume 4590 of *LNCS*, pages 298–302. Springer-Verlag, July 2007.
2. P. Baumgartner, A. Fuchs, , H. de Nivelle, and C. Tinelli. Computing finite models by reduction to function-free clause logic. In *Third Workshop on Disproving - Non-Theorems, Non-Validity, Non-Provability (DISPROVING'06)*, July 2006.
3. P. Baumgartner, A. Fuchs, and C. Tinelli. Implementing the model evolution calculus. *International Journal on Artificial Intelligence Tools*, 15(1):21–52, 2006.
4. P. Baumgartner, A. Fuchs, and C. Tinelli. ME(LIA) – Model evolution with linear integer arithmetic constraints. In *the 15th International Conference LPAR'08*, volume 5330 of *LNCS*, pages 258–273. Springer, 2008.
5. P. Baumgartner and R. A. Schmidt. Blocking and other enhancements for bottom-up model generation methods. In *Third International Joint Conference on Automated Reasoning (IJCAR'06)*, volume 4130 of *LNCS*, pages 125–139. Springer, 2006.
6. P. Baumgartner and C. Tinelli. The model evolution calculus. In *Proc. CADE-19*, number 2741 in LNCS, pages 350–364. Springer, 2003.
7. P. Baumgartner and C. Tinelli. The model evolution calculus with equality. In *the 20th International Conference CADE'05*, volume 3632 of *LNCS*, pages 392–408. Springer, 2005.
8. J.-P. Billon. The disconnection method: a confluent integration of unification in the analytic framework. In *TABLEAUX*, volume 1071 of *LNAI*, pages 110–126, 1996.
9. K. Claessen and N. Sörensson. New techniques that improve MACE-style model finding. In *Proc. of Workshop on Model Computation (MODEL)*, 2003.
10. L. M. de Moura and N. Bjørner. Deciding effectively propositional logic using DPLL and substitution sets. In *the 4th International Joint Conference on Automated Reasoning*, volume 5195 of *LNCS*, pages 410–425. Springer, 2008.
11. L. M. de Moura and N. Bjørner. Z3: an efficient SMT solver. In *TACAS'08*, volume 4963 of *LNCS*, pages 337–340. Springer, 2008.
12. N. Eén and N. Sörensson. An extensible SAT-solver. In *Proc. of the 6th International Conference SAT'03*, volume 2919 of *LNCS*, pages 502–518. Springer, 2004.
13. T. Eiter, W. Faber, and P. Traxler. Testing strong equivalence of datalog programs - implementation and examples. In *the 8th International Conference LPNMR'05*, volume 3662 of *LNCS*, pages 437–441, 2005.
14. H. Ganzinger and H. de Nivelle. A superposition decision procedure for the guarded fragment with equality. In *Poc. of LICS'99*, pages 295–304, 1999.
15. H. Ganzinger and K. Korovin. New directions in instantiation-based theorem proving. In *Proc. 18th IEEE Symposium on LICS*, pages 55–64. IEEE, 2003.

16. H. Ganzinger and K. Korovin. Integrating equational reasoning into instantiation-based theorem proving. In *CSL'04*, volume 3210 of *LNCS*, pages 71–84, 2004.
17. H Ganzinger and K. Korovin. Theory Instantiation. In *the 13th International Conference LPAR'06*, volume 4246 of *LNCS*, pages 497–511. Springer, 2006.
18. J.N. Hooker, G. Rago, V. Chandru, and A. Shrivastava. Partial instantiation methods for inference in first order logic. *J. Autom. Reasoning*, 28:371–396, 2002.
19. U. Hustadt, B. Motik, and U. Sattler. Reducing SHIQ-description logic to disjunctive datalog programs. In *the Ninth International Conference on Principles of Knowledge Representation and Reasoning*, pages 152–162. AAAI Press, 2004.
20. Y. Kazakov and B. Motik. A resolution-based decision procedure for SHOIQ. *J. Autom. Reasoning*, 40(2-3):89–116, 2008.
21. K. Korovin. An invitation to instantiation-based reasoning: a modular approach. In A. Podelski, A. Voronkov, and R. Wilhelm, editors, *Volume in memoriam of Harald Ganzinger*. Springer, 2006. Invited paper, to appear.
22. K. Korovin. iProver - an instantiation-based theorem prover for first-order logic (system description). In *the 4th International Joint Conference on Automated Reasoning*, volume 5195 of *LNCS*, pages 292–298. Springer, 2008.
23. S.-J. Lee and D. Plaisted. Eliminating duplication with the Hyper-linking strategy. *J. Autom. Reasoning*, 9:25–42, 1992.
24. R. Letz and G. Stenz. Proof and model generation with disconnection tableaux. In *Proc. LPAR 2001*, volume 2250 of *LNAI*, pages 142–156, 2001.
25. R. Letz and G. Stenz. Integration of equality reasoning into the disconnection calculus. In *International Conference TABLEAUX 2002*, volume 2381 of *LNCS*, pages 176–190, 2002.
26. A. Pease, G. Sutcliffe, N. Siegel, and S. Trac. The annual SUMO reasoning prizes at CASC. In *the First International Workshop on Practical Aspects of Automated Reasoning*, volume 373 of *CEUR Workshop Proceedings*, 2008.
27. J.A.N. Pérez. *Encoding and Solving Problems in Effectively Propositional Logic*. PhD thesis, University of Manchester, 2007.
28. J.A.N. Pérez and A. Voronkov. Encodings of bounded LTL model checking in effectively propositional logic. In *the 21st International Conference on Automated Deduction, (CADE'07)*, volume 4603 of *LNCS*, pages 346–361. Springer, 2007.
29. J.A.N. Pérez and A. Voronkov. Proof systems for effectively propositional logic. In *the 4th International Joint Conference on Automated Reasoning*, volume 5195 of *LNCS*, pages 426–440. Springer, 2008.
30. J.A.N. Pérez and A. Voronkov. Planning with effectively propositional logic. In A. Podelski, A. Voronkov, and R. Wilhelm, editors, *Volume in memoriam of Harald Ganzinger*. Springer, to appear. Invited paper.
31. D. Plaisted and Y. Zhu. Ordered semantic hyper-linking. *J. Autom. Reasoning*, 25(3):167–217, 2000.
32. R. A. Schmidt and U. Hustadt. First-order resolution methods for modal logics. In A. Podelski, A. Voronkov, and R. Wilhelm, editors, *Volume in memoriam of Harald Ganzinger*, Lecture Notes in Computer Science. Springer, 2006. Invited overview paper, to appear.
33. G. Stenz. DCTP 1.2 - system abstract. In *International Conference TABLEAUX 2002*, volume 2381 of *LNCS*, pages 335–340, 2002.
34. G. Sutcliffe. The 4th IJCAR automated theorem proving system competition - CASC-J4. *AI Communications*, 22(1):59–72, 2009.