CS389L: Automated Logical Reasoning

Lecture 10: Overview of First-Order Theories

Işıl Dillig

Motivation

- Last few lectures: Full first-order logic
- In FOL, functions/predicates are **uninterpreted** (i.e., structure can assign any meaning)
- But in many cases, we have a particular meaning in mind (e.g., $=, \leq$ etc.)
- First-order theories allow us to give meaning to the symbols used in a first-order language

Signature and Axioms of First-Order Theory

- A first-order theory T consists of:
  1. Signature Σ_T: set of constant, function, and predicate symbols
  2. Axioms A_T: A set of FOL sentences over Σ_T
- Σ_T formula: Formula constructed from symbols of Σ_T and variables, logical connectives, and quantifiers.
- Example: We could have a theory of heights T_H with signature $\Sigma_H : \{taller\}$ and axiom:

$$\forall x, y. \ (taller(x, y) \rightarrow \neg taller(y, x))$$

- Is $\exists x. \forall z. taller(x, z) \wedge taller(y, w)$ legal Σ_H formula? Yes
- What about $\exists x. \forall z. taller(x, z) \wedge taller(joe, tom)$? No

Axioms of First-Order Theory

- The axioms A_T provide the meaning of symbols in Σ_T.
- Specifically, axioms ensure that some interpretations legal in standard FOL are not legal in T
- Example: Consider relation constant $taller$, and $U = \{A, B, C\}$
- In FOL, possible interpretation: $I(taller) : \{\langle A, B\rangle, \langle B, A\rangle\}$
- In our theory of heights, this interpretation is not legal b/c does not satisfy axioms

Models of T

- A structure $M = \langle U, I\rangle$ is a model of theory T, or T-model, if $M \models A$ for every $A \in A_T$.
- Example: Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, A\rangle, \langle B, B\rangle\}$
- Is this a model of T? No
- Now, consider same U and interpretation $\{\langle A, B\rangle\}$. Is this a model? Yes
- Suppose our theory had another axiom:

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

- Consider $I(taller) : \{\langle A, B\rangle, \langle B, C\rangle\}$. Is (U, I) a model? No

Satisfiability and Validity Modulo T

- Formula F is satisfiable modulo T if there exists a T-model M and variable assignment σ such that $M, \sigma \models F$
- Formula F is valid modulo T if for all T-models M and variable assignments σ, $M, \sigma \models F$
- Question: How is validity modulo T different from FOL-validity?
- Answer: Disregards all structures that do not satisfy theory axioms.
- If a formula F is valid modulo theory T, we will write $T \models F$.
- Theory T consists of all sentences that are valid in T.

Questions

Consider some first order theory T:

- If a formula is valid in FOL, is it also valid modulo T? Yes
- If a formula is valid modulo T, is it also valid in FOL? No
- Counterexample: This formula is valid in "theory of heights":

$$\neg taller(x, x)$$

Equivalence Modulo T

- Two formulas F_1 and F_2 are equivalent modulo theory T if for every T-model M and for every variable assignment σ:

$$\boxed{M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2}$$

- Another way of stating equivalence of F_1 and F_2 modulo T:

$$T \models F_1 \leftrightarrow F_2$$

- Example: Consider a theory $T_=$ with predicate symbol $=$ and suppose A_T gives the intended meaning of equality to $=$.
- Are $x = y$ and $y = x$ equivalent modulo $T_=$? Yes
- Are they equivalent according to FOL semantics? No

Completeness of Theory

- A theory T is complete if for every sentence F, if T entails F or its negation:

$$\boxed{T \models F \text{ or } T \models \neg F}$$

- Question: In first-order logic, for every closed formula F, is either F or $\neg F$ valid?
- Answer: No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.

The Plan

- Remainder of this lecture: Introduction to commonly-used first-order theories:
  1. Theory of equality
  2. Peano Arithmetic
  3. Presburger Arithmetic
  4. Theory of Rationals
  5. Theory of Arrays
- In the following lectures, we will further explore these theories and look at decision procedures.

Overview of the Theory of Equality $T_=$

- Extends first-order logic with a "built-in" equality predicate $=$
- Signature:

$$\Sigma_= : \{=, a, b, c, \cdots, f, g, h, \cdots, p, q, r, \cdots\}$$

  - $=$, a binary predicate, interpreted by axioms.
  - all constant, function, and predicate symbols.

Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$
- Equality is reflexive, symmetric, and transitive:
  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)

Example

- Consider universe $U = \{\circ, \bullet\}$.
- Which interpretations of $=$ are allowed according to axioms?
  - $I(=) : \{\langle \circ, \bullet \rangle, \langle \bullet, \circ \rangle\}$?
  - $I(=) : \{\langle \circ, \circ \rangle, \langle \bullet, \bullet \rangle\}$?
  - $I(=) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle\}$?

Axioms of the Theory of Equality, cont.

- Function congruence:
  For any n-ary function f, two terms $f(\vec{x})$ and $f(\vec{y})$ are equal if $\vec{x}$ and $\vec{y}$ are equal:

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

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

  $$\forall x_1, \dots, x_n, y_1, \dots, y_n. \bigwedge_i x_i = y_i \rightarrow (p(x_1, \dots, x_n) \leftrightarrow p(y_1, \dots, y_n))$$

Congruence and Axiom Schemata

- Function/predicate congruence "axioms" stand for a set of axioms, instantiated for each function and predicate symbol.
- Thus, these are not really axioms, but axiom schemata.
- Example: For unary functions g and h, function congruence axiom scheme stands for two axioms:
  1. $\forall x, y.\ (x = y \rightarrow g(x) = g(y))$
  2. $\forall x, y.\ (x = y \rightarrow h(x) = h(y))$

Example

- Consider universe $\{\circ, \bullet, \star\}$, and

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

- Are the following valid interpretations?
  - $I(f) = \{\bullet \mapsto \circ, \circ \mapsto \star, \star \mapsto \star\}$
  - $I(f) = \{\bullet \mapsto \bullet, \circ \mapsto \bullet, \star \mapsto \bullet\}$
  - $I(f) = \{\bullet \mapsto \circ, \circ \mapsto \bullet, \star \mapsto \star\}$

Proving Validity in $T_=$ using Semantic Arguments

- Semantic argument method can be used to prove $T_=$ validity.
- In addition to proof rules for FOL, our proof can also use axioms of $T_=$.
- As before, if we derive contradiction in every branch, formula is valid modulo $T_=$.

Example

Prove

$$F:\ a = b \ \wedge\ b = c \ \rightarrow\ g(f(a), b) = g(f(c), a) \qquad T_E\text{-valid.}$$

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

Decidability and Completeness Results for $T_=$

- Is the full theory of equality decidable?
- No, because it is an extension of FOL
- However, quantifier-free fragment of $T_=$ is decidable but NP-complete
- Is $T_=$ complete? (i.e., for any F, $T_= \models F$ or $T_= \models \neg F$?)
-

Theories Involving Natural Numbers and Integers

- There are three major logical first-order theories involving natural numbers and arithmetic.
- Peano arithmetic: Allows multiplication and addition over natural numbers
- Presburger arithmetic: Allows only addition over natural numbers
- Theory of integers: Equivalent in expressiveness to Presburger arithmetic, but more convenient notation

Peano Arithmetic Signature

- The theory of Peano arithmetic T_{PA} has signature:

$$\Sigma_{PA} : \{0, 1, +, \cdot, =\}$$

- $0, 1$ are constants
- $+, \cdot$ binary functions
- $=$ is a binary predicate

Peano Arithmetic Examples

- Question: Is the following a well-formed formula in T_{PA}?

$$x + y = 1 \lor f(x) = 1 + 1$$

-
- What about $\forall x. \exists y. \exists z.\ x + y = 1 \lor z \cdot x = 1 + 1$?
- What about $2x = y$?
- But can be rewritten to equivalent T_{PA} formula:

$$(1 + 1) \cdot x = y$$

The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity
- In addition, axioms to give meaning to remaining symbols:
  1. $\forall x.\ \neg(x + 1 = 0)$: 0 minimal element of $\mathbb{N}$ (zero)
  2. $\forall x.\ x + 0 = x$: 0 identity for addition (plus zero)
  3. $\forall x, y.\ x + 1 = y + 1 \ \rightarrow\ x = y$ (successor)
  4. $\forall x, y.\ x + (y + 1) = (x + y) + 1$ (plus successor)
  5. $\forall x.\ x \cdot 0 = 0$ (times zero)
  6. $\forall x, y.\ x \cdot (y + 1) = x \cdot y + x$ (times successor)

Last Axiom

- One last axiom schema for induction:

$$(F[0] \ \land\ (\forall x.\ F[x] \ \rightarrow\ F[x + 1])) \ \rightarrow\ \forall x.\ F[x]$$

- States that any valid interpretation must obey induction

Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn't have inequality symbols $<, \leq, <, \geq$
- But all of these are expressible in T_{PA}
- Example: How can we express $x \cdot y \geq z$ in T_{PA}?
- Example: How can we express $x \cdot y < z$ in T_{PA}?

Decidability and Completeness Results for Peano Arithmetic

- Validity in full T_{PA} is undecidable. (Gödel)
- Validity in even the quantifier-free fragment of T_{PA} is undecidable. (Matiyasevitch, 1970)
- T_{PA} is also incomplete. (Gödel)
- Implication of this: There are valid propositions of number theory that are not valid according to T_{PA}
- To get decidability and completeness, we need to drop multiplication!

Presburger Arithmetic

- The theory of Presburger arithmetic $T_{\mathbb{N}}$ has signature:

$$\Sigma_{\mathbb{N}} : \{0, 1, +, =\}$$

- Axioms define meaning of symbols:
  1. $\forall x.\ \neg(x + 1 = 0)$ (zero)
  2. $\forall x.\ x + 0 = x$ (plus zero)
  3. $\forall x, y.\ x + 1 = y + 1 \ \rightarrow\ x = y$ (successor)
  4. $\forall x, y.\ x + (y + 1) = (x + y) + 1$ (plus successor)
  5. $F[0]\ \wedge\ (\forall x.\ F[x]\ \rightarrow\ F[x + 1])\ \rightarrow\ \forall x.\ F[x]$ (induction)

Decidability and Completeness Results for Presburger Arithmetic

- Validity in quantifier-free fragment of Presburger arithmetic is decidable (coNP-complete).
- Validity in full Presburger arithmetic is also decidable (Presburger, 1929)
- But super exponential complexity: $O(2^{2^n})$
- Presburger arithmetic is also complete: For any sentence F, $T_{\mathbb{N}} \models F$ or $T_{\mathbb{N}} \models \neg F$
- Admits quantifier elimination: For any formula F in $T_{\mathbb{N}}$, there exists an equivalent quantifier-free formula F'.

Theory of Integers $T_{\mathbb{Z}}$

- Signature:

$$\Sigma_{\mathbb{Z}} : \{\ldots, -2, -1, 0,\ 1,\ 2,\ \ldots, -3\cdot, -2\cdot,\ 2\cdot,\ 3\cdot,\ \ldots,\ +,\ -,\ =,\ >\}$$

- Also referred to as the theory of linear arithmetic over integers
- Equivalent in expressiveness to Presburger arithmetic (i.e., every $T_{\mathbb{Z}}$ can be encoded as a formula in Presburger arithmetic)

Theory of Rationals

- So far, looked at theories involving arithmetic over integers
- Next: the theory of rationals $T_{\mathbb{Q}}$, which is much more efficiently decidable
- Defined by signature:

$$\Sigma_{\mathbb{Q}} : \{0,\ 1,\ +,\ -,\ =,\ \geq\}$$

- Signature does not allow strict inequality, but easy to express:

$$\forall x, y. \exists z. x + y > z \Rightarrow \forall x, y. \exists z. \neg(x + y = z) \wedge x + y \geq z$$

Distinction between Theory of Rationals and Presburger Arithmetic

- $T_{\mathbb{Q}}$ has too many axioms, so we won't discuss them
- Distinction between $T_{\mathbb{Z}}$ and $T_{\mathbb{Q}}$: Rational numbers do not satisfy $T_{\mathbb{Z}}$ axioms, but they satisfy $T_{\mathbb{Q}}$ axioms
- Example: $\exists x. \ (1+1)x = 1+1+1$ Is this formula valid in $T_{\mathbb{Q}}$?
- Is it valid in $T_{\mathbb{Z}}$?
- In general, every formula valid in $T_{\mathbb{Z}}$ is valid in $T_{\mathbb{Q}}$, but not vice versa

Decidability and Complexity Results for $T_{\mathbb{Q}}$

- Full theory of rationals is decidable, but doubly exponential
- Conjunctive quantifier-free fragment efficiently decidable (polynomial time)

Theories about Data Structures

- So far, we only considered first-order theories involving numbers and arithmetic
- There are also theories that formalize data structures used in programming
- We'll look at one example: theory of arrays
- Commonly used in software verification

Theory of Arrays

Signature

$$\Sigma: \{\cdot[\cdot], \ \cdot\langle\cdot \triangleleft \cdot\rangle, \ =\}$$

where

- $a[i]$ binary function – read array a at index i ("read(a,i)")
- $a\langle i \triangleleft v\rangle$ ternary function – write value v to index i of array a ("write(a,i,e)")
- $a\langle i \triangleleft v\rangle$ represents the resulting array after writing value v at index i

Example Formulas in Theory of Arrays

- Example: $(a\langle 2 \triangleleft 5\rangle)[2] = 5$
- Says: "The value stored at position 2 of an array to whose second position we wrote the value 5 is 5"
- Example: $(a\langle 2 \triangleleft 5\rangle)[2] = 3$
- Says: "The value stored at position 2 of an array to whose second position we wrote the value 5 is 3"
- According to the usual semantics of array read and write, is the first formula valid/satisfiable/unsat?
- What about second formula?

Axioms of T_A

- To define "intended semantics of array read and write", we need to provide axioms of T_A.
- Axioms of T_A include reflexivity, symmetry, and transitivity
- In addition, they include axioms unique to arrays:
  1. $\forall a, i, j. \ i = j \ \rightarrow \ a[i] = a[j]$ (array congruence)
  2. $\forall a, v, i, j. \ i = j \ \rightarrow \ a\langle i \triangleleft v\rangle[j] = v$ (read-over-write 1)
  3. $\forall a, v, i, j. \ i \neq j \ \rightarrow \ a\langle i \triangleleft v\rangle[j] = a[j]$ (read-over-write 2)

Example

- Is the following T_A formula valid?

$$F : a[i] = e \rightarrow (\forall j.\ a\langle i \triangleleft e\rangle[j] = a[j])$$

- For any $j = i$, old value of j was already e, so its value didn't change
- Let's prove its validity using the semantic argument method
- Assume there exists a model M and variable assignment σ that does not satisfy F and derive contradiction.

Example cont.

1.	M, σ	$\not\models$	$a[i] = e \rightarrow (\forall j.\ a\langle i \triangleleft e\rangle[j] = a[j])$	assumption
2.	M, σ	$\models$	$a[i] = e$	1, $\rightarrow$
3.	M, σ	$\not\models$	$\forall j.\ a\langle i \triangleleft e\rangle[j] = a[j]$	1, $\rightarrow$
4.	$M, \sigma[j \mapsto k]$	$\not\models$	$a\langle i \triangleleft e\rangle[j] = a[j]$	3, $\forall$
5.	$M, \sigma[j \mapsto k]$	$\models$	$a\langle i \triangleleft e\rangle[j] \neq a[j]$	4, $\neg$
6.	$M, \sigma[j \mapsto k]$	$\models$	$i = j$	5, r-o-w 2
7.	$M, \sigma[j \mapsto k]$	$\models$	$a[i] = a[j]$	6, cong
8.	$M, \sigma[j \mapsto k]$	$\models$	$a\langle i \triangleleft e\rangle[j] = e$	6, r-o-w 1
9.	$M, \sigma[j \mapsto k]$	$\models$	$a\langle i \triangleleft e\rangle[j] = a[i]$	2,8,trans
10.	$M, \sigma[j \mapsto k]$	$\models$	$a\langle i \triangleleft e\rangle[j] = a[j]$	9,7,trans
11.	$M, \sigma[j \mapsto k]$	$\models$	$\bot$	5,10

Decidability Results for T_A

- The full theory of arrays if not decidable.
- The quantifier-free fragment of T_A is decidable.
- Unfortunately, the quantifier-free fragment not sufficiently expressive in many contexts
- Thus, people have studied other richer fragments that are still decidable.
- Example: array property fragment (disallows nested arrays, restrictions on where quantified variables can occur)

Combination of Theories

- So far, we only talked about individual first-order theories.
- Examples: $T_=, T_{PA}, T_{\mathbb{Z}}, T_A, \ldots$
- But in many applications, we need combined reasoning about several of these theories
- Example: The formula $f(x) + 3 = y$ isn't a well-formed formula in any individual theory, but belongs to combined theory $T_{\mathbb{Z}} \cup T_=$

Combined Theories

- Given two theories T_1 and T_2 that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$
- Signature of $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$
- Axioms of $T_1 \cup T_2$: $A_1 \cup A_2$
- Is this a well-formed $T_= \cup T_{\mathbb{Z}}$ formula?

$$1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

- Is this formula satisfiable according to axioms $A_{\mathbb{Z}} \cup A_=$?

Decision Procedures for Combined Theories

- Given decision procedures for individual theories T_1 and T_2, can we decide satisfiability of formulas in $T_1 \cup T_2$?
- In the early 80s, Nelson and Oppen showed this is possible
- Specifically, if
  1. quantifier-free fragment of T_1 is decidable
  2. quantifier-free fragment of T_2 is decidable
  3. and T_1 and T_2 meet certain technical requirements
- then quantifier-free fragment of $T_1 \cup T_2$ is also decidable
- Also, given decision procedures for T_1 and T_2, Nelson and Oppen's technique allows deciding satisfiability $T_1 \cup T_2$

Plan for Next Few Lectures

- We'll talk about decision procedures for some interesting first order-theories
- Next lecture: Quantifier-free theory of equality
- Later: Theory of rationals, Presburger arithmetic
- Initially, we'll only focus on decision procedures for formulas without disjunctions
- Ok because we can always convert to DNF to deal with disjunctions – just not very efficient!
- Later in the course, we'll see about how to handle disjunctions much more efficiently