SATISFIABILITY MODULO THEORIES (SMT)

SMT - INTRODUCTION

- In FOL, predicates and functions are in general uninterpreted
- In practice, we may have a specific meaning in mind for certain predicates and functions (e.g. $=$, $\leq$, $+$, etc.)
- First-order Theories allow us to formalise the meaning of certain structures.

FIRST-ORDER THEORY

- A First-order Theory (T) is defined by two components:
  - Signature (Σ_T) : Contains constant, predicate and function symbols
  - Axioms (A_T) : Set of closed FOL formulae containing only the symbols in Σ_T
- A Σ_T-formula is a FOL formula which only contains symbols from Σ_T

SATISFIABILITY AND VALIDITY

MODULO THEORIES

- An interpretation I is called a $T-$interpretation if it satisfies all the axioms of the theory T
  - For all $A \in A_T$, $I \models A$
- A Σ_T-formula F is satisfiable modulo T if there is a $T-$interpretation that satisfies F
- A Σ_T-formula F is valid modulo T if every $T-$interpretation satisfies F
  - Also denoted as $T \models F$

ENTAILS

QUESTIONS

- Which is of the following holds?
  - F is satisfiable ⇒ F is satisfiable modulo T
  - F is satisfiable modulo T ⇒ F is satisfiable
- Which is of the following holds?
  - F is valid ⇒ F is valid modulo T
  - F is valid modulo T ⇒ F is valid

COMPLETENESS AND DECIDABILITY

- A theory T is complete if for every closed formula F, either F or ¬F is valid modulo T
  - $T \vDash F$ or $T \vDash \neg F$
- Is FOL (i.e.'empty' theory) complete?
  - No. Consider $F : \exists x \, . \, p(x)$. Neither F nor $\neg F$ is valid.
- A theory T is decidable if $T \vDash F$ is decidable for every formula F.
- Even though FOL (or empty theory) is undecidable, various useful theories are actually decidable.

THEORY OF EQUALITY ($T_=$)

- One of the simplest first-order theories
  - $\Sigma_=$: All symbols used in FOL and the special symbol $=$
  - Allows uninterpreted functions and predicates, but $=$ is interpreted.
- Axioms of Equality:

1. $\forall x.\ x = x$	(reflexivity)
2. $\forall x, y.\ x = y \ \rightarrow\ y = x$	(symmetry)
3. $\forall x, y, z.\ x = y\ \wedge\ y = z\ \rightarrow\ x = z$	(transitivity)

AXIOMS OF EQUALITY

- Function Congruence: For a n-ary function f, two terms $f(\overrightarrow{x})$ and $f(\overrightarrow{y})$ are equal if $\overrightarrow{x}$ and $\overrightarrow{y}$ are equal:

$$\forall \overline{x}, \overline{y}. \left(\bigwedge_{i=1}^{n} x_i = y_i \right) \rightarrow f(\overline{x}) = f(\overline{y})$$

- Predicate Congruence: For a n-ary predicate p, two formulas $p(\overrightarrow{x})$ and $p(\overrightarrow{y})$ are equivalent if $\overrightarrow{x}$ and $\overrightarrow{y}$ are equal:

$$\forall \overline{x}, \overline{y}. \left(\bigwedge_{i=1}^{n} x_i = y_i \right) \rightarrow (p(\overline{x}) \leftrightarrow p(\overline{y}))$$

AXIOMS OF EQUALITY

- Function Congruence and Predicate Congruence are actually Axiom Schemes, which can be instantiated with any function or predicate to get axioms.
- For example, for a unary function g, the function congruence axiom is:
  - $\forall x, y \,.\, x = y \rightarrow g(x) = g(y)$

ANNOUNCEMENT

- Change in Grading Policy
  - Project: 30%
  - Assignments (3 Theory + 2 Tool): ~~40%~~ 35%
  - Class Participation: 5%
  - End sem - 30%
- Please participate in the class discussions
  - “Raise hand” if you want to answer a question or ask some doubt.
  - As far as possible, please unmute yourself and communicate verbally rather than using chat.
  - I am going to start asking questions to specific students now.
- Please revise the previous lectures before attending a new lecture.

EXAMPLE OF A $T_=$-INTERPRETATION

Consider the domain $D_I = \{a, b\}$.
What would be an appropriate
interpretation $\alpha_I(=)$?

FRAGMENTS OF THEORY

- A fragment of a theory is a syntactically-restricted subset of formulae of the theory.
  - For example, the **quantifier-free fragment** of a theory T is the set of Σ_T-formulae that do not contain any quantifiers.
- Technically, while considering validity of quantifier-free formula, we assume that all variables are universally quantified.
  - Hence, for validity, the quantifier-free fragment is the same as the fragment which allows only universal quantification.
- Quantifier-free fragments are of great practical and theoretical importance.

SEMANTIC ARGUMENT METHOD FOR VALIDITY MODULO THEORY

- We can use the semantic argument method to prove validity modulo theory.
- Along with the usual proof rules, axioms of the theory can be used to derive facts.
- As usual, we look for a contradiction in all branches.

EXAMPLE

Prove that $F : a = b \wedge b = c \rightarrow g(f(a), b) = g(f(c), a)$ is valid

1.	I	$\not\models$	F	assumption
2.	I	$\models$	$a = b \;\wedge\; b = c$	1, $\rightarrow$
3.	I	$\not\models$	$g(f(a), b) = g(f(c), a)$	1, $\rightarrow$
4.	I	$\models$	$a = b$	2, $\wedge$
5.	I	$\models$	$b = c$	2, $\wedge$
6.	I	$\models$	$a = c$	4, 5, (transitivity)
7.	I	$\models$	$f(a) = f(c)$	6, (function congruence)
8.	I	$\models$	$b = a$	4, (symmetry)
9.	I	$\models$	$g(f(a), b) = g(f(c), a)$	7, 8 (function congruence)
10.	I	$\models$	$\perp$	3, 9

DECIDABILITY OF VALIDITY IN $T_=$

- $T_=$ being an extension of FOL, the validity problem is clearly undecidable.
- However, validity in the quantifier-free fragment of $T_=$ is decidable, but NP-complete.
- Conjunctions of quantifier-free equality constraints can be solved efficiently.
  - Congruence closure algorithm can be used to decide satisfiability of conjunctions of equality constraints in polynomial time

PRESBURGER ARITHMETIC ($T_{\mathbb{N}}$)

THE THEORY OF NATURAL NUMBERS

- Signature, $\Sigma_{\mathbb{N}}$: $0, 1, +, =$
  - $0, 1$ are constants
  - $+$ is a binary function
  - $=$ is a binary predicate.
- Axioms:

1. $\forall x.\ \neg(x + 1 = 0)$ (zero)
2. $\forall x, y.\ x + 1 = y + 1 \ \rightarrow\ x = y$ (successor)
3. $F[0]\ \wedge\ (\forall x.\ F[x] \rightarrow F[x+1])\ \rightarrow\ \forall x.\ F[x]$ (induction)
4. $\forall x.\ x + 0 = x$ (plus zero)
5. $\forall x, y.\ x + (y + 1) = (x + y) + 1$ (plus successor)

PRESBURGER ARITHMETIC

INTERPRETATION

1. $\forall x.\ \neg(x + 1 = 0)$ (zero)
2. $\forall x, y.\ x + 1 = y + 1 \ \rightarrow\ x = y$ (successor)
3. $F[0]\ \land\ (\forall x.\ F[x] \rightarrow F[x+1])\ \rightarrow\ \forall x.\ F[x]$ (induction)
4. $\forall x.\ x + 0 = x$ (plus zero)
5. $\forall x, y.\ x + (y + 1) = (x + y) + 1$ (plus successor)

- The intended $T_{\mathbb{N}}$−interpretation is $\mathbb{N}$, the set of natural numbers
- Does there exist a finite subset of $\mathbb{N}$ which is also a $T_{\mathbb{N}}$−interpretation?
  - Which axiom(s) will be violated by any finite subset?
- Are negative numbers allowed by the axioms?

PRESBURGER ARITHMETIC

EXAMPLES

- Examples of $\Sigma_{\mathbb{N}}$-formulae
  - $\forall x \,.\, \exists y \,.\, x = y + 1$
  - $3x + 5 = 2y$
    - Can be expressed as $(x + x + x) + (1 + 1 + 1 + 1 + 1) = (y + y)$
  - $\forall x \,.\, \exists y \,.\, x + f(y) = 5$ is not a $\Sigma_{\mathbb{N}}$-formula
- How to express $x < y$ and $x \leq y$?
  - $\exists z \,.\, z \neq 0 \wedge y = x + z$
  - $\exists z \,.\, y = x + z$

PRESBURGER ARITHMETIC

EXPANDING TO THEORY OF INTEGERS

- How to expand the domain to negative numbers?
  - $x + y < 0$
  - Converted to $(x_p - x_n) + (y_p - y_n) < 0$
  - Converted to $x_p + y_p < x_n + y_n$
  - Converted to $\exists z \, . \, z \neq 0 \wedge x_p + y_p + z = x_n + y_n$

THEORY OF INTEGERS ($T_{\mathbb{Z}}$)

LINEAR INTEGER ARITHMETIC

SIGNATURE:

$$\{\ldots, -2, -1, 0, 1, 2, \ldots\} \cup \{\ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots\} \cup \{+, -, =, <, \leq\}$$

- Signature:
  - $\ldots, -2, -1, 0, 1, 2, \ldots$ are constants
  - $\ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots$ are unary functions to represent coefficients of variables
  - $+, -$ are binary functions
  - $=, <, \leq$ are binary predicates.
- Any $T_{\mathbb{Z}}-$formula can be converted to a $T_{\mathbb{N}}-$formula.

PRESBURGER ARITHMETIC

DECIDABILITY

- Validity in quantifier-free fragment of Presgurber Arithmetic is decidable
  - NP-Complete
- Validity in full Presburger Arithmetic is also decidable
  - Super Exponential Complexity : $O(2^{2^n})$
- Conjunctions of quantifier-free linear constraints can be solved efficiently
  - Using Simplex Method or Omega test.
- Presburger Arithmetic is also complete
  - For any closed $T_{\mathbb{N}}-$formula F, either $T_{\mathbb{N}} \models F$ or $T_{\mathbb{N}} \models \neg F$

ANNOUNCEMENTS

- Assignment-1 (Theory) will be released next week.
  - Questions on PL,FOL,SMT.
  - Deadline will be 10 days after release.
  - Use Latex for writing the solutions, submit the final pdf. Compulsory.
  - Please work on the assignment on your own. Any plagiarism attempts will result in 0 marks in the assignment and 1-grade drop penalty.
- Course Project
  - Start working on the project proposal (Due Date: Feb 28).
  - Explore sub-areas, case studies, study advanced verification tools,…
  - We will have one-on-one meetings next Tuesday during the lecture to discuss plans.
  - I will share a poll to pick a 10-minute slot.

THEORY OF RATIONALS

- Theory of Rationals ($T_{\mathbb{Q}}$)
  - Also called Linear Real Arithmetic.
  - Same symbols as Presburger arithmetic, but many more axioms.
    - Interpretation is $\mathbb{R}$.
  - Example: $\exists x \,.\, 2x = 3$. Satisfiable in $T_{\mathbb{Q}}$.
    - Is it satisfiable in $T_{\mathbb{Z}}$?
  - Conjunctive quantifier-free fragment is efficiently decidable in polynomial time.

THEORIES ABOUT DATA STRUCTURES

- So far, we have looked at theories of numbers and arithmetic.
- But, we can also formalize behaviour of data structures using theories.
    - Very useful for automated verification

THEORY OF ARRAYS (T_A)

- Signature, $\Sigma_A : \{ \cdot [\cdot], \cdot \langle \cdot \triangleleft \cdot \rangle, = \}$
- $a[i]$ is a binary function
  - Read array a at index i
  - Returns the value read.
- $a\langle i \triangleleft v \rangle$ is a ternary function
  - Write value v at index i in array a
  - Returns the modified array.
- $=$ is a binary predicate

EXAMPLES

- $(a\langle 2 \lhd 5\rangle)[2] = 5$
  - Write the value 5 at index 2 in array a, then from the resulting array, the value at index 2 is 5.
- $(a\langle 2 \lhd 5\rangle)[2] = 3$
  - Write the value 5 at index 2 in array a, then from the resulting array, the value at index 2 is 3.
- According to the usual semantics of arrays, which of the formulae is valid/sat/unsat?

AXIOMS OF T_A

- The axioms of T_A include reflexivity, symmetry and transitivity axioms of $T_=$.
- Array Congruence:
  - $\forall a, i, j \,.\, i = j \rightarrow a[i] = a[j]$
- Read over Write 1:
  - $\forall a, i, j, v \,.\, i = j \rightarrow a\langle i \triangleleft v\rangle[j] = v$
- Read over Write 2:
  - $\forall a, i, j, v \,.\, i \neq j \rightarrow a\langle i \triangleleft v\rangle[j] = a[j]$

EXAMPLE

Prove that $F : \forall a, i, e \,.\, a[i] = e \rightarrow \forall j \,.\, a\langle i \triangleleft e\rangle[j] = a[j]$ is valid

1. $I \vDash a[i] = e$	assumption, $\rightarrow$
2. $I \nvDash \forall j \,.\, a\langle i \triangleleft e\rangle[j] = a[j]$	assumption, $\rightarrow$
3. $I_1 \vDash a\langle i \triangleleft e\rangle[j] \neq a[j]$	$2, \forall, j \in D_I$
4. $I_1 \vDash i = j$	3,contra-positive of ROW-2
5. $I_1 \vDash a\langle i \triangleleft e\rangle[j] = e$	4,ROW-1
6. $I_1 \vDash a\langle i \triangleleft e\rangle[j] = a[i]$	$1,5$,transitivity of $=$
7. $I_1 \vDash a[i] = a[j]$	4,Array Congruence
8. $I_1 \vDash a\langle i \triangleleft e\rangle[j] = a[j]$	$6,7$,transitivity of $=$
9. $I_1 \vDash \perp$	$3,8$,contradiction

DECIDABILITY IN T_A

- The validity problem in T_A is not decidable.
  - Any formula in FOL can be encoded as an equisatisfiable T_A–formula (How?).
- Quantifier-free fragment of T_A is decidable.
  - Unfortunately, this only allows us to express properties about specific elements of the array.
- Richer Fragments of T_A are also decidable.
  - Array Property Fragment, which allows (syntactically restricted) formulae with universal quantification over index variables.

QUANTIFIER-FREE FRAGMENT OF FOL

- Formula constructed using FOL syntax, but without quantifiers.
  - All variables are free.
- For the satisfiability problem, we assume implicit existential quantification of all variables.
- For the validity problem, we assume implicit universal quantification of all variables.
  - Validity and Satisfiability are still duals: For a quantifier-free F, $\forall * .F$ is valid iff $\exists * . \neg F$ is unsatisfiable.
- Any quantifier-free FOL formula can be converted to a PL formula. (How?)
  - Hence, Validity in the quantifier-free fragment of FOL is decidable and NP-complete.

OTHER COMMON THEORIES

- Many more theories..
  - Theory of bit-vectors
  - Theory of Lists
  - Theory of Heap
  - …
- The aim is to build efficient decision procedures for the satisfiability modulo theory problem.

COMBINATION OF THEORIES

- We talked about individual theories: $T_=, T_{\mathbb{N}}, T_{\mathbb{Z}}, T_A, \ldots$, each imposing different restrictions on the symbols used in a FOL formula.
- However, in practice, we may have FOL formulae which combine symbols across theories.
- Consider the formula: $x' = f(x) + 1$.
  - Which theories are used in this formula?
  - $T_{\mathbb{Z}}$ and $T_=$

COMBINED THEORIES

- Given two theories T_1 and T_2, such that $\Sigma_1 \cap \Sigma_2 = \{ = \}$, the combined theory $T_1 \cup T_2$ is defined as follows:
  - Signature: $\Sigma_1 \cup \Sigma_2$
  - Axioms: $A_1 \cup A_2$
- Consider the following formula:
  - $1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$
  - Is it well-formed in $T_= \cup T_{\mathbb{N}}$?
  - Is it valid/sat/unsat in $T_= \cup T_{\mathbb{N}}$?
  - How about in $T_=$?