Lecture 8
SMT Solvers

Zvonimir Rakamarić
University of Utah

slides acknowledgements: Leonardo de Moura

Last Time

- SMT solver Z3
- Simple exercises with Z3

This Time

- SMT solvers
  - What are they?
  - How they work?

Many Theories

- Theory of equality
- Peano arithmetic
- Presburger arithmetic
- Linear integer arithmetic
- Reals
- Rationals
- Arrays
- Recursive data structures
- …

Combination of Theories

- In practice, we often need a combination of theories
- Example:

  $x+2=y \rightarrow f(select(store(a,x,3),y-2)=f(y-x+1)$
- Problem: given satisfiability procedures for conjunction of literals of $Theory_1$ and $Theory_2$, how to decide satisfiability of their combination?

Satisfiability Modulo Theories (SMT) Solver

- Satisfiability checker with built-in support for useful theories
  - Arithmetic
  - Equality with uninterpreted functions
  - Arrays
  - …
- Combines a SAT solver with theory solvers
- Next generation of reasoning engines
  - Automatic
  - Fast

SMT Solvers, Library, Competition

- Solvers
  - AProve, Barcelogic, Boolector, CVC4, MathSAT5, OpenSMT, SMTInterpol, SOLONAR, STP2, veriT, Yices, Z3
- SMT-LIB
  - Standardizes various theories and input format
  - Library of benchmarks
  - http://www.smtlib.org
- SMT-COMP
  - Annual competition
  - http://www.smtcomp.org

Applications

- Test case generation
- Verifying compilers
- Software verification
- Hardware verification
- Equivalence checking
- Type checking
- Model based testing
- Scheduling and planning
- …

Nelson-Oppen Combination Procedure

- Initial State
  - F is a conjunction of literals over $\Sigma_1 \cup \Sigma_2$
- Purification
  - Preserving satisfiability transform F into $F_1 \wedge F_2$, such that $F_i \in \Sigma_i$
- Interaction
  - Deduce an equality x = y if $F_1 \rightarrow x = y$, where x and y are common (shared) variables
  - Update $F_2 := F_2 \wedge x = y$
  - And vice-versa
  - Repeat until no further changes

Nelson-Oppen Combination Procedure

- Component procedures
  - Use individual decision procedures to decide whether F_i is satisfiable
- Return
  - If both return yes, return yes
  - No, otherwise

- Remark:

  $F_i \rightarrow x = y$ iff $F_i \wedge x \neq y$ is not satisfiable

Purification Example

$f(x - 1) - 1 = x \wedge f(y) + 1 = y$

Nelson-Oppen Procedure Example I

$x + y = z \wedge f(z) = z \wedge f(x + y) \neq z$

Nelson-Oppen Procedure Example II

$x+2=y \wedge f(select(store(a,x,3), y-2)) \neq f(y-x+1)$