Tutorial on World-Level Model Checking

Armin Biere
Johannes Kepler University Linz, Altenbergerstr. 69, 4040 Linz, Austria
armin.biere@jku.at

***Abstract*—In SMT bit-vectors and thus word-level reasoning is common and widely used in industry. However, it took until 2019 that the hardware model checking competition started to use word-level benchmarks. Reasoning on the word-level opens up many possibilities for simplification and more powerful reasoning. In SMT we do see advantages due to operating on the word-level, even though, ultimately, bit-blasting and thus transforming the word-level problem into SAT is still the dominant and most important technique. For word-level model checking the situation is different. As the hardware model checking competition in 2019 has shown bit-level solvers are far superior (after bit-blasting the model through an SMT solver though). On the other hand word-level model checking shines for problems with memory modeled with arrays. In this tutorial we revisit the problem of word level model checking, also from a theoretical perspective, give an overview on classical and more recent approaches for word-level model checking and then discuss challenges and future work. The tutorial covered material from the following papers.**

References

[1] Z. S. Andraus, M. H. Liffiton, and K. A. Sakallah, "Refinement strategies for verification methods based on datapath abstraction," in *Proc. ASP-DAC'06*. IEEE, 2006, pp. 19–24.
[2] ——, "Reveal: A formal verification tool for Verilog designs," in *Proc. LPAR'08*, ser. LNCS, vol. 5330. Springer, 2008, pp. 343–352.
[3] C. Barrett, P. Fontaine, and C. Tinelli, "The Satisfiability Modulo Theories Library (SMT-LIB)," `www.SMT-LIB.org`, 2016.
[4] A. Biere, "The AIGER And-Inverter Graph (AIG) format version 20071012," FMV Reports Series, JKU Linz, Tech. Rep., 2007.
[5] A. Biere, K. Heljanko, and S. Wieringa, "AIGER 1.9 and beyond," FMV Reports Series, JKU Linz, Tech. Rep., 2011.
[6] A. Biere and M. Preiner, "Hardware model checking competition 2019," http://fmv.jku.at/hwmcc19.
[7] A. Biere, T. van Dijk, and K. Heljanko, "Hardware model checking competition 2017," in *Proc. FMCAD'17*. IEEE, 2017, p. 9.
[8] P. Bjesse, "A practical approach to word level model checking of industrial netlists," in *Proc. CAV'08*, ser. LNCS, vol. 5123. Springer, 2008, pp. 446–458.
[9] ——, "Word-level sequential memory abstraction for model checking," in *Proc. FMCAD'08*. IEEE, 2008, pp. 1–9.
[10] ——, "Word level bitwidth reduction for unbounded hardware model checking," *Formal Methods Syst. Des.*, vol. 35, no. 1, pp. 56–72, 2009.
[11] R. Brummayer, A. Biere, and F. Lonsing, "BTOR: Bit-precise modelling of word-level problems for model checking," in *Proc. SMT'08*. ACM, 2008, pp. 33–38.
[12] G. Cabodi, C. Loiacono, M. Palena, P. Pasini, D. Patti, S. Quer, D. Vendraminetto, A. Biere, and K. Heljanko, "Hardware model checking competition 2014: An analysis and comparison of solvers and benchmarks," *JSAT*, vol. 9, pp. 135–172, 2014 (published 2016).
[13] R. Cavada, A. Cimatti, M. Dorigatti, A. Griggio, A. Mariotti, A. Micheli, S. Mover, M. Roveri, and S. Tonetta, "The nuXmv symbolic model checker," in *Proc. CAV'14*, ser. LNCS, vol. 8559. Springer, 2014, pp. 334–342.
[14] L. De Moura, S. Owre, and N. Shankar, "The SAL language manual," *Computer Science Laboratory, SRI Intl., Tech. Rep. CSL-01-01*, 2003.
[15] S. M. German, "A theory of abstraction for arrays," in *Proc. FMCAD'11*. FMCAD Inc., 2011, pp. 176–185.
[16] A. Goel and K. A. Sakallah, "Empirical evaluation of IC3-based model checking techniques on verilog RTL designs," in *Proc. DATE'19*. IEEE, 2019, pp. 618–621.
[17] ——, "Model checking of Verilog RTL using IC3 with syntax-guided abstraction," in *Proc. NFM'19*, ser. LNCS, vol. 11460. Springer, 2019, pp. 166–185.
[18] ——, "AVR: abstractly verifying reachability," in *Proc. TACAS'20*, ser. LNCS, vol. 12078. Springer, 2020, pp. 413–422.
[19] Y. Ho, A. Mishchenko, and R. K. Brayton, "Property directed reachability with word-level abstraction," in *Proc. FMCAD'17*. IEEE, 2017, pp. 132–139.
[20] K. Hoder, N. Bjørner, and L. M. de Moura, "μZ- an efficient engine for fixed points with constraints," in *Proc. CAV'11*, ser. LNCS, vol. 6806. Springer, 2011, pp. 457–462.
[21] A. Irfan, A. Cimatti, A. Griggio, M. Roveri, and R. Sebastiani, "Verilog2SMV: A tool for word-level verification," in *Proc. DATE'16*. IEEE, 2016, pp. 1156–1159.
[22] H. Jain, D. Kroening, N. Sharygina, and E. M. Clarke, "Word-level predicate-abstraction and refinement techniques for verifying RTL Verilog," *IEEE TCAD*, vol. 27, no. 2, pp. 366–379, 2008.
[23] T. Jussila and A. Biere, "Compressing BMC encodings with QBF," *ENTCS*, vol. 174, no. 3, pp. 45–56, 2007.
[24] A. Kölbl, R. Jacoby, H. Jain, and C. Pixley, "Solver technology for system-level to RTL equivalence checking," in *Proc. DATE'09*. IEEE, 2009, pp. 196–201.
[25] G. Kovásznai, A. Fröhlich, and A. Biere, "Complexity of fixed-size bit-vector logics," *Theory Comp. Sys.*, vol. 59, no. 2, pp. 323–376, 2016.
[26] G. Kovásznai, H. Veith, A. Fröhlich, and A. Biere, "On the complexity of symbolic verification and decision problems in bit-vector logic," in *MFCS'14*, ser. LNCS, vol. 8635. Springer, 2014, pp. 481–492.
[27] D. Kroening, "Computing over-approximations with bounded model checking," *ENTCS*, vol. 144, no. 1, pp. 79–92, 2006.
[28] D. Kroening and S. A. Seshia, "Formal verification at higher levels of abstraction," in *Proc. ICCAD'07*. IEEE Comp. Soc., 2007, pp. 572–578.
[29] S. Lee and K. A. Sakallah, "Unbounded scalable verification based on approximate property-directed reachability and datapath abstraction," in *Proc. CAV'14*, ser. LNCS, vol. 8559. Springer, 2014, pp. 849–865.
[30] J. Long, S. Ray, B. Sterin, A. Mishchenko, and R. K. Brayton, "Enhancing ABC for stabilization verification of SystemVerilog/VHDL models," in *Proc. DIFTS'11*, ser. CEUR Work. Proc., vol. 832, 2011.
[31] P. Manolios, S. K. Srinivasan, and D. Vroon, "Automatic memory reductions for RTL model verification," in *Proc. ICCAD'06*. ACM, 2006, pp. 786–793.
[32] R. Mukherjee, P. Schrammel, D. Kroening, and T. Melham, "Unbounded safety verification for hardware using software analyzers," in *Proc. DATE'16*. IEEE, 2016, pp. 1152–1155.
[33] R. Mukherjee, M. Tautschnig, and D. Kroening, "v2c - A Verilog to C translator," in *Proc. TACAS'16*, ser. LNCS, vol. 9636. Springer, 2016, pp. 580–586.
[34] A. Niemetz, M. Preiner, C. Wolf, and A. Biere, "Btor2 , BtorMC and Boolector 3.0," in *Proc. CAV'18*, ser. LNCS, vol. 10981. Springer, 2018, pp. 587–595.
[35] M. Sagiv, "Harnessing SMT solvers for verifying low level programs," 2020, invited talk, *SMT'20*.
[36] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, 1997.
[37] T. Welp and A. Kuehlmann, "QF BV model checking with property directed reachability," in *Proc. DATE'13*, 2013, pp. 791–796.
[38] ——, "Property directed invariant refinement for program verification," in *Proc. DATE'14*. Europ. Design and Automation Ass., 2014, pp. 1–6.
[39] ——, "Property directed reachability for QF_BV with mixed type atomic reasoning units," in *Proc. ASP-DAC'14*. IEEE, 2014, pp. 738–743.
[40] C. Wolf, "Yosys," https://github.com/YosysHQ/yosys.

https://doi.org/10.34727/2020/isbn.978-3-85448-042-6_3