STP2

Trevor Hansen, Peter Schachte and Harald Søndergaard
The University of Melbourne

Vijay Ganesh
Massachusetts Institute of Technology

June 2012

STP [Gan07] is an efficient open source solver for `QF_BV` and arrays without extensionality. STP recursively simplifies bit-vector constraints, solves linear bit-vector equations, and then eagerly encodes them to CNF for solving. Array axioms are added as needed, during an abstraction-refinement phase.

The version of STP submitted to STMCOMP 2012 is based on revision 1659 from STP's publicly available source code repository[1].

For the parallel track STP2 converts `QF_BV` problems into CNF then loads that CNF into ppFolio, a simple portfolio SAT Solver. ppFolio in turn calls: Cryptominisat, LingeLing, Clasp, March_hi and TNM.

Contributions to STP

STP 1 was developed by Vijay Ganesh under the supervision of Professor David Dill. STP 2 was developed by Trevor Hansen under the supervision of Peter Schachte and Harald Søndergaard. STP handles arbitrary precision integers using Steffen Beyers library. STP encodes into CNF via the and-inverter graph package ABC of Alan Mishchenko [BM10]. We found many defects using Robert Brummayer and Armin Bieres fuzzing and delta debugging tools [BB09].

Thanks for recent bug reports and patches to: Xu Zhongxing (help with the C-API), Edward Schwartz (nice test cases), Spencer Whitman (build script), Tom Bergan (help with the C-API), Stephan Falke (build script), Khoo Yit Phang (important defects), Jianjun Huang (Bug report), and Jingyue Wu (infinite loop).

References

[BB09] Robert Brummayer and Armin Biere. Fuzzing and delta-debugging SMT solvers. In *SMT '09: Proceedings of the 7th International Workshop on Satisfiability Modulo Theories*, pages 1–5, New York, NY, USA, 2009. ACM.

[BM10] Robert Brayton and Alan Mishchenko. ABC: An academic industrial-strength verification tool. In *Computer Aided Verification*, 2010.

[Gan07] Vijay Ganesh. *Decision Procedures for Bit-Vectors, Arrays and Integers*. PhD thesis, Computer Science Department, Standford University, 2007.

[SNC09] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending SAT solvers to cryptographic problems. In *SAT '09: Proceedings of the 12th International Conference on Theory and Applications of Satisfiability Testing*, pages 244–257, Berlin, Heidelberg, 2009. Springer-Verlag.

[1] To obtain the C++ source code follow the link from STP's website: `http://sites.google.com/site/stpfastprover/`