# Tight coupling between bit-vector and integer domains can surpass bit-blasting SMT solvers*

Zakaria Chihani (first.last@cea.fr)

The fundamental unit on which all computers are built is the bit. Therefore, it is unsurprising that, in a world where safety of critical systems is paramount, a considerable effort [1, 2, 1, 3] has been deployed to deal with the theory of bit-vectors (BV) [4]. The components of this theory are fixed-size arrays (or vectors) of bits along with their basic operations, logical (such as conjunction and disjunction), arithmetic (such as addition, multiplication) and structural (such as concatenation and extraction). It is used with increasing popularity both in software and hardware safety.

The most applied technique for solving BV problems is bit-blasting [5], in which every bit in the BV is encoded as a propositional variable and BV operations are encoded as circuits. The original problem then becomes a regular satisfiability problem This allows to benefit from the expertise of the mature and yet ever evolving SAT community.

On the other hand, one can attribute to the bit-blasting technique two main inconveniences. First, it has difficulty scaling to larger problems (in terms of BV size). Second, it looses the inherent structure of the BV, thus disallowing detection of instances that can be simplified as well as the use of fast and low-level operations readily available that can improve efficiency.

This present submission aims at presenting a work in progress that pushes further an emerging exploration effort started by Bardin [6] through the use of a new domain for BV along with relying on reduced products with integer domains to cut the search space. That effort was also undertaken by Michel and Van Hentenryck [7] who introduced a finer implementation of the BV domain and bitwise propagations. While Bardin et al supplied their paper with preliminary experimentations showing the potential of their approach, Michel and Van Hentenryck only introduced theoretical results, which were applied to a certain extent[8] (with no reduced products, to a limited set of BV operations and on BV not larger than 64 bits) as an extension of MiniSat [9].

In this presentation, a more complete implementation in the COLIBRI solver [10] of the theory of QF_BV (quantifier free bit-vector) is presented. It handles all operations of SMT-LIB 2.5, is not restricted size-wise. It shows the full impact of relying on a much finer reduced product with unions of intervals (an extension of the usual notion of intervals) in addition to congruence domains and global difference constraints [11, 12]. Bardin already argued that keeping the bit-vector structure can reduce the gap of efficiency between CLP and SMT, the present results will show that on many hard examples, COLIBRI actually surpasses traditional solvers participating in the SMT competition.

*This work was partially funded by the French ANR (project SOPRANO, grant ANR-14-CE28-0020)

# References


[1] V. Ganesh and D. L. Dill, "A decision procedure for bit-vectors and arrays," in *Computer Aided Verification: 19th International Conference, CAV 2007, Berlin, Germany, July 3-7, 2007. Proceedings* (W. Damm and H. Hermanns, eds.), (Berlin, Heidelberg), pp. 519–531, Springer Berlin Heidelberg, 2007.

[2] R. Brummayer and A. Biere, "Boolector: An efficient smt solver for bit-vectors and arrays," in *Tools and Algorithms for the Construction and Analysis of Systems: 15th International Conference, TACAS 2009, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009, York, UK, March 22-29, 2009. Proceedings* (S. Kowalewski and A. Philippou, eds.), (Berlin, Heidelberg), pp. 174–177, Springer Berlin Heidelberg, 2009.

[3] S. Jha, R. Limaye, and S. A. Seshia, "Beaver: Engineering an efficient smt solver for bit-vector arithmetic," tech. rep., Berlin, Heidelberg, 2009.

[4] D. Kroening and O. Strichman, *Decision Procedures: An Algorithmic Point of View*. Springer Publishing Company, Incorporated, 1 ed., 2008.

[5] A. Biere, A. Cimatti, E. Clarke, and Y. Zhu, "Symbolic model checking without bdds," in *Tools and Algorithms for the Construction and Analysis of Systems: 5th International Conference, TACAS'99 Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS'99 Amsterdam, The Netherlands, March 22–28, 1999 Proceedings* (W. R. Cleaveland, ed.), (Berlin, Heidelberg), pp. 193–207, Springer Berlin Heidelberg, 1999.

[6] S. Bardin, P. Herrmann, and F. Perroud, "An alternative to sat-based approaches for bit-vectors," in *Tools and Algorithms for the Construction and Analysis of Systems: 16th International Conference, TACAS 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2010, Paphos, Cyprus, March 20-28, 2010. Proceedings* (J. Esparza and R. Majumdar, eds.), (Berlin, Heidelberg), pp. 84–98, Springer Berlin Heidelberg, 2010.

[7] L. Michel and P. Van Hentenryck, "Constraint satisfaction over bit-vectors," in *Principles and Practice of Constraint Programming* (M. Milano, ed.), vol. 7514 of *Lecture Notes in Computer Science*, pp. 527–543, Springer Berlin Heidelberg, 2012.

[8] W. Wang, H. Søndergaard, and P. J. Stuckey, "A bit-vector solver with word-level propagation," in *Integration of AI and OR Techniques in Constraint Programming: 13th International Conference, CPAIOR 2016, Banff, AB, Canada, May 29 - June 1, 2016, Proceedings* (C.-G. Quimper, ed.), (Cham), pp. 374–391, Springer International Publishing, 2016.

[9] N. Eén and N. Sörensson, "An extensible sat-solver," in *Theory and Applications of Satisfiability Testing: 6th International Conference, SAT 2003, Santa Margherita Ligure, Italy, May 5-8, 2003, Selected Revised Papers* (E. Giunchiglia and A. Tacchella, eds.), (Berlin, Heidelberg), pp. 502–518, Springer Berlin Heidelberg, 2004.

[10] B. Marre and B. Blanc, *Test Selection Strategies for Lustre Descriptions in GATeL*, vol. 111, pp. 93–111. Amsterdam, The Netherlands, The Netherlands: Elsevier Science Publishers B. V., Jan. 2005.

[11] R. Nieuwenhuis and A. Oliveras, "Dpll(t) with exhaustive theory propagation and its application to difference logic," in *Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005. Proceedings* (K. Etessami and S. K. Rajamani, eds.), (Berlin, Heidelberg), pp. 321–334, Springer Berlin Heidelberg, 2005.

[12] T. Feydy, A. Schutt, and P. J. Stuckey, "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, (New York, NY, USA), pp. 226–235, ACM, 2008.