Wang, Wenxi; **Søndergaard, Harald**; **Stuckey, Peter J.**
Wombit: a portfolio bit-vector solver using word-level propagation. (English) Zbl 07100461
J. Autom. Reasoning 63, No. 3, 723-762 (2019).

Summary: We develop an idea originally proposed by Michel and Van Hentenryck of how to perform bit-vector constraint propagation on the word level. Most operations are propagated in constant time, assuming the bit-vector fits in a machine word. In contrast, bit-vector SMT solvers usually solve bit-vector problems by (ultimately) bit-blasting, that is, mapping the resulting operations to conjunctive normal form clauses, and using SAT technology to solve them. Bit-blasting generates intermediate variables which can be an advantage, as these can be searched on and learnt about. As each approach has advantages, it makes sense to try to combine them. In this paper, we describe an approach to bit-vector solving using word-level propagation with learning. We have designed alternative word-level propagators to Michel and Van Hentenryck's, and evaluated different variants of the approach. We have also experimented with different approaches to learning and back-jumping in the solver. Based on the insights gained, we have built a portfolio solver, Wombit, which essentially extends the STP bit-vector solver. Using machine learning techniques, the solver makes a judicious up-front decision about whether to use word-level propagation or fall back on bit-blasting.

MSC:

68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)

Keywords:

bit-vector solver; bit-blasting; constraint propagation; word-level reasoning; machine learning; portfolio solvers

Software:

BLAST; Boogie; C4.5; Chaff; CPAchecker; KLEE; LIBSVM; meSAT; MiniSat; MiniZinc; PMTK; Proteus; SCIP; STP; SUNNY; sunny-cp; Why3; Yices; z3

Full Text: DOI

References:

[1] Abío, I., Stuckey, P.J.: Conflict directed lazy decomposition. In: Milano, M. (ed.) Principles and Practice of Constraint Programming: Proceedings of the 18th International Conference, Lecture Notes in Computer Science, vol. 7514, pp. 70-85. Springer (2012)

[2] Achterberg, T., Berthold, T., Koch, T., Wolter, K.: Constraint integer programming: a new approach to integrate CP and MIP. In: Perron, L., Trick, M.A. (eds.) Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems, Lecture Notes in Computer Science, vol. 5015, pp. 6-20. Springer (2008) · Zbl 1142.68504

[3] Amadini, R., Gabbrielli, M., Mauro, J.: An empirical evaluation of portfolios approaches for solving CSPs. In: Gomes, C., Sellmann, M. (eds.) Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems: Proceedings of the 10th International Conference, Lecture Notes in Computer Science, pp. 316-324. Springer (2013) · Zbl 1382.68219

[4] Amadini, R.; Gabbrielli, M.; Mauro, J., SUNNY: a lazy portfolio approach for constraint solving, Theory Pract. Log. Program., 14, 509-524, (2014) · Zbl 1307.68077

[5] Amadini, R., Gabbrielli, M., Mauro, J.: A multicore tool for constraint solving. In: Proceedings of the 24th International Conference on Artificial Intelligence (IJCAI'15), pp. 232-238. AAAI Press (2015)

[6] Amadini, R., Gabbrielli, M., Mauro, J.: SUNNY-CP: a sequential CP portfolio solver. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing (SAC'15), pp. 1861-1867. ACM (2015)

[7] Amadini, R.; Gabbrielli, M.; Mauro, J., An extensive evaluation of portfolio approaches for constraint satisfaction problems, Int. J. Interact. Multimed. Artif. Intell., 3, 81-86, (2016) · Zbl 1335.90077

[8] Arbelaez, A., Hamadi, Y., Sebag, M.: Online heuristic selection in constraint programming. In: Proceedings of the International Symposium on Combinatorial Search (2009). https://hal.inria.fr/inria-00392752/. Accessed 12 Mar 2018

[9] Arbelaez, A.; Hamadi, Y.; Sebag, M.; Hamadi, Y. (ed.); etal., Continuous search in constraint programming, 219-243, (2011),

Berlin

[10] Avgerinos, T.; Cha, SK; Rebert, A.; Schwartz, EJ; Woo, M.; Brumley, D., Automatic exploit generation, Commun. ACM, 57, 74-84, (2014)

[11] Aziz, M.A., Wassal, A., Darwish, N.: A machine learning technique for hardness estimation of QFBV SMT problems. In: Fontaine, P., Goel, A. (eds.) Proceedings of the 10th International Workshop on Satisfiability Modulo Theories (SMT'12), EPiC Series in Computing, vol. 20, pp. 57-66. EasyChair (2013)

[12] Babić, D.: Exploiting Structure for Scalable Software Verification. PhD thesis, University of British Columbia, Vancouver, Canada (2008)

[13] Baray, F., Codognet, P., Diaz, D., Michel, H.: Code-based test generation for validation of functional processor descriptions. In: Garavel, H., Hatcliff, J. (eds.) Tools and Algorithms for the Construction and Analysis of Systems (TACAS'03), Lecture Notes in Computer Science, vol. 2619, pp. 569-584. Springer (2003) · Zbl 1031.68509

[14] Bardin, S., Herrmann, P., Perroud, F.: An alternative to SAT-based approaches for bit-vectors. In: Esparza, J., Majumdar, R. (eds.) Tools and Algorithms for the Construction and Analysis of Systems (TACAS'10), Lecture Notes in Computer Science, vol. 6015, pp. 84-98. Springer (2010) · Zbl 1284.68379

[15] Beyer, D.; Henzinger, TA; Jhala, R.; Majumdar, R., The software model checker blast: applications to software engineering, Int. J. Softw. Tools Technol. Transf., 9, 505-525, (2007)

[16] Beyer, D., Keremoglu, M.E.: CPAchecker: a tool for configurable software verification. In: Gopalakrishnan, G., Qadeer, S. (eds.) Computer Aided Verification: Proceedings of the 23rd International Conference (CAV'11), Lecture Notes in Computer Science, vol. 6806, pp. 184-190. Springer (2011)

[17] Bobot, F., Filliâtre, J.-C., Marché, C., Paskevich, A.: Why3: Shepherd your herd of provers. In: Boogie 2011: First International Workshop on Intermediate Verification Languages, pp. 53-64, Wrocław, Poland (2011)

[18] Brinkmann, R., Drechsler, R.: RTL-datapath verification using integer linear programming. In: Proceedings of the Asia and South Pacific Design Automation Conference and VLSI Design 2002, pp. 741-746. IEEE Computer Society (2002)

[19] Cadar, C., Dunbar, D., Engler, D.: KLEE: Unassisted and automatic generation of high-coverage tests for complex systems programs. In: Proceedings of the 8th USENIX Conference on Operating Systems Design and Implementation, pp. 209-224. USENIX Association (2008)

[20] Chang, C-C; Lin, C-J, LIBSVM: a library for support vector machines, ACM Trans. Intell. Syst. Technol., 2, 27:1-27:27, (2011)

[21] Chihani, Z., Bobot, F., Bardin, S.: CDCL-inspired word-level learning for bit-vector constraint solving (2017). HAL. arXiv:1706.09229 · Zbl 06756571

[22] Chihani, Z., Marre, B., Bobot, F., Bardin, S.: Sharpening constraint programming approaches for bit-vector theory. In: Salvagnin, D., Lombardi, M. (eds.) Integration of AI and OR Techniques in Constraint Programming: Proceedings of the 14th International Conference, Lecture Notes in Computer Science, vol. 10335, pp. 3-20. Springer (2017) · Zbl 06756571

[23] de Moura, L., Bjørner, N.: Z3: An efficient SMT solver. In: Ramakrishnan, C.R., Rehof, J. (eds.) Tools and Algorithms for the Construction and Analysis of Systems (TACAS'08), Lecture Notes in Computer Science, vol. 4963, pp. 337-340. Springer (2008)

[24] de Moura, L., Jovanović, D.: A model-constructing satisfiability calculus. In: Giacobazzi, R., Berdine, J., Mastroeni, I. (eds.) Verification Model Checking and Abstract Interpretation: Proceedings of the 14th International Conference, Lecture Notes in Computer Science, vol. 7737, pp. 1-12. Springer (2013) · Zbl 1426.68251

[25] Dutertre, B.: Yices 2.2. In: Biere, A., Bloem, R. (eds.) Computer-Aided Verification, Lecture Notes in Computer Science, vol. 8559, pp. 737-744. Springer (2014)

[26] Eén, N., Sörensson, N.: An extensible SAT-solver. In: Giunchiglia, E., Tacchella, A. (eds.) Theory and Applications of Satisfiability Testing (SAT'04), Lecture Notes in Computer Science, vol. 2919, pp. 333-336. Springer (2004)

[27] Erkinger, C.: Rotating workforce scheduling as satisfiability modulo theories. Master's thesis, Vienna University of Technology (2013)

[28] Fallah, F., Devadas, S., Keutzer, K.: Functional vector generation for HDL models using linear programming and 3-satisfiability. In: Proceedings of the 35th Annual Design Automation Conference (DAC'98), pp. 528-533. ACM (1998)

[29] Feydy, T., Schutt, A., Stuckey, P.J.: Global difference constraint propagation for finite domain solvers. In: Proceedings of the 10th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming (PPDP'08), pp. 226-235. ACM (2008)

[30] Fröhlich, A., Biere, A., Wintersteiger, C.M., Hamadi, Y.: Stochastic local search for satisfiability modulo theories. In: Proceedings of the 29th AAAI Conference on Artificial Intelligence, pp. 1136-1143. AAAI Press (2015)

[31] Ganesh, V., Dill, D.L.: A decision procedure for bit-vectors and arrays. In: Damm, W., Hermanns, H. (eds.) Computer Aided Verification (CAV'07), Lecture Notes in Computer Science, vol. 4590, pp. 519-531. Springer (2007) · Zbl 1135.68472

[32] Gent, I.P., Miguel, I., Moore, N.C.A.: Lazy explanations for constraint propagators. In: Carro, M., Pena, R. (eds.) Practical Aspects of Declarative Languages (PADL'10), Lecture Notes in Computer Science, vol. 5937, pp. 217-233. Springer (2010)

[33] Gotlieb, A., Leconte, M., Marre, B.: Constraint solving on modular integers. In: Proceedings of the Ninth International Workshop on Constraint Modelling and Reformulation (ModRef'10) (2010)

[34] Hadarean, L., Barrett, C., Jovanović, D., Tinelli, C., Bansal, K.: A tale of two solvers: eager and lazy approaches to bit-vectors. In: Biere, A., Bloem, R. (eds.) Computer Aided Verification (CAV'14), Lecture Notes in Computer Science, vol. 8559, pp. 680-695. Springer (2014)

[35] Hoos, H.: On the run-time behaviour of stochastic local search algorithms for SAT. In: Proceedings of the 16th National

Conference on Artificial Intelligence, pp. 661-666. AAAI Press (1999)

[36] Hoos, H., Stützle, T.: Stochastic Local Search: Foundations and Applications. Morgan Kaufmann, Burlington (2004) · Zbl 1126.68032

[37] Hurley, B., Kotthoff, L., Malitsky, Y., O'Sullivan, B.: Proteus: A hierarchical portfolio of solvers and transformations. In: Simonis, H. (ed.) Integration of AI and OR Techniques in Constraint Programming: Proceedings of the 11th International Conference (CPAIOR'14), Lecture Notes in Computer Science, vol. 8451, pp. 301-317. Springer (2014)

[38] Hutter, F., Xu, L., Hoos, H.H., Leyton-Brown, K.: Algorithm runtime prediction: The state of the art, 2012. CoRR, arXiv: 1211.0906 · Zbl 1334.68185

[39] Jovanović, D.; Moura, L., Cutting to the chase, J. Autom. Reason., 51, 79-108, (2013) · Zbl 1314.90053

[40] Kosko, B.: Neural Networks and Fuzzy Systems: A Dynamical Systems Approach to Machine Intelligence. Prentice-Hall, Upper Saddle River (1992) · Zbl 0755.94024

[41] Kotthoff, L., Algorithm selection for combinatorial search problems: a survey, AI Mag., 35, 48-60, (2014)

[42] Kovásznai, G.; Fröhlich, A.; Biere, A., Complexity of fixed-size bit-vector logics, Theory Comput. Syst., 59, 323-376, (2016) · Zbl 1357.68086

[43] Kroening, D., Strichman, O.: Decision Procedures: An Algorithmic Point of View. Springer, Berlin (2008) · Zbl 1149.68071

[44] Kunapareddy, S., Turaga, S.D., Sajjan, S.S.T.M.: Comparison between LPSAT and SMT for RTL verification. In: Proceedings of the 2015 International Conference on Circuit, Power and Computing Technologies, pp. 1-5. IEEE Computer Society (2015)

[45] Leino, K.R.M.: This is Boogie 2 (2008). Unpublished manuscript

[46] Limaye, R.S., Seshia, S.A.: Beaver: an SMT solver for quantifier-free bit-vector logic. Master's thesis, University of California, Berkeley (2010)

[47] Loreggia, A., Malitsky, Y., Samulowitz, H., Saraswat, V.A.: Deep learning for algorithm portfolios. In: Proceedings of the 30th AAAI Conference on Artificial Intelligence, pp. 1280-1286. AAAI Press (2016)

[48] Marriott, K., Stuckey, P.J.: Programming with Constraints: An Introduction. MIT Press, Cambridge (1998) · Zbl 0935.68098

[49] McCullagh, P., Nelder, J.A.: Generalized Linear Models, 2nd edn. Chapman \& Hall, Boca Raton (1989) · Zbl 0744.62098

[50] Michel, L.D., Van Hentenryck, P.: Constraint satisfaction over bit-vectors. In: Milano, M. (ed.) Constraint Programming: Proceedings of the 2012 Conference, Lecture Notes in Computer Science, vol. 7514, pp. 527-543. Springer (2012)

[51] Moskewicz, M.W., Madigan, C.F., Zhao, Y., Zhang, L., Malik, S.: Chaff: Engineering an efficient SAT solver. In: Proceedings of the 38th Annual Design Automation Conference, DAC'01, pp. 530-535, New York, NY, USA. ACM (2001)

[52] Murphy, K.P.: Machine Learning: A Probabilistic Perspective. MIT Press, Cambridge (2012) · Zbl 1295.68003

[53] Niemetz, A.; Preiner, M.; Biere, A., Boolector 2.0, J. Satisf. Boolean Model. Comput., 9, 53-58, (2015)

[54] Niemetz, A.; Preiner, M.; Biere, A., Propagation based local search for bit-precise reasoning, Form. Methods Syst. Des., 51, 608-636, (2017) · Zbl 1377.68134

[55] Niemetz, A., Preiner, M., Fröhlich, A., Biere, A.: Improving local search for bit-vector logics in SMT with path propagation. In: Proceedings of the 4th International Workshop on Design and Implementation of Formal Tools and Systems (DIFTS'15) (2015)

[56] Nieuwenhuis, R.; Oliveras, A.; Tinelli, C., Solving SAT and SAT modulo theories: from an abstract Davis-Putnam-Logemann-Loveland procedure to DPLL(T), J. ACM, 53, 937-977, (2006) · Zbl 1326.68164

[57] Ohrimenko, O.; Stuckey, PJ; Codish, M., Propagation via lazy clause generation, Constraints, 14, 357-391, (2009) · Zbl 1192.68654

[58] O'Mahony, E., Hebrard, E., Holland, A., Nugent, C., O'Sullivan, B.: Using case-based reasoning in an algorithm portfolio for constraint solving. In: Irish Conference on Artificial Intelligence and Cognitive Science, pp. 210-216 (2008)

[59] Quinlan, JR, Induction of decision trees, Mach. Learn., 1, 81-106, (1986)

[60] Quinlan, J.R.: C4.5: Programs for Machine Learning. Morgan Kaufmann, Burlington (1993)

[61] Schapire, RE; Denison, DD (ed.); etal., The boosting approach to machine learning: an overview, 149-171, (2003), Berlin

[62] Schulte, C.; Stuckey, PJ, Efficient constraint propagation engines, ACM Trans. Program. Lang. Syst., 31, 2:1-2:43, (2008)

[63] Serpette, B., Vuillemin, J., Hervé, J.-C.: BigNum: a portable and efficient package for arbitrary-precision arithmetic. Technical Report PRL 2, DEC Paris (1989)

[64] Smith-Miles, KA, Cross-disciplinary perspectives on meta-learning for algorithm selection, ACM Comput. Surv., 41, 6:1-6:25, (2009)

[65] Stojadinović, M.; Marić, F., meSAT: multiple encodings of CSP to SAT, Constraints, 19, 380-403, (2014) · Zbl 1316.90049

[66] Stojadinović, M., Nikolić, M., Marić, F.: Short portfolio training for CSP solving (2015). CoRR, arXiv: 1505.02070

[67] Stuckey, PJ; Becket, R.; Fischer, J., Philosophy of the MiniZinc challenge, Constraints, 15, 307-316, (2010) · Zbl 1208.68207

[68] Wang, W.: A bit-vector solver based on word-level propagation. Master's thesis, Computing and Information Systems, The University of Melbourne (2016). https://minerva-access.unimelb.edu.au/handle/11343/120613

[69] Wang, W., Søndergaard, H., Stuckey, PJ.: A bit-vector solver with word-level propagation. In: Quimper, C.-G. (ed.) Integration of AI and OR Techniques in Constraint Programming: Proceedings of the 13th International Conference, Lecture Notes in Computer Science, vol. 9676, pp. 374-391. Springer (2016) · Zbl 06598678

[70] Warren Jr., H.S.: Hacker's Delight. Addison Wesley, Reading (2003)

[71] Wille, R., Fey, G., Große, D., Eggersglüß, S., Drechsler, R.: SWORD: a SAT like prover using word level information. In: VLSI-SoC: Advanced Topics on Systems on a Chip: A Selection of Extended Versions of the Best Papers of the Fourteenth International Conference on Very Large Scale Integration of System on Chip, pp. 1-17. Springer (2009)

[72] Zeljić, A., Wintersteiger, C.M., Rümmer, P.: Deciding bit-vector formulas with mcSAT. In: Creignou, N., Le Berre, D. (eds.) Theory and Applications of Satisfiability Testing (SAT 2016): Proceedings of the 19th International Conference, Lecture Notes in Computer Science, vol. 9710, pp. 249-266. Springer (2016) · Zbl 06623516

[73] Zeng, Z., Kalla, P., Ciesielski, M.: LPSAT: a unified approach to RTL satisfiability. In: Design, Automation and Test in Europe (DATE'01), pp. 398-402. IEEE Press (2001)