

The Calculus of Computation

Zohar Manna
Spring 2009

Chapter 3: First-Order Theories

First-Order Theories I

First-order theory T consists of

- ▶ Signature Σ_T - set of constant, function, and predicate symbols
- ▶ Set of axioms A_T - set of closed (no free variables) Σ_T -formulae

A Σ_T -formula is a formula constructed of constants, functions, and predicate symbols from Σ_T , and variables, logical connectives, and quantifiers.

The symbols of Σ_T are just symbols without prior meaning — the axioms of T provide their meaning.

First-Order Theories II

A Σ_T -formula F is valid in theory T (T -valid, also $T \models F$), iff every interpretation I that satisfies the axioms of T ,
i.e. $I \models A$ for every $A \in A_T$ (T -interpretation)
also satisfies F ,
i.e. $I \models F$

A Σ_T -formula F is satisfiable in T (T -satisfiable), if there is a T -interpretation (i.e. satisfies all the axioms of T) that satisfies F

Two formulae F_1 and F_2 are equivalent in T (T -equivalent), iff $T \models F_1 \leftrightarrow F_2$,
i.e. if for every T -interpretation I , $I \models F_1$ iff $I \models F_2$

Note:

- ▶ $I \models F$ stands for “ F true under interpretation I ”
- ▶ $T \models F$ stands for “ F is valid in theory T ”

Fragments of Theories

A fragment of theory T is a syntactically-restricted subset of formulae of the theory.

Example: a quantifier-free fragment of theory T is the set of quantifier-free formulae in T .

A theory T is decidable if $T \models F$ (T -validity) is decidable for every Σ_T -formula F ;

i.e., there is an algorithm that always terminate with “yes”, if F is T -valid, and “no”, if F is T -invalid.

A fragment of T is decidable if $T \models F$ is decidable for every Σ_T -formula F obeying the syntactic restriction.

Theory of Equality T_E I

Signature:

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

consists of

- ▶ $=$, a binary predicate, interpreted with meaning provided by axioms
- ▶ all constant, function, and predicate symbols

Axioms of T_E

- $\forall x. x = x$ (reflexivity)
- $\forall x, y. x = y \rightarrow y = x$ (symmetry)
- $\forall x, y, z. x = y \wedge y = z \rightarrow x = z$ (transitivity)
- for each positive integer n and n -ary function symbol f ,
 $\forall x_1, \dots, x_n, y_1, \dots, y_n. \bigwedge_i x_i = y_i$
 $\rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$ (function congruence)

Page 5 of 31

Theory of Equality T_E II

- for each positive integer n and n -ary predicate symbol p ,
 $\forall x_1, \dots, x_n, y_1, \dots, y_n. \bigwedge_i x_i = y_i$
 $\rightarrow (p(x_1, \dots, x_n) \leftrightarrow p(y_1, \dots, y_n))$ (predicate congruence)

(function) and (predicate) are axiom schemata.

Example:

(function) for binary function f for $n = 2$:

$$\forall x_1, x_2, y_1, y_2. x_1 = y_1 \wedge x_2 = y_2 \rightarrow f(x_1, x_2) = f(y_1, y_2)$$

(predicate) for unary predicate p for $n = 1$:

$$\forall x, y. x = y \rightarrow (p(x) \leftrightarrow p(y))$$

Note: we omit “congruence” for brevity.

Page 6 of 31

Decidability of T_E I

T_E is undecidable.

The quantifier-free fragment of T_E is decidable. Very efficient algorithm.

Semantic argument method can be used for T_E

Example: Prove

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

is T_E -valid.

Page 7 of 31

Decidability of T_E II

Suppose not; then there exists a T_E -interpretation I such that $I \not\models F$. Then,

- | | |
|--|----------------------|
| 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) |
| 8. $I \models b = a$ | 4, (symmetry) |
| 9. $I \models g(f(a), b) = g(f(c), a)$ | 7, 8, (function) |
| 10. $I \models \perp$ | 3, 9 contradictory |

F is T_E -valid.

Page 8 of 31

Natural Numbers and Integers

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

Three variations:

- ▶ Peano arithmetic T_{PA} : natural numbers with addition, multiplication, =
- ▶ Presburger arithmetic $T_{\mathbb{N}}$: natural numbers with addition, =
- ▶ Theory of integers $T_{\mathbb{Z}}$: integers with +, -, >, =, multiplication by constants

1. Peano Arithmetic T_{PA} (first-order arithmetic)

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

Equality Axioms: (reflexivity), (symmetry), (transitivity), (function) for +, (function) for \cdot .

And the axioms:

- $\forall x. \neg(x + 1 = 0)$ (zero)
- $\forall x, y. x + 1 = y + 1 \rightarrow x = y$ (successor)
- $F[0] \wedge (\forall x. F[x] \rightarrow F[x + 1]) \rightarrow \forall x. F[x]$ (induction)
- $\forall x. x + 0 = x$ (plus zero)
- $\forall x, y. x + (y + 1) = (x + y) + 1$ (plus successor)
- $\forall x. x \cdot 0 = 0$ (times zero)
- $\forall x, y. x \cdot (y + 1) = x \cdot y + x$ (times successor)

Line 3 is an axiom schema.

Example: $3x + 5 = 2y$ can be written using Σ_{PA} as

$$x + x + x + 1 + 1 + 1 + 1 + 1 = y + y$$

Note: we have $>$ and \geq since

$$3x + 5 > 2y \quad \text{write as} \quad \exists z. z \neq 0 \wedge 3x + 5 = 2y + z$$

$$3x + 5 \geq 2y \quad \text{write as} \quad \exists z. 3x + 5 = 2y + z$$

Example:

Existence of pythagorean triples (F is T_{PA} -valid):

$$F : \exists x, y, z. x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge x \cdot x + y \cdot y = z \cdot z$$

Decidability of Peano Arithmetic

T_{PA} is undecidable. (Gödel, Turing, Post, Church)

The quantifier-free fragment of T_{PA} is undecidable. (Matiyasevich, 1970)

Remark: Gödel's first incompleteness theorem

Peano arithmetic T_{PA} does not capture true arithmetic:

There exist closed Σ_{PA} -formulae representing valid propositions of number theory that are not T_{PA} -valid.

The reason: T_{PA} actually admits *nonstandard interpretations*.

For decidability: no multiplication

2. Presburger Arithmetic T_N

Signature $\Sigma_N : \{0, 1, +, =\}$ no multiplication!

Axioms of T_N (equality axioms, with 1-5):

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

Line 3 is an axiom schema.

T_N -satisfiability (and thus T_N -validity) is decidable
(Presburger, 1929)

3. Theory of Integers T_Z

Signature:

$\Sigma_Z : \{\dots, -2, -1, 0, 1, 2, \dots, -3, -2, 2, 3, \dots, +, -, >, =\}$

where

- $\dots, -2, -1, 0, 1, 2, \dots$ are constants
- $\dots, -3, -2, 2, 3, \dots$ are unary functions
(intended meaning: $2 \cdot x$ is $x + x$, $-3 \cdot x$ is $-x - x - x$)
- $+, -, >, =$ have the usual meanings.

Relation between T_Z and T_N :

T_Z and T_N have the same expressiveness:

- For every Σ_Z -formula there is an equisatisfiable Σ_N -formula.
- For every Σ_N -formula there is an equisatisfiable Σ_Z -formula.

Σ_Z -formula F and Σ_N -formula G are *equisatisfiable* iff:

F is T_Z -satisfiable iff G is T_N -satisfiable

Σ_Z -formula to Σ_N -formula I

Example: consider the Σ_Z -formula

$$F_0 : \forall w, x. \exists y, z. x + 2y - z - 7 > -3w + 4.$$

Introduce two variables, v_p and v_n (range over the nonnegative integers) for each variable v (range over the integers) of F_0 :

$$F_1 : \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \\ (x_p - x_n) + 2(y_p - y_n) - (z_p - z_n) - 7 > -3(w_p - w_n) + 4$$

Eliminate $-$ by moving to the other side of $>$:

$$F_2 : \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \\ x_p + 2y_p + z_n + 3w_p > x_n + 2y_n + z_p + 7 + 3w_n + 4$$

Σ_Z -formula to Σ_N -formula II

Eliminate $>$ and numbers:

$$\forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \exists u. \\ \neg(u = 0) \wedge x_p + y_p + y_p + z_n + w_p + w_p + w_p \\ = x_n + y_n + y_n + z_p + w_n + w_n + w_n + u \\ + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$$

which is a Σ_N -formula equisatisfiable to F_0 .

To decide T_Z -validity for a Σ_Z -formula F :

- transform $\neg F$ to an equisatisfiable Σ_N -formula $\neg G$,
- decide T_N -validity of G .

Example: The $\Sigma_{\mathbb{N}}$ -formula

$$\forall x. \exists y. x = y + 1$$

is equisatisfiable to the $\Sigma_{\mathbb{Z}}$ -formula:

$$\forall x. x > -1 \rightarrow \exists y. y > -1 \wedge x = y + 1.$$

1. Theory of Reals $T_{\mathbb{R}}$

Signature:

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

with multiplication. Axioms in text.

Example:

$$\forall a, b, c. b^2 - 4ac \geq 0 \leftrightarrow \exists x. ax^2 + bx + c = 0$$

is $T_{\mathbb{R}}$ -valid.

$T_{\mathbb{R}}$ is decidable (Tarski, 1930)
High time complexity

Signatures:

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

$$\Sigma_{\mathbb{R}} = \Sigma_{\mathbb{Q}} \cup \{\cdot\}$$

► Theory of Reals $T_{\mathbb{R}}$ (with multiplication)

$$x \cdot x = 2 \Rightarrow x = \pm\sqrt{2}$$

► Theory of Rationals $T_{\mathbb{Q}}$ (no multiplication)

$$\underbrace{2x}_{x+x} = 7 \Rightarrow x = \frac{7}{2}$$

Note: strict inequality okay; simply rewrite

$$x + y > z$$

as follows:

$$\neg(x + y = z) \wedge x + y \geq z$$

2. Theory of Rationals $T_{\mathbb{Q}}$

Signature:

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

without multiplication. Axioms in text.

Rational coefficients are simple to express in $T_{\mathbb{Q}}$.

Example: Rewrite

$$\frac{1}{2}x + \frac{2}{3}y \geq 4$$

as the $\Sigma_{\mathbb{Q}}$ -formula

$$3x + 4y \geq 24$$

$T_{\mathbb{Q}}$ is decidable
Quantifier-free fragment of $T_{\mathbb{Q}}$ is efficiently decidable

Recursive Data Structures (RDS) I

Tuples of variables where the elements can be instances of the same structure: e.g., linked lists or trees.

1. Theory T_{cons} (LISP-like lists)

Signature:

$$\Sigma_{\text{cons}} : \{\text{cons}, \text{car}, \text{cdr}, \text{atom}, =\}$$

where

$\text{cons}(a, b)$ – list constructed by concatenating a and b
 $\text{car}(x)$ – left projector of x : $\text{car}(\text{cons}(a, b)) = a$
 $\text{cdr}(x)$ – right projector of x : $\text{cdr}(\text{cons}(a, b)) = b$
 $\text{atom}(x)$ – true iff x is a single-element list

Note: an atom is simply something that is not a cons. In this formulation, there is no NIL value.

3. Predicate Congruence axiom

$$\forall x, y. x = y \rightarrow (\text{atom}(x) \leftrightarrow \text{atom}(y))$$

- $\forall x, y. \text{car}(\text{cons}(x, y)) = x$ (left projection)
- $\forall x, y. \text{cdr}(\text{cons}(x, y)) = y$ (right projection)
- $\forall x. \neg \text{atom}(x) \rightarrow \text{cons}(\text{car}(x), \text{cdr}(x)) = x$ (construction)
- $\forall x, y. \neg \text{atom}(\text{cons}(x, y))$ (atom)

Note: the behavior of car and cons on atoms is not specified.

T_{cons} is undecidable
Quantifier-free fragment of T_{cons} is efficiently decidable

Recursive Data Structures (RDS) II

Axioms:

- The axioms of reflexivity, symmetry, and transitivity of =
- Function Congruence axioms

$$\forall x_1, x_2, y_1, y_2. x_1 = x_2 \wedge y_1 = y_2 \rightarrow \text{cons}(x_1, y_1) = \text{cons}(x_2, y_2)$$

$$\forall x, y. x = y \rightarrow \text{car}(x) = \text{car}(y)$$

$$\forall x, y. x = y \rightarrow \text{cdr}(x) = \text{cdr}(y)$$

Lists with equality

2. Theory T_{cons}^E (lists with equality)

$$T_{\text{cons}}^E = T_E \cup T_{\text{cons}}$$

Signature:

$$\Sigma_E \cup \Sigma_{\text{cons}}$$

(this includes uninterpreted constants, functions, and predicates)

Axioms: union of the axioms of T_E and T_{cons}

T_{cons}^E is undecidable
Quantifier-free fragment of T_{cons}^E is efficiently decidable

Example: The Σ_{cons}^E -formula

$$F : \text{car}(x) = \text{car}(y) \wedge \text{cdr}(x) = \text{cdr}(y) \wedge \neg \text{atom}(x) \wedge \neg \text{atom}(y) \\ \rightarrow f(x) = f(y)$$

is T_{cons}^E -valid.

Suppose not; then there exists a T_{cons}^E -interpretation I such that $I \not\models F$. Then,

1. $I \not\models F$ assumption
2. $I \models \text{car}(x) = \text{car}(y)$ 1, \rightarrow, \wedge
3. $I \models \text{cdr}(x) = \text{cdr}(y)$ 1, \rightarrow, \wedge
4. $I \models \neg \text{atom}(x)$ 1, \rightarrow, \wedge
5. $I \models \neg \text{atom}(y)$ 1, \rightarrow, \wedge
6. $I \not\models f(x) = f(y)$ 1, \rightarrow
7. $I \models \text{cons}(\text{car}(x), \text{cdr}(x)) = \text{cons}(\text{car}(y), \text{cdr}(y))$
2, 3, (function)
8. $I \models \text{cons}(\text{car}(x), \text{cdr}(x)) = x$ 4, (construction)
9. $I \models \text{cons}(\text{car}(y), \text{cdr}(y)) = y$ 5, (construction)
10. $I \models x = y$ 7, 8, 9, (transitivity)
11. $I \models f(x) = f(y)$ 10, (function)

Lines 6 and 11 are contradictory, so our assumption that $I \not\models F$ must be wrong. Therefore, F is T_{cons}^E -valid. Page 25 of 31

Note: = is only defined for array elements

$$F : a[i] = e \rightarrow a(i \triangleleft e) = a$$

not T_A -valid, but

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

is T_A -valid.

Also

$$a = b \rightarrow a[i] = b[i]$$

is not T_A -valid: We have only axiomatized a restricted congruence.

T_A is undecidable
Quantifier-free fragment of T_A is decidable

Theory of Arrays T_A

Signature:

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

where

- ▶ $a[i]$ binary function – read array a at index i (“read(a, i)”)
- ▶ $a(i \triangleleft v)$ ternary function – write value v to index i of array a (“write(a, i, v)”)

Axioms

1. the axioms of (reflexivity), (symmetry), and (transitivity) of T_E
2. $\forall a, i, j. i = j \rightarrow a[i] = a[j]$ (array congruence)
3. $\forall a, v, i, j. i = j \rightarrow a(i \triangleleft v)[j] = v$ (read-over-write 1)
4. $\forall a, v, i, j. i \neq j \rightarrow a(i \triangleleft v)[j] = a[j]$ (read-over-write 2)

2. Theory of Arrays T_A^- (with extensionality)

Signature and axioms of T_A^- are the same as T_A , with one additional axiom

$$\forall a, b. (\forall i. a[i] = b[i]) \leftrightarrow a = b \quad (\text{extensionality})$$

Example:

$$F : a[i] = e \rightarrow a(i \triangleleft e) = a$$

is T_A^- -valid.

T_A^- is undecidable
Quantifier-free fragment of T_A^- is decidable

Theory	Quantifiers	
	Decidable	QFF
T_E Equality	–	✓
T_{PA} Peano Arithmetic	–	–
T_N Presburger Arithmetic	✓	✓
T_Z Linear Integer Arithmetic	✓	✓
T_R Real Arithmetic	✓	✓
T_Q Linear Rationals	✓	✓
T_{cons} Lists	–	✓
T_{cons}^E Lists with Equality	–	✓

How do we show that

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

is $(T_E \cup T_Z)$ -valid?

Or how do we prove properties about
an array of integers, or
a list of reals ... ?

Given theories T_1 and T_2 such that

$$\Sigma_1 \cap \Sigma_2 = \{=\}$$

The combined theory $T_1 \cup T_2$ has

- ▶ signature $\Sigma_1 \cup \Sigma_2$
- ▶ axioms $A_1 \cup A_2$

Nelson & Oppen showed that,
if

- ▶ validity of the quantifier-free fragment (qff) of T_1 is decidable,
- ▶ validity of qff of T_2 is decidable, and
- ▶ certain technical simple requirements are met,

then validity of qff of $T_1 \cup T_2$ is decidable.