Precise and Complete Propagation-Based Local Search for Satisfiability Modulo Theories

Aina Niemetz, Mathias Preiner, and Armin Biere

Institute for Formal Models and Verification (FMV)
Johannes Kepler University, Linz, Austria
http://fmv.jku.at/

CAV 2016
July 17 - 23, 2016
Toronto, Ontario, Canada

Completeness of local search algorithms

⟶ local search in general does not allow to determine unsatisfiability

⟶ Probabilistically Approximately Complete (PAC) [AAAI'99]

- will find a solution (if there is one)
- given unlimited run time

Bit-Vectors in Sat Modulo Theories (SMT)

- State-of-the-art: **Bit-Blasting**
  - eager reduction to propositional logic (SAT)
  - relies heavily on rewriting and other techniques to simplify the input formula

⟶ efficient in practice, may not scale if input size not reduced sufficiently

- Recently: **Stochastic Local Search (SLS)** for SMT [AAAI'15][DIFTS'15]
  - lifts SLS from SAT (bit-level) to the theory level (word-level)
  - without bit-blasting (orthogonal approach)

[AAAI'15] implemented in Z3

⟶ mostly simulates bit-level local search
⟶ focus on single bit flips

[DIFTS'15] implemented in Boolector

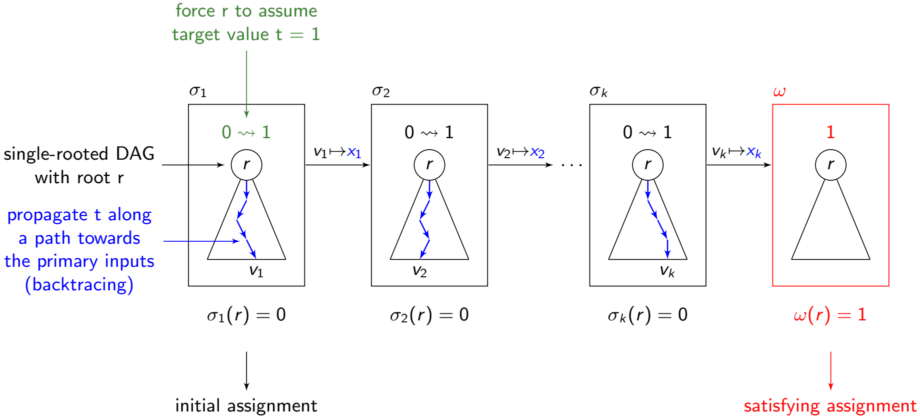
⟶ extends [AAAI'15] by introducing an additional propagation-based strategy
⟶ exploits word-level structure

⟶ both rely on brute force randomization and restarts to achieve **completeness**

This work

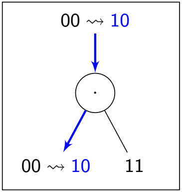
- **complete** propagation-based local search strategy
  - ⟶ relies on propagation of assignments only
  - ⟶ without SLS techniques
  - ⟶ no brute force randomization, no restarts to achieve completeness
- lifts the concept of **backtracing** from ATPG to the word-level
  - new notion: essential inputs
    - ⟶ lifts the notion of controlling inputs from the bit-level to the word-level
- provides a formal completeness **proof**

Basic Idea



- complete
- not satisfying

Down Propagation of Assignments via Backtracing



Word-Level

⟶ maximally reduce non-deterministic choices

⟶ without sacrificing completeness

- **Path** Selection
  - **Bit-Level**: controlling inputs
  - **Word-Level**: essential inputs

  (lifted)

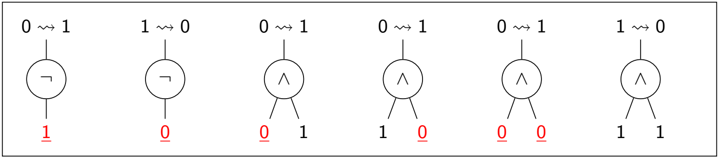
  ⟶ select essential input if any, else choose randomly

- **Value** Selection

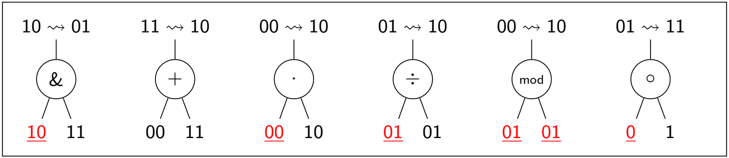
  ⟶ compute consistent or inverse value

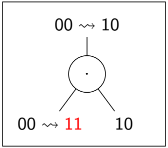
Definition An input to a node is **controlling** (**essential**), if the node can not assume a given target value as long as the value of the input does not change.

Example **Bit-Level** - controlling inputs



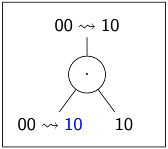
Example **Word-Level** - essential inputs





inverse value

Definition A value is **inverse** for an input to a node, if it produces the target value without changing the value of other inputs.



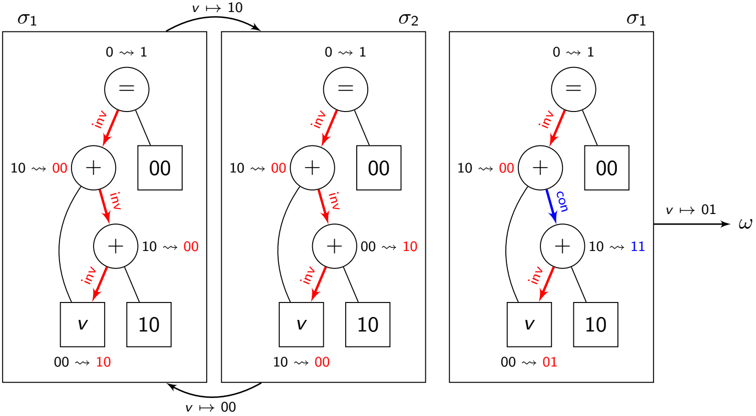
consistent value

Definition A value is **consistent**, if it allows the node to assume a target value after changing the value of other inputs if necessary.

- select inverse over consistent values with higher probability
- if no inverse value exists, select non-inverse consistent value

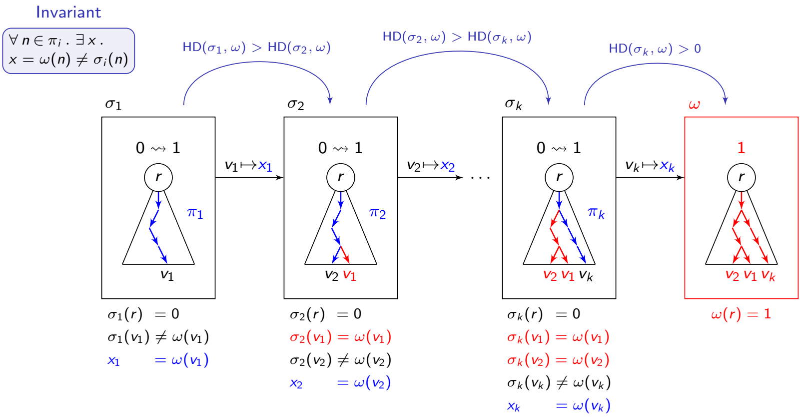
$\longrightarrow$ using **only** inverse values without further randomization is **incomplete**!

Example $v + v + 2_{[2]} = 0_{[2]}$



Goal: Show that our strategy is distance reducing, therefore complete (PAC).

$\longrightarrow$ show that there always exists a propagation path from the root to a primary input that reduces the Hamming Distance ($HD(\sigma, \omega)$) between σ and ω



Experimental Evaluation

Benchmark Set: **16436** total

all SMT-LIBv2 compliant QF_BV benchmarks in SMT-LIB with status sat and unknown **except** those

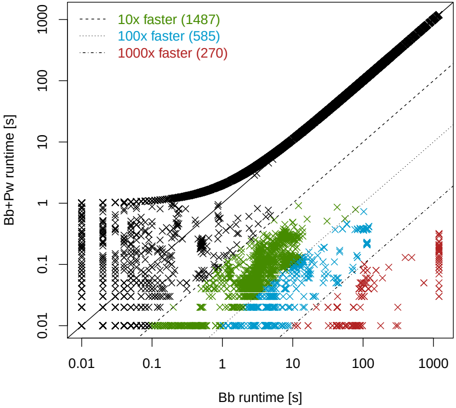
- solved through rewriting alone
- proved by Bb to be unsat within 1200 seconds

Boolector Configurations:

- **Bit-blasting engine: Bb**
  winner of QF_BV main track of SMT-COMP'15
- **Propagation-based: Pw**
- **Sequential portfolio: Bb+Pw**
  Bb with Pw as a preproc. step

Results:

time limit	**Pw** 1 sec	**Bb** 1200 sec	**Bb+Pw** 1200 sec	
# solved	7632	14806	14866	+60
total time	9106	2611840	2513348	

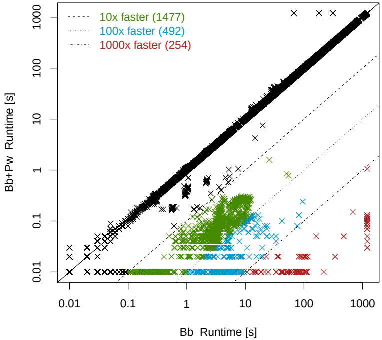


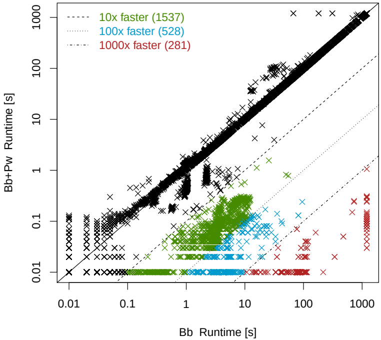
Time limit 1200 seconds (total), 1 second for Pw

Memory limit 7GB

Conclusion

- **complete** propagation-based local search for SMT
  - ⟶ propagation of assignments only
  - ⟶ without brute force randomization or restarts
- **improves** performance
  - ⟶ especially within a sequential portfolio
  - ⟶ in combination with state-of-the-art bit-blasting (Bb+Pw)
- **here:** for the theory of quantifier-free bit-vectors (QF_BV)
  - ⟶ but not limited to QF_BV
  - ⟶ application to other logics interesting direction for **future work**





Time limit 1200 seconds (total), 1000 propagations for Pw

Memory limit 7GB

Time limit 1200 seconds (total), 10000 propagations for Pw

Memory limit 7GB

References

- H. H. Hoos. On the Run-time Behaviour of Stochastic Local Search Algorithms for SAT. In Proc. AAAI/IAAI'99,AAAI Press / The MIT Press, 1999.
- A. Fröhlich, A. Biere, C. M. Wintersteiger and Y. Hamadi. Stochastic Local Search for Satisfiability Modulo Theories. In Proc. AAAI'15, AAAI Press, 2015.
- A. Niemetz, M. Preiner, A. Biere and A. Fröhlich. Improving Local Search For Bit-Vector Logics in SMT with Path Propagation. In Proc. DIFTS'15, 2015.