

Examples of First Order Theories

*Edited slides from the original
slides from CS156 by Prof. Z.Manna*

CS156: The Calculus of Computation

Zohar Manna
Autumn 2008

Chapter 3: First-Order Theories

First-Order Theories

	Theory	Quantifiers Decidable	QFF Decidable
T_E	Equality	—	✓
T_{PA}	Peano Arithmetic	—	—
$T_{\mathbb{N}}$	Presburger Arithmetic	✓	✓
$T_{\mathbb{Z}}$	Linear Integer Arithmetic	✓	✓
$T_{\mathbb{R}}$	Real Arithmetic	✓	✓
$T_{\mathbb{Q}}$	Linear Rationals	✓	✓
T_{cons}	Lists	—	✓
T_{cons}^E	Lists with Equality	—	✓

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

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 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)

Theory of Equality T_E II

5. for each positive integer n and n -ary predicate symbol p ,

$$\forall x_1, \dots, x_n, y_1, \dots, y_n. \bigwedge_i x_i = y_i$$

$$\rightarrow (p(x_1, \dots, x_n) \leftrightarrow p(y_1, \dots, y_n)) \text{ (predicate congruence)}$$

(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.

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.

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.

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:

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)
6. $\forall x. x \cdot 0 = 0$ (times zero)
7. $\forall x, y. x \cdot (y + 1) = x \cdot y + x$ (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):

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

2. Presburger Arithmetic $T_{\mathbb{N}}$

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

no multiplication!

Axioms of $T_{\mathbb{N}}$ (equality axioms, with 1-5):

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)

Line 3 is an axiom schema.

$T_{\mathbb{N}}$ -satisfiability (and thus $T_{\mathbb{N}}$ -validity) is decidable
(Presburger, 1929)

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

Signature:

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

where

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

Relation between $T_{\mathbb{Z}}$ and $T_{\mathbb{N}}$:

$T_{\mathbb{Z}}$ and $T_{\mathbb{N}}$ have the same expressiveness:

- ▶ For every $\Sigma_{\mathbb{Z}}$ -formula there is an equisatisfiable $\Sigma_{\mathbb{N}}$ -formula.
- ▶ For every $\Sigma_{\mathbb{N}}$ -formula there is an equisatisfiable $\Sigma_{\mathbb{Z}}$ -formula.

$\Sigma_{\mathbb{Z}}$ -formula F and $\Sigma_{\mathbb{N}}$ -formula G are *equisatisfiable* iff:

$$F \text{ is } T_{\mathbb{Z}}\text{-satisfiable} \quad \text{iff} \quad G \text{ is } T_{\mathbb{N}}\text{-satisfiable}$$

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
--

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

Theory of Arrays T_A

Signature:

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

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

Note: $=$ is only defined for array elements

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

not T_A -valid, but

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

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

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:

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

is $T_A^=$ -valid.

$T_A^=$ is undecidable

Quantifier-free fragment of $T_A^=$ is decidable