SWORD: A SAT like Prover Using Word Level Information

Robert Wille, Görschwin Fey, Daniel Große,
Stephan Eggersglüß, Rolf Drechsler

University of Bremen, Germany

{rwille,fey,grosse,segg,drechsle}@informatik.uni-bremen.de

Outline

- Motivation
- SWORD
  - Architecture
  - Using Word Level Information
- Experimental Results
- Conclusion & Future Work

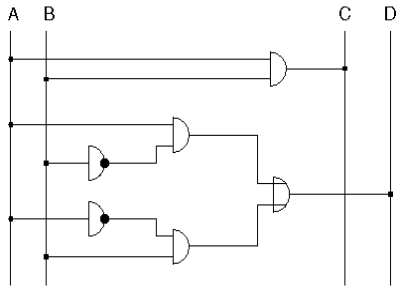
Motivation #1

- Solving NP-hard problems
  - Circuit Verification, Property/Equivalence Checking
  - ATPG
  - Graphcoloring
  - ...

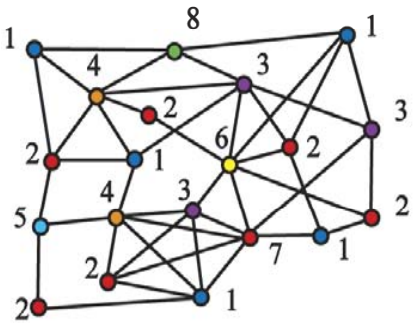
- Common: Exploiting **Boolean Satisfiability**

  For a given Boolean function *f* find an assignment *A*, such that *f(A)=1* or prove that no such assignment exist.

Motivation #2



...



```
p cnf 450 19084
1 2 3 4 5 6 7 8 9 10
16 17 18 19 20 21 22
31 32 33 34 35 36 37
46 47 48 49 50 51 52
61 62 63 64 65 66 67
76 77 78 79 80 81 82
91 92 93 94 95 96 97
106 107 108 109 110
121 122 123 124 125
136 137 138 139 140
151 152 153 154 155
166 167 168 169 170
181 182 183 184 185
196 197 198 199 200
211 212 213 214 215
226 227 228 229 230
241 242 243 244 245
256 257 258 259 260
271 272 273 274 275
```

SAT Solver

Loss of information

- Properties of modules in circuits
- Position of modules in circuits
- Neighbours of a node in a graph
- ...

Advanced Techniques

- Efficient Implication Strategies (BCP)
- Conflict based Learning
- Non-chronological Backtracking
- ...

Goal

- New Solver that
  - Uses state-of-the-art SAT techniques
  - Works on Word Level
  - Utilizes Word Level information for dedicated solve strategies

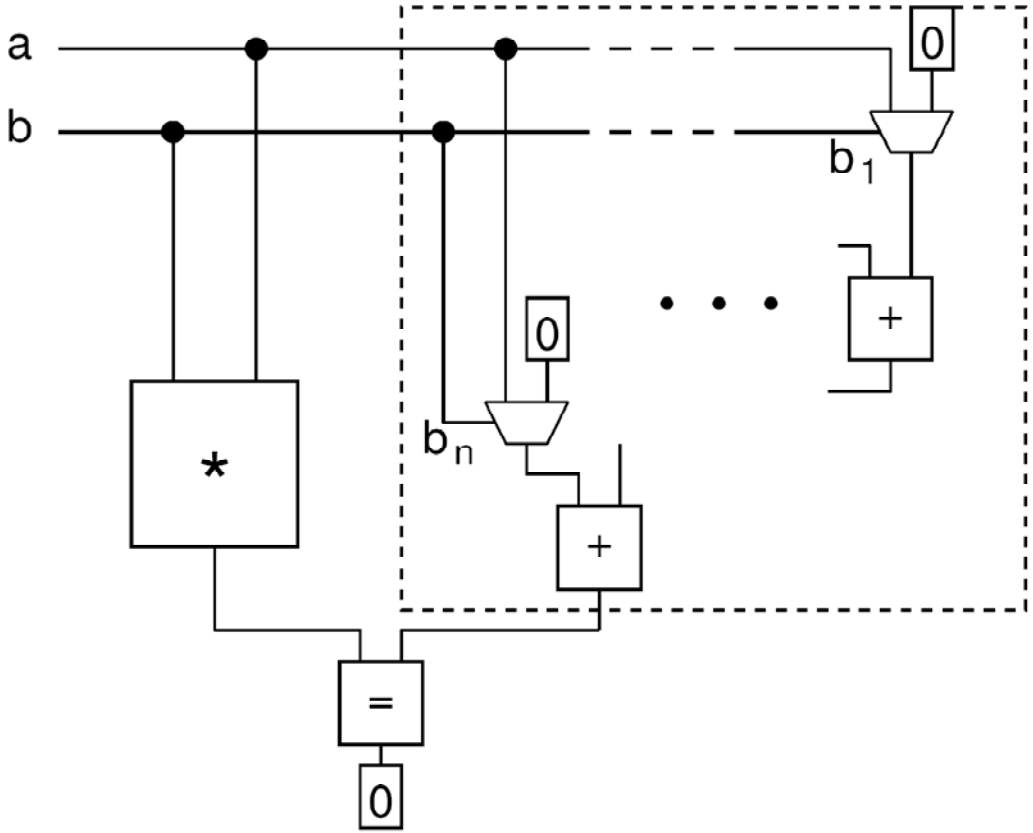
→ More compact representation

→ More efficient algorithms

Outline

- Motivation
- SWORD
  - Architecture
  - Using Word Level Information
- Experimental Results
- Conclusion & Future Work

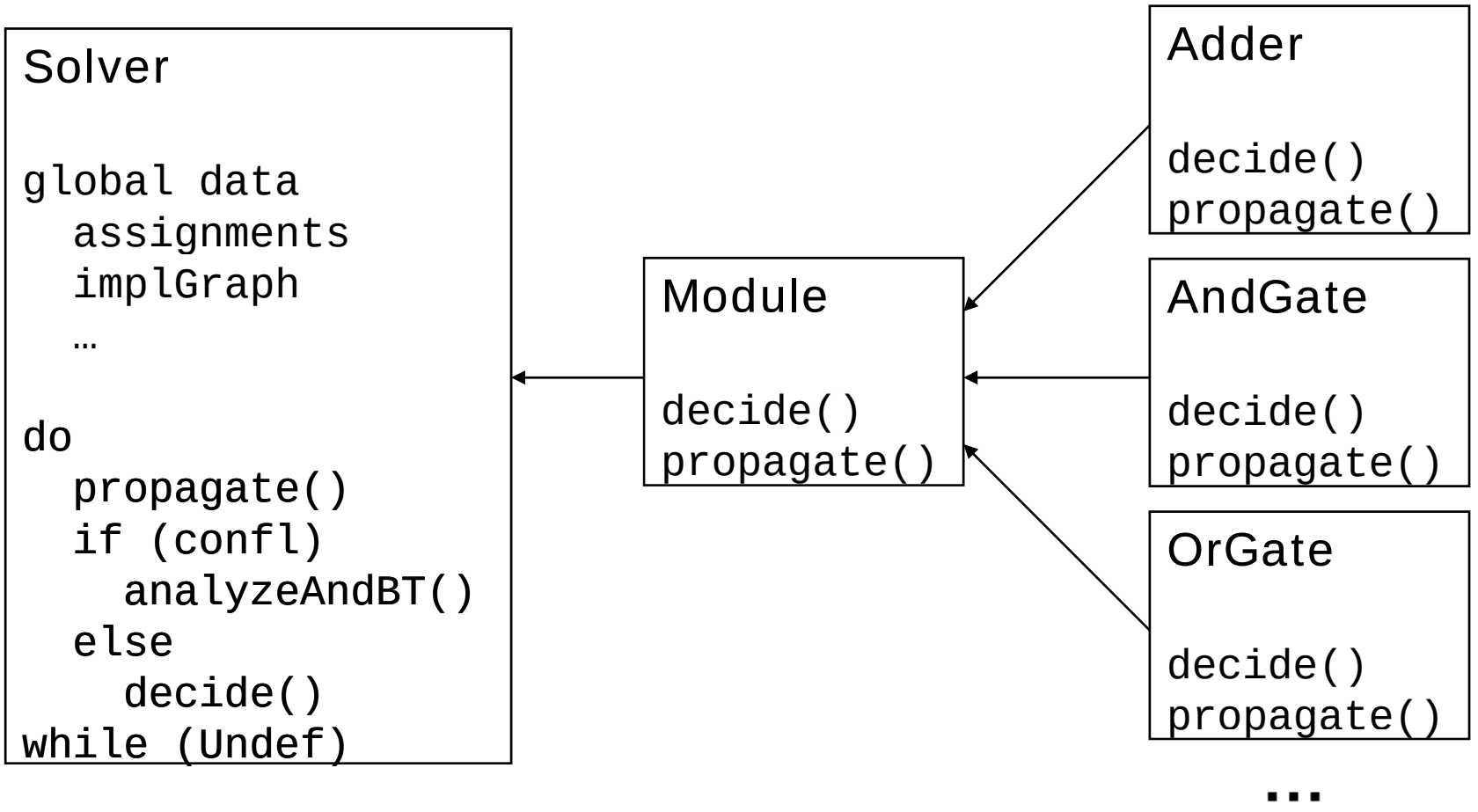
Representation



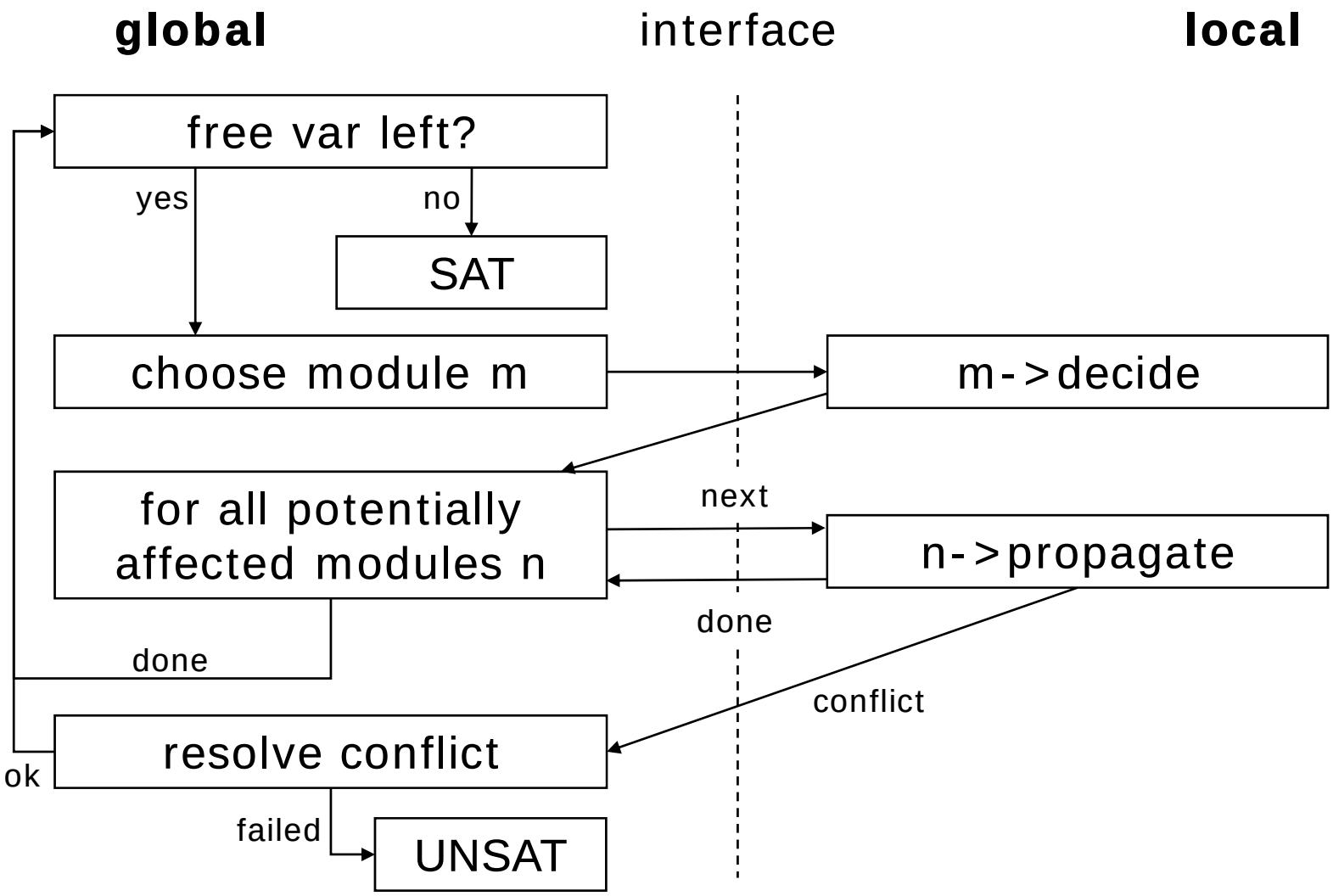
- Modules defined over bitvectors
- Each circuit element has to be supported separately

Architecture

global interface **local**



Flow


global
interface
local
free var left?
yes
no
SAT
choose module m
m->decide
for all potentially affected modules n
next
n->propagate
done
done
conflict
resolve conflict
ok
failed
UNSAT

Outline

- Motivation
- SWORD
  - Architecture
  - Using Word Level Information
- Experimental Results
- Conclusion & Future Work

Global Decision-Heuristic

- Which module makes the best decision?
  - Multiplier often better than an MUX-gate

→ Classify modules into priority-classes

- Priority-class influences the probability that a module makes a decision

Local Decision Heuristic

- ADDER:

$$
\begin{array}{cccccc}
 & & a_2 & & a_1 & a_0 \\
+ & & b_2 & & b_1 & b_0 \\
 & c_3 & & c_2 & & c_1 \\
\hline
 & s_3 & s_2 & & s_1 & s_0
\end{array}
$$

→ Deciding unassigned **least significant** bit first provides the most benefit

- realized as FSM

Local Implication

- ADDER:

$$
\begin{array}{cccccc}
 & & a_2 & & a_1 & & a_0 \\
+ & & b_2 & & b_1 & & b_0 \\
 & c_3 & & c_2 & & c_1 & \\
\hline
 & s_3 & s_2 & & s_1 & & s_0
\end{array}
$$

→ If a_i and b_i are assigned, then c_i and s_{i+1} are implied

Conflict Analysis and Learning

- Quite similar to the classical approach
  - Separate implication graph
  - Additional clause module
- Improved identification of reasons for conflicts
- Conflict clauses are not learned if they contain variables associated to complex modules like multiplier

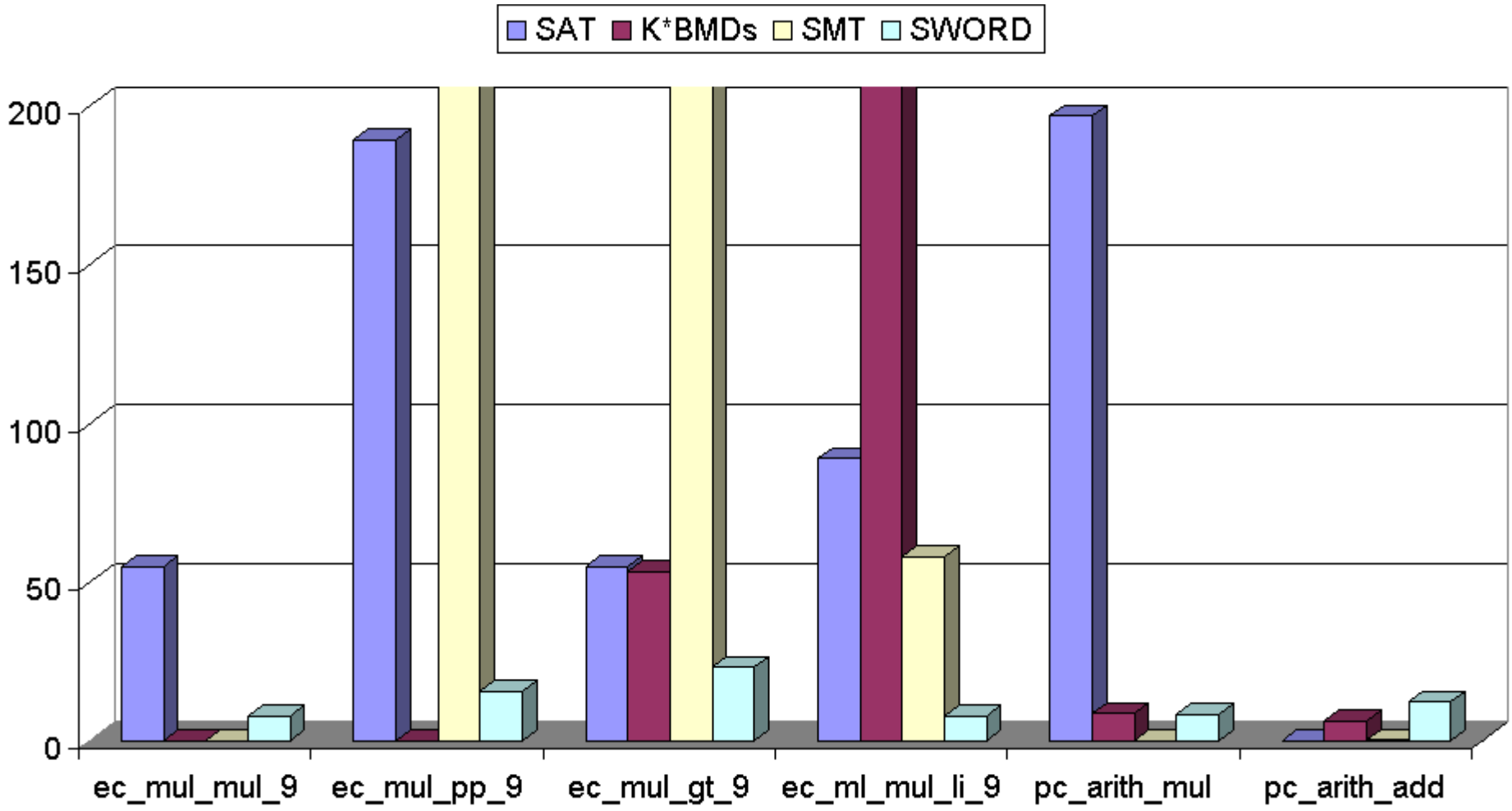
Outline

- Motivation
- SWORD
  - Architecture
  - Using Word Level Information
- Experimental Results
- Conclusion & Future Work

Experimental Setup

- Benchmarks
  - Equivalence Checks using multiplier
    - Word Level vs. Word Level (ec_mul_mul)
    - Word Level vs. Partial Products (ec_mul_pp)
    - Word Level vs. Gate Level (ec_mul_gt)
    - Failed Eqivalence Check (ec_mul_mul_li)
  - Property Checks (pc_arith_mul)
- Solver:
  - MiniSat v1.14
  - K*BMDs
  - SMT (Yices)
  - SWORD
- AMD Athlon 3500+, 1 GB main memory

Experimental Results



Outline

- Motivation
- SWORD
  - Architecture
  - Using Word Level Information
- Experimental Results
- Conclusion & Future Work

Conclusion

- Compact problem representation
- Word Level information is utilized during search process
- Powerful reasoning

Future Work

- Better heuristics & implications-strategies
- Apply further SAT- techniques (restarts, activities ...)
- New conflict analysis (better use of information)
- (Half-)Automatic creation and verification of modules

Questions

- Motivation
- SWORD
  - Architecture
  - Using Word Level Information
- Experimental Results
- Conclusion & Future Work