Lecture 5
First-Order Theories

Zvonimir Rakamarić
University of Utah

slides acknowledgements: Zohar Manna

Announcements

- Posted homework assignment 2
  - Implement KenKen puzzle solver using Z3 (or some other SMT solver)
  - Present your solution in class on Jan 31
- Project deadlines
  - Project ideas (2 points, Feb 14 at 1:25pm)
  - Project proposal (8 points, Feb 28 at 1:25pm)
  - Final presentation (30 points, Apr 18 at 1:25pm, presenting on Apr 23 in class)
    - Can you stay later (or start earlier) on Apr 23?
  - Final report (50 points, Apr 25 at 08:00am)
  - Peer review of other students’ final reports (10 points, Apr 28 at 08:00am)

Last Time

- First-order theories
- Theory of equality
- Arithmetic over integers and natural numbers
  - Peano arithmetic
    - Undecidable
  - Presburger arithmetic
    - No multiplication between two variables
    - Decidable
  - Theory of integers
    - Same expressiveness as Presburger arithmetic
- Reals, rationals, arrays

This Time

- Exercises with SMT solver Z3

Discussion

First-order logic

$$\forall x.\ \exists y.\ \mathrm{p}(\mathrm{x}, \mathrm{y}) \to \neg \mathrm{p}(\mathrm{y}, \mathrm{x})$$

Is this formula satisfiable?

Is this formula valid?

Theory of integers

$$\forall x.\ \exists y.\ \mathrm{x} > \mathrm{y} \to \neg(\mathrm{y} > \mathrm{x})$$

Is this formula satisfiable?

Is this formula valid?

Z3 SMT Solver

- http://rise4fun.com/z3/
- Input format is an extension of SMT-LIB standard
- Commands
  - `declare-const` – declare a constant of a given type
  - `declare-fun` – declare a function of a given type
  - `assert` – add a formula to Z3's internal stack
  - `check-sat` – determine if formulas currently on stack are satisfiable
  - `get-model` – retrieve an interpretation
  - `exit`

Linear Integer Arith. Example 1

$$x \leq y \wedge z = x + 1 \rightarrow z \leq y$$

Linear Integer Arith. Example 2

$$x \leq y \wedge z = x - 1 \rightarrow z \leq y$$

Linear Integer Arith. Example 3

$$1 \leq x \wedge x + y \leq 3 \wedge 1 \leq y \rightarrow x = 1 \vee x = 2$$

Dog, Cat, and Mouse Puzzle (from Z3 page)

- Puzzle
  - Spend exactly $100 and buy exactly 100 animals.
  - Dogs cost $15, cats cost $1, and mice cost 25 cents each.
  - You have to buy at least one of each.
  - How many of each should you buy?
- Use linear integer arithmetic
  - Hint: turn dollar amounts into cents

XOR Swap Algorithm

- Use Z3 to prove that the XOR swap algorithm is correct for 32 bits bitvectors
- XOR swap does not use a temporary variable:
  X := X XOR Y
  Y := Y XOR X
  X := X XOR Y
- Help with syntax
  (declare-const x (_ BitVec 32))
  (bvxor x y)
- SMT solvers are used to prove correctness of compiler optimizations
  - And to synthesize them (project Souper)!

Scheduling Example

	Machine 1	Machine 2
Job 1	2	1
Job 2	3	1
Job 3	2	3

- Table gives time units required to process Job x on Machine y
- For a job, complete a phase on Machine 1 before starting the next on Machine 2
- Find using Z3 whether jobs can be scheduled in T time units
  - Try T=6, T=7, T=8

Next Time

- Symbolic execution