EECS 598. Program Synthesis: Techniques and Applications

Lecture 4: SAT/SMT

Xinyu Wang

Administrivia

- Paper presentation on Sept 15
  - Send your reviews by **midnight Sept 14**
  - Use template (link here)
  - Email title: [598 review] YourName: PaperTitle

Last lecture

- L2 paper
  - Use types (inferred from examples) to prune partial programs
  - Use examples to further prune partial programs
  - Use cost model for generalization

Today’s lecture

- Propositional logic
- First-order logic
- First-order theories

Propositional logic

Propositional logic syntax

- E.g., $(p \wedge q) \rightarrow (p \vee \neg q)$

- Logical constants: $\top$ (“true”, 1) and $\bot$ (“false”, 0)
- Propositional variable: $p, q, r, x, y, z, p_1, q_1, r_1, \ldots$
- Logic connectives: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

- Formulas of propositional logic
  - Each logical constant is a formula
  - Each propositional variable is a formula
  - If F_1 and F_2 are formulas, all of the following are also formulas

    $(F_1), \neg F_1, F_1 \wedge F_2, F_1 \vee F_2, F_1 \rightarrow F_2, F_1 \leftrightarrow F_2$

Propositional logic semantics

- What does a formula evaluate to?

- Interpretation I: assignment of boolean values to propositional variables

$$I : \{p \mapsto \top, q \mapsto \bot, \ldots\}$$

- A formula F evaluates to a truth value, under an interpretation I
  - $I \vDash F$: F evaluates to $\top$ under I (i.e., F is a satisfying assignment/model)
  - $I \nvDash F$: F evaluates to $\bot$ under I (i.e., F is a falsifying assignment/counter-model)

- $\vDash$ is defined inductively

Propositional logic semantics (cont'd)

- Base cases
  - $I \models \top$ $\quad I \not\models \bot$ $\quad I \models p$ iff $I[p] = \top$ $\quad I \not\models p$ iff $I[p] = \bot$

- Inductive cases
  - $I \models (F)$ iff $I \models F$
  - $I \models \neg F$ iff $I \not\models F$
  - $I \models F_1 \wedge F_2$ iff $I \models F_1$ and $I \models F_2$
  - $I \models F_1 \vee F_2$ iff $I \models F_1$ or $I \models F_2$
  - $I \models F_1 \rightarrow F_2$ iff $I \not\models F_1$ or $I \models F_2$
  - $I \models F_1 \leftrightarrow F_2$ iff $I \models F_1$ and $I \models F_2$
    or $I \not\models F_1$ and $I \not\models F_2$

Examples

- Consider $F : (p \vee q) \rightarrow (p \wedge q)$
  - What does F evaluate to under $I : \{p \mapsto \top, q \mapsto \top\}$
  - What does F evaluate to under $I : \{p \mapsto \bot, q \mapsto \bot\}$
  - What does F evaluate to under $I : \{p \mapsto \top, q \mapsto \bot\}$

Satisfiability and validity

- F is **satisfiable** iff **there exists** an interpretation I such that $I \vDash F$
  - F is **unsatisfiable** iff **for all** interpretations I, $I \nvDash F$
- F is **valid** iff **for all** interpretations I, $I \vDash F$
  - F is **not valid** iff **there exists** an interpretations I such that $I \nvDash F$
- Duality between satisfiability and validity

$$F \text{ is valid iff } \neg F \text{ is unsatisfiable}$$

  - … which means: if we know how to check satisfiability, we can check validity as well

Examples

- Decide sat, unsat, valid, not valid?

sat? unsat? valid? not valid?

  - p
  - $(p \wedge q) \rightarrow p$
  - $(p \rightarrow q) \rightarrow (\neg(p \wedge \neg q))$

Deciding satisfiability and validity

- Manually
  - Truth table method
  - Semantic argument method

- Automatically
  - NP-complete
  - SAT solvers (e.g., Microsoft z3, CVC4)
  - Demo (link)

First-order logic

First-order logic (FOL) vs. propositional logic

- FOL has more constants
  - Propositional logic: $\top$ and $\bot$
  - FOL: object constants, function constants, relation constants
- FOL has quantifiers
- FOL syntax and semantics become a bit more complex

First-order logic (FOL) syntax

- Object constants (a, b, c, …)
  - Objects in a universe of discourse
  - E.g., people {Jack, Smith, …}, numbers {…, -1, 0, 1, …}
- Function constants (f, g, h, …)
  - Functions
  - E.g., motherOf, ageOf, plus
  - Arity: unary, binary, ternay, …
- Relation constants (p, q, r, …)
  - Relations between objects, or properties of objects, also called predicates
  - E.g., loves, isBiggerThan
  - Arity: unary, binary, ternay, …
- Variables (x, y, z, …)

First-order logic (FOL) syntax (cont'd)

- Terms
  - Basic terms: any object constant or a variable (e.g., Jack, Apple, x, y)
  - Compound terms: function constants applied to terms (e.g., motherOf(Jack), f(x))

- Formulas
  - Base case: relation constant applied to terms (e.g., isOlder(motherOf(Jack), Jack))
  - Inductive case:
    - If F_1, F_2 are formulas, then $F_1 \star F_2$ is also formula ($\star \in \{ \wedge , \vee , \rightarrow , \leftrightarrow \}$)
    - If F is formula, then (F), $\neg F$ are also formulas
    - If F is formula and x is variable, then $\forall x \,.\, F$, $\exists x \,.\, F$ are also formulas

Examples

- $\forall x \,.\, p(a, f(b)) \wedge q(x)$
  - Object constants? Function constants? Relation constants? Variables?

- "For any x, y, z, if x is bigger than y in size and y is bigger than z, then x is bigger than z." Express this in FOL using function constant *size*, relation constant *biggerThan.*

First-order logic (FOL) semantics

- What does a FOL formula evaluate to?

- Similar to propositional logic, need an interpretation
- Different from propositional logic, need universe of discourse (i.e., universe, domain)

- Universe of discourse U
  - Non-empty set of objects
  - E.g., set of positive integers, all real numbers, all students in this class

First-order logic (FOL) semantics (cont'd)

- First-order interpretation
  - Mapping I from object, function, relation constants to objects in universe U
  - E.g.,
    - Object constants: $a, b, c \in U$
    - Unary function constants: $f : U \to U$
    - Binary relation constant: $p \subseteq U^2$
    - $U = \{1,2,3,4\}$
    - A possible interpretation:

$$I(a) = 1, I(b) = 2, I(c) = 3 \qquad I(f) = \{1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1\}$$

$$I(p) = \{\langle 1,2 \rangle, \langle 3,4 \rangle\}$$

First-order logic (FOL) semantics (cont'd)

- Variable assignment σ
  - Given formula F and universe U, σ maps each variable in F to an object in U

First-order logic (FOL) semantics (cont'd)

- What does FOL formula F evaluate to?
- Given U, I, σ, FOL formula F evaluates to a truth value
  - $U, I, \sigma \vDash F$: F evaluates to $\top$ under U, I, σ
  - $U, I, \sigma \nvDash F$: F evaluates to $\bot$ under U, I, σ
- $\vDash$ is defined inductively

First-order logic (FOL) semantics (cont'd)

- Base cases
  - $U, I, \sigma \vDash \top \qquad U, I, \sigma \nvDash \bot$
  - $U, I, \sigma \vDash p(t_1, \ldots, t_n)$ iff $\langle \langle I, \sigma \rangle (t_1), \ldots, \langle I, \sigma \rangle (t_n) \rangle \in I(p)$
    - Evaluating terms
      - Base cases: $\langle I, \sigma \rangle (a) = I(a) \qquad \langle I, \sigma \rangle (x) = \sigma(x)$
      - Inductive case: $\langle I, \sigma \rangle (f(t_1, \ldots, t_n)) = I(f)(\langle I, \sigma \rangle (t_1), \ldots, \langle I, \sigma \rangle (t_n))$

First-order logic (FOL) semantics (cont'd)

- Inductive cases
  - $U, I, \sigma \vDash (F)$ iff $U, I, \sigma \vDash F$
  - $U, I, \sigma \vDash \neg F$ iff $U, I, \sigma \nvDash F$
  - $U, I, \sigma \vDash F_1 \wedge F_2$ iff $U, I, \sigma \vDash F_1$ and $U, I, \sigma \vDash F_2$
  - $U, I, \sigma \vDash F_1 \vee F_2$ iff $U, I, \sigma \vDash F_1$ or $U, I, \sigma \vDash F_2$
  - $U, I, \sigma \vDash F_1 \rightarrow F_2$ iff $U, I, \sigma \nvDash F_1$ or $U, I, \sigma \vDash F_2$
  - $U, I, \sigma \vDash F_1 \leftrightarrow F_2$ iff $U, I, \sigma \vDash F_1$ and $U, I, \sigma \vDash F_2$ or $U, I, \sigma \nvDash F_1$ and $U, I, \sigma \nvDash F_2$
  - $U, I, \sigma \vDash \forall x \,.\, F$ iff for all $o \in U, U, I, \sigma[x \mapsto o] \vDash F$
  - $U, I, \sigma \vDash \exists x \,.\, F$ iff there exists $o \in U,$ such that $U, I, \sigma[x \mapsto o] \vDash F$

Examples

- Consider $U = \{ \star , \bullet \}, \sigma = \{x \mapsto \bullet \}$, and I :

$$I(a) = \bullet , I(b) = \star$$

$$I(f) = \{ \star \mapsto \bullet , \bullet \mapsto \star \}$$

$$I(p) = \{\langle \bullet , \bullet \rangle, \langle \star , \bullet \rangle\}$$

- Given U, I, σ, what do these formulas evaluate to?
  - $\forall x \,.\, p(a, x)$
  - $\forall x \,.\, p(x, a)$
  - $\exists x \,.\, p(a, x)$
  - $\exists x \,.\, p(f(x), f(a))$

Satisfiability and validity

- A FOL formula F is **satisfiable** iff **there exists** a universe U, an interpretation I, and a variable assignment σ such that $U, I, \sigma \vDash F$
  - Otherwise, unsatisfiable
- F is **valid** iff **for all** universes U, interpretations I, variable assignments σ, $U, I, \sigma \vDash F$
  - Otherwise, not valid

Examples

- Is $\forall x \,.\, \exists y \,.\, p(x, y)$
  - satisfiable?
  - valid?

- Is $(\forall x \,.\, p(x, x)) \rightarrow (\exists y \,.\, p(y, y))$
  - satisfiable?
  - valid?

Deciding satisfiability and validity

- Manually
  - Truth table? No, you can’t
  - Semantic argument method

- Automatically
  - Undecidable (for satisfiability and validity)
  - Solvers (e.g., Microsoft z3, CVC4)
  - Solvers work pretty well in practice!

First-order theories

Why first-order theories

- So far, propositional logic and first-order logic
  - Propositional logic is limited in expressiveness
  - FOL is more expressive, but functions are uninterpreted (one can assign any meaning)
- In many cases, we want functions to have certain meanings (e.g., +, =, >)
- First-order theories assign meanings to symbols

First-order theories syntax

- A first-order theory has
  - object/function/relation constants, variables, quantifiers, logical connectives (just like in FOL)
  - axioms (new!)

- E.g., let's make up a first-order theory — theory of heights T_H
  - T_H has only one relation constant called $taller$ and no other constants
  - T_H has one axiom $\forall x, y \,.\, (taller(x, y) \rightarrow \neg taller(y, x))$
  - Is $\forall x \,.\, \exists y \,.\, taller(y, x)$ in T_H?
  - Is $\forall x \,.\, taller(Jack, x)$ in T_H?

First-order theories semantics

- Axioms provide meaning of symbols
- Some universes/interpretations may not be consistent with axioms
  - E.g., $U = \{A, B\}, I(taller) = \{\langle A, B\rangle, \langle B, A\rangle\}$ is not consistent with the axiom $\forall x, y \,.\, (taller(x, y) \rightarrow \neg taller(y, x))$ in T_H
  - We are only interested in those interpretations that are consistent!
- Given U, I, σ, formula F can be evaluated in the same way as in FOL, but we only consider interpretations that are consistent with axioms
  - … which means some formulas not valid in FOL may be valid in first-order theories

Satisfiability and validity modulo theory T

- "modulo" $\approx$ "in terms of"

- Formula F is **satisfiable modulo T** if **there exists** a universe U, an interpretation I, and a variable assignment σ, such that (1) U, I is consistent with axioms in T, and (2) $U, I, \sigma \vDash F$

- Formula F is **valid modulo T** if **for all** universes U, interpretations I, and variable assignments σ, if U, I is consistent with axioms in T then we have $U, I, \sigma \vDash F$

- SMT solvers: Microsoft z3, CVC4, …

Quiz

- If F is valid in FOL, is it also valid modulo T ?
- If F is not valid in FOL, is it also not valid modulo T ?
- If F is satisfiable in FOL, is it also satisfiable modulo T ?
- If F is not satisfiable in FOL, is it also not satisfiable modulo T ?

- If F is valid modulo T, is it also valid in FOL?
- If F is not valid modulo T, is it also not valid in FOL?
- If F is satisfiable modulo T, is it also satisfiable in FOL?
- If F is not satisfiable modulo T, is it also not satisfiable in FOL?

Theory of equality

- Extend FOL to include a “built-in” predicate =

- Axioms assign meaning to =

$\forall x \,.\, x = x$ (reflexivity)

$\forall x, y \,.\, (x = y \rightarrow y = x)$ (symmetry)

$\forall x, y, z \,.\, (x = y \wedge y = z \rightarrow x = z)$ (transitivity)

$\forall x_1, \ldots, x_n, y_1, \ldots, y_n \,.\, \bigwedge_i x_i = y_i \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$ (function congruence)

$\forall x_1, \ldots, x_n, y_1, \ldots, y_n \,.\, \bigwedge_i x_i = y_i \leftrightarrow p(x_1, \ldots, x_n) = p(y_1, \ldots, y_n)$ (predicate congruence)

Theory of equality (cont'd)

- Is $\forall x, y, z \,.\, \left(x = y \wedge y = z \rightarrow f(x) = f(z) \right)$ in theory of equality?
  - Is it satisfiable, unsatisfiable, valid?
- Is $\forall x, y, z, w \,.\, \left(x = y \wedge z = w \rightarrow f(x + z) = f(y + w) \right)$ in theory of equality?
- Undecidable (but quantifier-free fragment is decidable)

Theory of integers

- Also known as linear arithmetic over integers
- Symbols that are allowed:
  - Object constants: $\ldots, -2, -1, 0, 1, 2, \ldots$
  - Function constants: $\ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots, +, -$
  - Relation constants: $=, >$
  - Variables: $x, y, z, \ldots$
  - Logical connectives: $\wedge, \vee, \rightarrow, \leftrightarrow, \neg$
- Axioms
  - Define meaning of symbols
  - E.g., $\forall x \,.\, x + 0 = x$

Theory of integers (cont'd)

- Is $\forall x, y, z, w \,.\, \left(x = y \wedge z = w \rightarrow f(x + z) = f(y + w) \right)$ in theory of integers?
- Is $\forall x, y \,.\, \exists z \,.\, x + y = z$ in theory of integers?
  - Is it satisfiable, unsatisfiable, valid?
- Is $\forall x, y \,.\, \exists z \,.\, x \cdot y = z$ in theory of integers?
- Decidable

Other theories

- Peano arithmetic
- Presburger arithmetic
- Theory of rationals
- Theory of arrays
- …
- You can also combine theories

Summary of this lecture

- Propositional logic: true, false, propositional variables, logical connectives
- First-order logic: universe, object constants, functions, predicates, quantifiers
- First-order theories: axioms
- Satisfiability, validity
- SAT/SMT solvers: Microsoft z3, CVC4, …