Lecture 19
Course Summary

Zvonimir Rakamarić
University of Utah

Announcements

- Project presentations on Wednesday in class
  - Don’t go over your time limit
- Final project report due on Apr 29
  - Can be pushed back if you email me

Propositional Logic

- Syntax
- Semantics
- Normal forms
  - Negation Normal Form (NNF)
  - Disjunctive Normal Form (DNF)
  - Conjunctive Normal Form (CNF)
- Tseitin transformation for generating CNF

SAT

- Algorithm that in some finite amount of computation decides if given propositional logic formula is satisfiable
- Modern SAT solvers
  - DPLL algorithm
  - Operates on Conjunctive Normal Form (CNF)
- Using MiniSAT
- Encoding problems into SAT

First-Order Logic

- Extends propositional logic with predicates, functions, and quantifiers
- Syntax
- Semantics
- Satisfiability and validity
- Proving validity with semantic argument method using proof rules

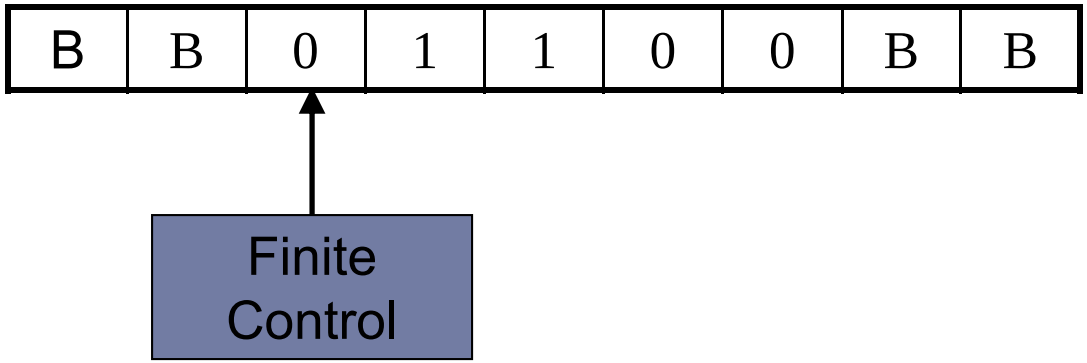
First-Order Theories

- Introduced theories
  - Theory of equality
  - Peano arithmetic
  - Presburger arithmetic
  - Linear integer arithmetic
  - Reals and Rationals
  - Arrays
- Decidability and complexity
- Z3 SMT solver

SMT Solvers

- Nelson-Oppen algorithm for satisfiability of a combination of first-order theories
- Modern SMT solvers combine SAT with Nelson-Oppen
  - SAT solver
    - Manages the boolean structure and assigns truth values to the atoms in a formula
  - Theory solvers
    - Efficiently validate (partial) assignments produced by the SAT solver
- Encoding problems into SMT

Turing Machine and Computability

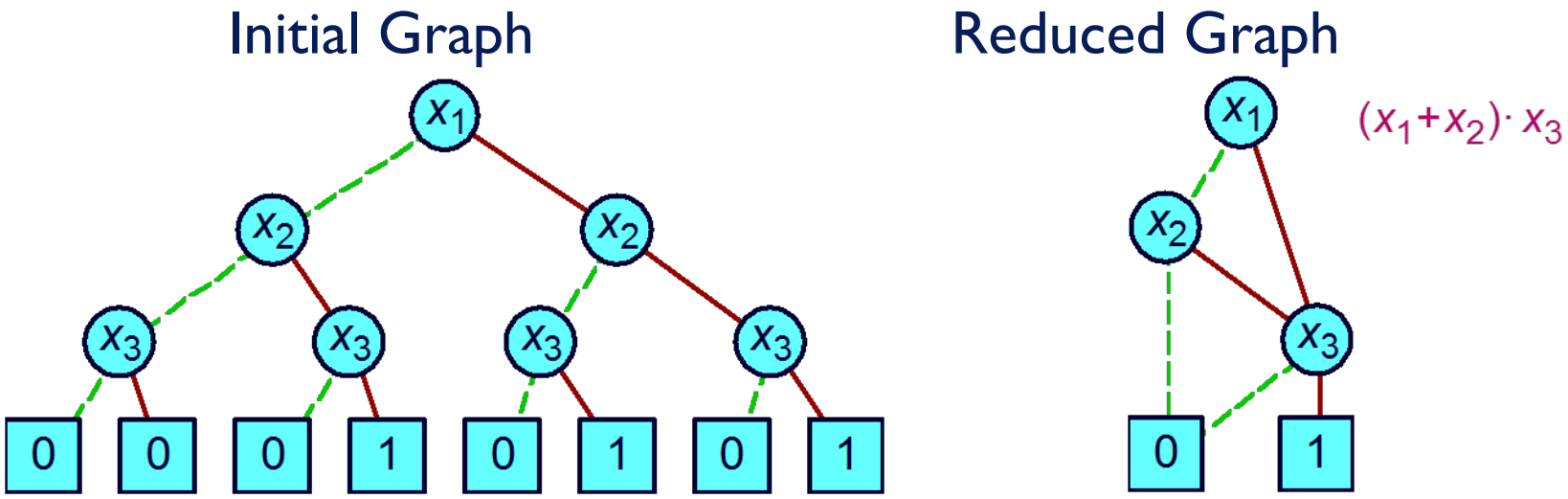


- Any mathematical problem solving that can be described by a mechanical procedure (algorithm) can be modeled by a Turing machine.
- Halting problem
  - Proof of undecidability
- Rice's theorem
  - Any interesting question about the behavior of a program is undecidable

Complexity

- Decision problems
- P complexity class
  - Poly-time algorithm
- NP complexity class
  - Poly-time certifier
- Polynomial transformation
- NP-complete problems
  - A problem in NP with the property that every other problem in NP can be polynomialy transformed into it
- Proving NP-completeness

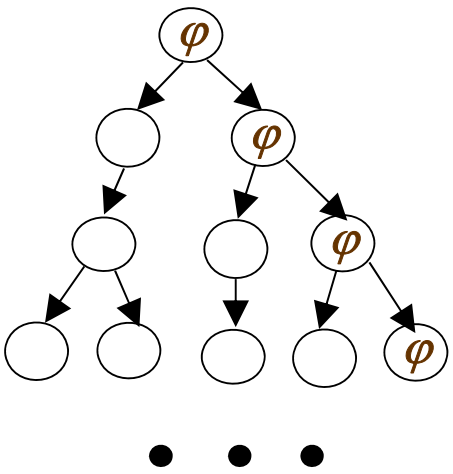
Binary Decision Diagrams



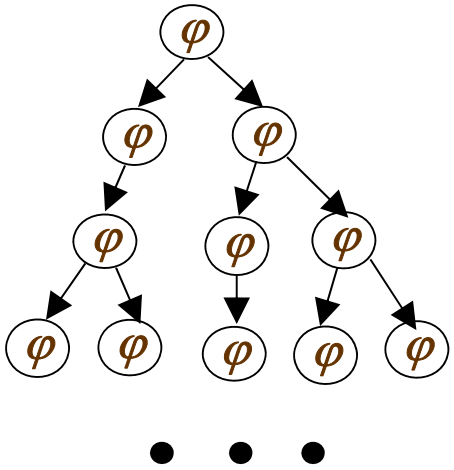
- Canonical data structure for representing quantifier-free boolean formulas
- Efficient boolean operations

Model Checking

- Good for finding bugs in hardware and software
- Kripke structures
- Temporal logics
  - Computational tree logic (CTL)



EG (exists global)



AG (all global)

Model Checking cont.

- Explicit state algorithm for CTL model checking
  - Recursively label states with CTL formulas that hold in a state
- Using NuSMV
- Symbolic model checking
  - Sets of states and the transition relation are represented implicitly by formulas
  - Set operations are defined in terms of formula manipulations
  - Use BDDs

Next Time

- Student project presentations