First-Order Theories

CS560: Reasoning About Programs

Roopsha Samanta

PURDUE UNIVERSITY

Partly based on slides by Aaron Bradley and Isil Dillig

Roadmap

Previously

- FOL

Today

- Overview of first-order theories

Review

Syntax of FOL

constants: a, b, c
variables: x, y, z
n-ary functions: f, g, h
n-ary predicates: p, q, r

logical connectives: $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$
quantifiers: $\exists$, $\forall$

Term
constant, variable, or,
n-ary function applied to n terms

Atom
$\top$, $\bot$, or,
n-ary predicate applied to n terms

Literal
atom or its negation

FOL formula:
Literal, or, application of logical connectives to an FOL formula, or, application of a quantifier to an FOL formula

Semantics of FOL: first-order structure $\langle U, I \rangle$

- **Universe** of discourse/domain, U:
  - Non-empty set of values or objects of interest
  - May be finite (set of students at Purdue), countably infinite (integers) or uncountable infinite (positive reals)

- **Interpretation**, I: Mapping of variables, functions and predicates to values in U
  - I maps each variable symbol x to some value $I[x] \in U$
  - I maps each n-ary function symbol f to some function $f_I: U^n \rightarrow U$
  - I maps each n-ary predicate symbol p to some predicate $p_I: U^n \rightarrow \{true, false\}$

Evaluation of formulas: inductive definition

Base Cases:

$\langle U, I \rangle \vDash \top$
$\langle U, I \rangle \nvDash \bot$
$\langle U, I \rangle \vDash p(t_1, \ldots, t_n)$
iff $I[p(t_1, \ldots, t_n)] = true$

Inductive Cases:

$\langle U, I \rangle \vDash \neg F$ iff $\langle U, I \rangle \nvDash F$
$\langle U, I \rangle \vDash F_1 \vee F_2$ iff $\langle U, I \rangle \vDash F_1$ or $\langle U, I \rangle \vDash F_2$
…
$\langle U, I \rangle \vDash \forall x. F$ iff for all $v \in U, I[x \mapsto v] \vDash F$
$\langle U, I \rangle \vDash \exists x. F$ iff there exists $v \in U, I[x \mapsto v] \vDash F$

x-variant of $\langle \mathrm{U}, \mathrm{I} \rangle$ that agrees with U, I on everything except the variable x, with $\mathrm{I}[\mathrm{x}] = \mathrm{v}$.

Soundness and Completeness of Proof Rules

Soundness:
If every branch of semantic argument proof derives $\perp$, then F is valid

Completeness:
If F is valid, there exists a finite-length semantic argument proof in which every branch derives $\perp$.

Undecidability of FOL

A problem is decidable if there exists a procedure that, for any input:
1. halts and says “yes” if answer is positive, and
2. halts and says “no” if answer is negative
(Such a procedure is called an algorithm or a decision procedure)

Undecidability of FOL [Church and Turing]:
Deciding the validity of an FOL formula is undecidable

Deciding the validity of a PL formula is decidable
The truth table method is a decision procedure

Church

Turing

Semi-decidability of FOL

A problem is semi-decidable iff there exists a procedure that, for any input:

1. halts and says “yes” if answer is positive, and
2. may not terminate if answer is negative.

Semi-decidability of FOL

A problem is semi-decidable iff there exists a procedure that, for any input:
1. halts and says “yes” if answer is positive, and
2. may not terminate if answer is negative.

Semi-decidability of FOL:
For every valid FOL formula, there exists a procedure (semantic argument method) that always terminates and says “yes”.
If an FOL formula is invalid, there exists no procedure that is guaranteed to terminate.

Motivation

- FOL is very expressive, powerful and undecidable in general
- Some application domains do not need the full power of FOL
- **First-order theories** are useful for reasoning about specific applications
  - e.g., programs with arithmetic operations over integers
- Specialized, efficient decision procedures!

First-Order Theories

Signature Σ_{T} : set of constant, function, and predicate symbols
Axioms A_T : set of closed formulas over Σ_T

First-Order Theories

Signature Σ_{T} : set of constant, function, and predicate symbols
Axioms A_T : set of closed formulas over Σ_T

Axioms provide the meaning of symbols in Σ_T

First-Order Theories

Signature Σ_T : set of constant, function, and predicate symbols

Axioms A_T : set of closed formulas over Σ_T

Axioms provide the meaning of symbols in Σ_T

Σ_T-formula : constructed from symbols of Σ_T, and variables, logical connectives, and quantifiers

First-Order Theories

Signature Σ_{T} : set of constant, function, and predicate symbols
Axioms A_T : set of closed formulas over Σ_T

Axioms provide the meaning of symbols in Σ_T

Σ_{T}-formula : constructed from symbols of Σ_T, and variables, logical connectives, and quantifiers

T-model : a first-order structure $M = \langle U, I \rangle$ such that $M \vDash A$ for all $A \in A_T$

Satisfiability and Validity Modulo T

F is **satisfiable modulo $\boldsymbol{T}$** iff there exists some T-model M : $M \vDash F$

F is **valid modulo $\boldsymbol{T}$** (written $T \vDash F$) iff for all T-models M : $M \vDash F$

Satisfiability and Validity Modulo T

F is **satisfiable modulo $\boldsymbol{T}$** iff there exists some T-model M : $M \vDash F$

F is **valid modulo $\boldsymbol{T}$** (written $T \vDash F$) iff for all T-models M : $M \vDash F$

The theory $\boldsymbol{T}$ consists of all closed formulas that are valid modulo T

Satisfiability and Validity Modulo T

F is **satisfiable modulo $\boldsymbol{T}$** iff there exists some T-model M : $M \vDash F$

F is **valid modulo $\boldsymbol{T}$** (written $T \vDash F$) iff for all T-models M : $M \vDash F$

The theory $\boldsymbol{T}$ consists of all closed formulas that are valid modulo T

- How is validity modulo T different from FOL-validity?
- If a formula is valid in FOL, is it also valid modulo T for any T?
- If a formula is valid modulo T for some T, is it valid in FOL?

Theory of heights T_H

Σ_H : $\{ \text{taller} \}$

A_H : $\{ \forall x, y.\ \text{taller}(x, y) \rightarrow \neg \text{taller}(y, x) \}$

$U = \{A, B\}$

$I[\text{taller}] \neq \{(A, B), (B, A)\}$

$I[\text{taller}] = \{(A, B)\}$

$\langle U, I \rangle$ is T_H model !

$\neg \text{taller}(x, x)$ T_H-valid

Not valid FOL

Equivalence Modulo T

Two formulas F_1 and F_2 are **equivalent modulo T**

iff $T \vDash F_1 \leftrightarrow F_2$, i.e.,

iff for every T- model M, $M \vDash F_1$ iff $M \vDash F_2$

$T_= : \Sigma_= : \{=\}, A_= : \{\text{Equality axioms}\}$

$T_= \overset{?}{\vDash} x=y \leftrightarrow y=x$

$M \vDash x=y$ iff $M \vDash y=x$

Equisat:

F_1 sat iff F_2 sat

$\exists M_1 \cdot M_1 \vDash F_1$ iff

$\exists M_2 \cdot M_2 \vDash F_2$

M_1 & M_2 can be different

Completeness of a theory

$\vDash$: $\vdash$

valid provable

A theory T is complete iff for every formula F, either $T \vDash F$ or $T \vDash \neg F$

Decidability of a theory

A theory T is decidable iff for every formula F, there is an algorithm that :

1. terminates and answers “yes” if F is valid modulo T, and
2. terminates and answers “no”, if F is not valid modulo T

Next: decidable first-order theories, and theories with decidable fragments

Common first-order theories

- Theory of equality (with uninterpreted functions)
- Peano arithmetic (first-order arithmetic)
- Presburger arithmetic
- Theory of reals
- Theory of rationals
- Theory of arrays

Theory of equality $T_=$

Signature

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

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

Theory of equality $T_=$

Axioms

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)
4. for n-ary function symbol f, (function congruence)
   $\forall x_1, \dots \dots, x_n, y_1, \dots . y_n.\ (\bigwedge_\mathrm{i}\ x_i = y_i) \rightarrow \big(f(x_1, \dots \dots, x_n) = f(y_1, \dots ., y_n)\big)$
5. for each n-ary predicate symbol p, (predicate congruence)
   $\forall x_1, \dots \dots, x_n, y_1, \dots . y_n.\ (\bigwedge_\mathrm{i} x_i = y_i) \rightarrow ((p(x_1, \dots \dots, x_n) \leftrightarrow p(y_1, \dots ., y_n))$

Theory of equality $T_=$

Axioms

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

Equivalence relation

4. for n-ary function symbol f, (function congruence)
   $\forall x_1, \ldots \ldots, x_n, y_1, \ldots . y_n.\ (\bigwedge_i x_i = y_i) \rightarrow \big(f(x_1, \ldots \ldots, x_n) = f(y_1, \ldots ., y_n)\big)$
5. for each n-ary predicate symbol p, (predicate congruence)
   $\forall x_1, \ldots \ldots, x_n, y_1, \ldots . y_n.\ (\bigwedge_i x_i = y_i) \rightarrow ((p(x_1, \ldots \ldots, x_n) \leftrightarrow p(y_1, \ldots ., y_n))$

Proving validity in $T_=$ using semantic arguments

T_{EUF}

Example: Prove F is valid in $T_=$

$$F : a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a)$$

Suppose not; then there exists a $T_=$-model M such that $M \nvDash F$. Then,

1.	$M \nvDash F$	assumption
2.	$M \vDash a = b \land b = c$	1, $\rightarrow$
3.	$M \nvDash g(f(a), b) = g(f(c), a)$	1, $\rightarrow$
4.	$M \vDash a = c$	2, transitivity
5.	$M \vDash f(a) = f(c)$	4, function congruence
6.	$M \vDash a = b$	2, $\land$
7.	$M \vDash b = a$	6, symmetry
8.	$M \vDash g(f(a), b) = g(f(c), a)$	5, 7, function congruence
9.	$M \vDash \bot$	3, 8

Decidability results for $T_{=}$

$\boldsymbol{T}_{=}$ is undecidable

Decidability results for $T_=$

$T_=$ is undecidable

Quantifier-free fragment of $T_=$ is (efficiently) decidable

Congruence closure

Theories with natural numbers and integers

Natural numbers $\mathbb{N} = \{0,1,2,\dots\}$

Integers $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$

Peano arithmetic $\boldsymbol{T_{PA}}$: natural numbers with addition and multiplication

Presburger arithmetic $\boldsymbol{T}_{\mathbb{N}}$: natural numbers with addition

Theory of integers $\boldsymbol{T}_{\mathbb{Z}}$: integers with +, - , >

Peano arithmetic T_{PA}

Signature

- $0, 1$ constants
- $+, .$ binary functions
- $=$ binary predicate

$$\Sigma_{\mathrm{PA}} = \{0, 1, +, ., =\}$$

Peano arithmetic T_{PA}

Axioms

- Includes equivalence axioms: reflexivity, symmetry, transitivity
- In addition:

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

Peano arithmetic T_{PA}

Axioms

- Includes equivalence axioms: reflexivity, symmetry, transitivity
- In addition:
  1. $\forall x.\ \neg(x + 1 = 0)$ (zero)
  2. $\forall x.\ x + 0 = x$ (plus zero)
  3. $\forall x.\ x . 0 = 0$ (times zero)
  4. $\forall x, y.\ (x + 1 = y + 1) \longrightarrow x = y$ (successor)
  5. $\forall x, y.\ x + (y + 1) = (x + y) + 1$ (plus successor)
  6. $\forall x, y.\ x . (y + 1) = (x . y) + x$ (times successor)
  7. $(F[0] \wedge (\forall x.\ F[x] \rightarrow F[x + 1])) \rightarrow \forall x.\ F[x]$ (induction) Axiom schema

Can we express $<, \leq, >, \geq$ in T_{PA} ?

$$2x = y+3$$

T_{PA}: $\underline{x+x} = y+1+1+1$

or, $(1+1) \cdot x$

$$2x = y+3$$

$\exists n.\ n \neq 0 \wedge 2x = y+3+n$

Decidability and completeness results for T_{PA}

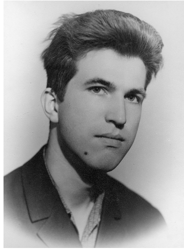
Validity in T_{PA} is undecidable

Decidability and completeness results for T_{PA}

Validity in T_{PA} is undecidable

Validity in quantifier-free fragment of T_{PA} is also undecidable [Matiyasevitch, 1970]

Matiyasevitch



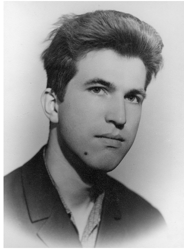
Decidability and completeness results for T_{PA}

Validity in T_{PA} is undecidable

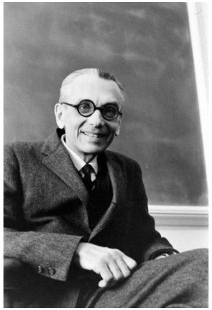
Validity in quantifier-free fragment of T_{PA} is also undecidable [Matiyasevitch, 1970]

T_{PA} does not capture true arithmetic [Gödel]

Matiyasevitch



Gödel



Decidability and completeness results for T_{PA}

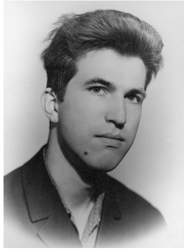
Validity in T_{PA} is undecidable

Validity in quantifier-free fragment of T_{PA} is also undecidable [Matiyasevitch, 1970]

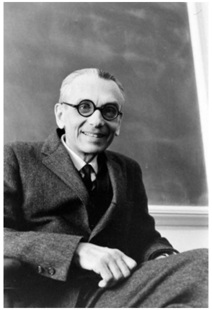
T_{PA} does not capture true arithmetic [Gödel]

$\exists$ valid propositions of number theory that cannot be proven valid in T_{PA}

Matiyasevitch



Gödel



Decidability and completeness results for T_{PA}

Validity in T_{PA} is undecidable

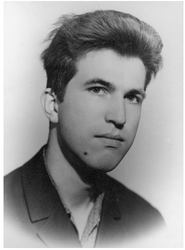
Validity in quantifier-free fragment of T_{PA} is also undecidable [Matiyasevitch, 1970]

T_{PA} does not capture true arithmetic [Gödel]

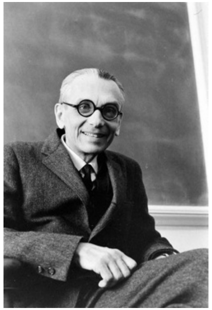
$\exists$ valid propositions of number theory that cannot be proven valid in T_{PA}

Drop multiplication to get decidability and completeness!

Matiyasevitch



Gödel



Presburger arithmetic $T_{\mathbb{N}}$

Signature

- $0, 1$ constants
- $+$ binary function
- $=$ binary predicate

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

Presburger arithmetic $T_{\mathbb{N}}$

Axioms

- Includes equivalence axioms: reflexivity, symmetry, transitivity
- In addition:

1. $\forall x.\ \neg(x + 1 = 0)$ (zero)
2. $\forall x.\ x + 0 = x$ (plus zero)
3. $\forall x, y.\ (x + 1 = y + 1) \longrightarrow x = y$ (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 $T_{\mathbb{N}}$

Validity in quantifier-free fragment of $T_{\mathbb{N}}$ is (efficiently) decidable

Decidability and completeness results for $T_{\mathbb{N}}$

Validity in quantifier-free fragment of $T_{\mathbb{N}}$ is (efficiently) decidable

Validity in $T_{\mathbb{N}}$ is also decidable [Presburger, 1929]

Presburger

Decidability and completeness results for $T_{\mathbb{N}}$

Validity in quantifier-free fragment of $T_{\mathbb{N}}$ is (efficiently) decidable

Validity in $T_{\mathbb{N}}$ is also decidable [Presburger, 1929]

$T_{\mathbb{N}}$ is also complete

Presburger

Decidability and completeness results for $T_{\mathbb{N}}$

$\exists x.\ ax^2 + bx + c = 0 \equiv b^2 - 4ac \geq 0$

Validity in quantifier-free fragment of $T_{\mathbb{N}}$ is (efficiently) decidable

Validity in $T_{\mathbb{N}}$ is also decidable [Presburger, 1929]

$T_{\mathbb{N}}$ is also complete

$T_{\mathbb{N}}$ admits quantifier elimination:
for every formula F, there exists an equivalent quantifier-free formula F'

Presburger

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

$\underbrace{x + x + \ldots + x}_{k}$

Signature

- $\ldots, -2, -1, 0, 1, 2, \ldots$ constants
- $\ldots, -3\,\cdot, -2\,\cdot, 2\,\cdot, 3\,\cdot, \ldots$ unary functions
- $+, -$ binary functions
- $=, >$ binary predicates

kx

shorthand

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

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

Signature

- $\ldots, -2, -1, 0, 1, 2, \ldots$ constants
- $\ldots, -3\,\cdot, -2\,\cdot, 2\,\cdot, 3\,\cdot, \ldots$ unary functions
- $+, -$ binary functions
- $=, >$ binary predicates

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

- Also referred to as the theory of **linear arithmetic over integers**
- Equivalent in expressiveness to Presburger arithemetic
- More convenient notation

LIA

Theory of reals $T_{\mathbb{R}}$

Signature

- $0, 1$ constants
- $+\,,-,\;.$ binary functions
- $=, \geq$ binary predicates

$$\Sigma_{\mathbb{R}} = \{0, 1, \cancel{+, =}, \geq\} \quad \{0, 1, +, -, \cdot, =, \geq\}$$

Too many axioms, won't discuss.

Decidability results for $T_{\mathbb{R}}$

Tarski

Validity in $T_{\mathbb{R}}$ is decidable

Decidability results for $T_{\mathbb{R}}$

Tarski

Validity in $T_{\mathbb{R}}$ is decidable

Validity in quantifier-free fragment of $T_{\mathbb{R}}$ is decidable

Decidability results for $T_{\mathbb{R}}$

Tarski

Validity in $T_{\mathbb{R}}$ is decidable

Validity in quantifier-free fragment of $T_{\mathbb{R}}$ is decidable

$T_{\mathbb{R}}$ admits quantifier elimination:
for every formula F, there exists an equivalent quantifier-free formula F'

Theory of rationals $T_{\mathbb{Q}}$

Signature

- $0, 1$ constants
- $+$ binary function
- $=, \geq$ binary predicates

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

Theory of rationals $T_{\mathbb{Q}}$

Signature

- $0, 1$ constants
- $+$ binary function
- $=, \geq$ binary predicates

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

Can we express $>$ in $T_{\mathbb{Q}}$?

$\forall x, y. \exists z.\ x+y > z$

$\forall x, y. \exists z.$

$x+y \geq z \wedge$

$\neg(x+y = z)$

Theory of rationals $T_{\mathbb{Q}}$

Too many axioms, won't discuss.

Divisibility axiom

For each positive integer n, $\forall x . \exists y . \; x = ny$

Theory of rationals $T_{\mathbb{Q}}$

Too many axioms, won't discuss.

If a formula is valid in $T_{\mathbb{Z}}$, is it valid in $T_{\mathbb{Q}}$?
If a formula is valid in $T_{\mathbb{Q}}$, is it valid in $T_{\mathbb{Z}}$?

$\exists x.\ 2x = 3$

T_Q: $x = \frac{3}{2}$ $\quad T_Z$: ?

??: $\forall x, y.\ x > y \rightarrow x \geq y + 1$

Decidability results for $T_{\mathbb{Q}}$

Validity in $T_{\mathbb{Q}}$ is decidable

Decidability results for $T_{\mathbb{Q}}$

Validity in $T_{\mathbb{Q}}$ is decidable

Validity in conjunctive quantifier-free fragment of $T_{\mathbb{N}}$ is (efficiently) decidable

Theory of arrays T_A

Signature

- $a[i]$ binary function “read(a,i)”
- $a\langle i \triangleleft v\rangle$ ternary function “write(a, i, v)”

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

Theory of arrays T_A

Axioms

- Includes equivalence axioms: reflexivity, symmetry, transitivity
- In addition:

1. $\forall a, i, j.\ (i = j) \rightarrow a[i] = a[j]$ (array congruence)

2. $\forall a, v, i, j.\ (i = j) \rightarrow a\langle i \vartriangleleft v\rangle[j] = v$ (read-over-write 1)

3. $\forall a, v, i, j.\ (i \neq j) \rightarrow a\langle i \vartriangleleft v\rangle[j] = a[j]$ (read-over-write 2)

$a[i] = e \rightarrow a\langle i \triangleleft e \rangle = a$

T_A-valid? No

$T_A^{=}$ Extensionality: $\forall a b. (\forall i. a[i] = b[i]) \leftrightarrow a = b$

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

Decidability results for T_A

Validity in T_A is not decidable

Decidability results for T_A

Validity in T_A is not decidable

Quantifier-free fragment of T_A is decidable

Combination of Theories

Given theories T_1 and T_2 that have the $=$ predicate, define combined theory $T_1 \cup T_2$:

Signature $\Sigma_1 \cup \Sigma_2$

Axioms $A_1 \cup A_2$

$$\underbrace{\underline{1 \leq x} \land x \leq 2} \land f(x) \neq f(1) \land f(x) \neq f(2)$$

$$\left(\frac{T_= \cup T_Q}{T_= \cup T_N} \right)$$

— valid

— not valid

Decision procedures for combined theories

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.
[Nelson and Oppen]

Summary

Today

- Overview of of first-order theories

Next

- SMT solving