

### 3. First-Order Theories

# First-Order Theories

First-order theory  $T$  defined by

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

$\Sigma$ -formula constructed of constants, functions, and predicate symbols from  $\Sigma$ , and variables, logical connectives, and quantifiers

The symbols of  $\Sigma$  are just symbols without prior meaning — the axioms of  $T$  provide their meaning

A  $\Sigma$ -formula  $F$  is valid in theory  $T$  ( $T$ -valid, also  $T \models F$ ), if 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  $\Sigma$ -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), if  $T \models F_1 \leftrightarrow F_2$ ,

i.e. if for every  $T$ -interpretation  $I$ ,  $I \models F_1$  iff  $I \models F_2$

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

Example: quantifier-free segment 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  $\Sigma$ -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  $\Sigma$ -formula  $F$  in the fragment.

# Theory of Equality $T_E$

## Signature

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

consists of

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

Congruence and Equivalence are axiom schemata. For example,

Congruence for binary function  $f_2$  for  $n = 2$ :

$$\forall x_1, x_2, y_1, y_2. x_1 = y_1 \wedge x_2 = y_2 \rightarrow f_2(x_1, x_2) = f_2(y_1, y_2)$$

$T_E$  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

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

Suppose not; then there exists a  $T_=$ -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, (congruence)                |
| 8. | $I \models g(f(a), b) = g(f(c), a)$     | 4, 7, (congruence), (symmetry) |

3 and 8 are contradictory  $\Rightarrow F$  is  $T_=$ -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 and multiplication
- ▶ Presburger arithmetic  $T_{\mathbb{N}}$ : natural numbers with addition
- ▶ Theory of integers  $T_{\mathbb{Z}}$ : integers with  $+$ ,  $-$ ,  $>$

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

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

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  $\Sigma_{PA}$  as

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

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:

- ▶ Pythagorean Theorem is  $T_{PA}$ -valid

$$\exists x, y, z. x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge xx + yy = zz$$

- ▶ Fermat's Last Theorem is  $T_{PA}$ -invalid (Andrew Wiles, 1994)

$$\exists n. n > 2 \rightarrow \exists x, y, z. x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge x^n + y^n = z^n$$

Remark (Gödel's first incompleteness theorem)

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

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

The reason:  $T_{PA}$  actually admits nonstandard interpretations

Satisfiability and validity in  $T_{PA}$  is undecidable.

Restricted theory – no multiplication



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

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

where

- ▶  $\dots, -2, -1, 0, 1, 2, \dots$  are constants
- ▶  $\dots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \dots$  are unary functions  
(intended  $2 \cdot x$  is  $2x$ )
- ▶  $+, -, =, >$

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

- Every  $T_{\mathbb{Z}}$ -formula can be reduced to  $\Sigma_{\mathbb{N}}$ -formula.

Example: Consider the  $T_{\mathbb{Z}}$ -formula

$$F_0 : \forall w, x. \exists y, z. x + 2y - z - 13 > -3w + 5$$

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

$$F_1 : \quad \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \\ (x_p - x_n) + 2(y_p - y_n) - (z_p - z_n) - 13 > -3(w_p - w_n) + 5$$

Eliminate – by moving to the other side of >

$$F_2 : \quad \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \\ x_p + 2y_p + z_n + 3w_p > x_n + 2y_n + z_p + 13 + 3w_n + 5$$

Eliminate >

$$F_3 : \quad \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \exists u. \\ \neg(u = 0) \wedge \\ x_p + y_p + y_p + z_n + w_p + w_p + w_p \\ = x_n + y_n + y_n + z_p + w_n + w_n + w_n + u \\ +1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \\ +1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 .$$

which is a  $T_{\mathbb{N}}$ -formula equivalent to  $F_0$ .

- Every  $T_{\mathbb{N}}$ -formula can be reduced to  $\Sigma_{\mathbb{Z}}$ -formula.

Example: To decide the  $T_{\mathbb{N}}$ -validity of the  $T_{\mathbb{N}}$ -formula

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

decide the  $T_{\mathbb{Z}}$ -validity of the  $T_{\mathbb{Z}}$ -formula

$$\forall x. x \geq 0 \rightarrow \exists y. y \geq 0 \wedge x = y + 1 ,$$

where  $t_1 \geq t_2$  expands to  $t_1 = t_2 \vee t_1 > t_2$

$T_{\mathbb{Z}}$ -satisfiability and  $T_{\mathbb{N}}$ -validity is decidable

# Rationals and Reals

$$\Sigma = \{0, 1, +, -, =, \geq\}$$

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

$$x^2 = 2 \quad \Rightarrow \quad x = \pm\sqrt{2}$$

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

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

Note: Strict inequality OK

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

rewrite as

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

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

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

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 $T_{\mathbb{Q}}$

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

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)

## 1. RDS theory of LISP-like lists, $T_{\text{cons}}$

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

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

Axioms:

1. The axioms of reflexivity, symmetry, and transitivity of  $=$
2. Congruence axioms

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

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

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

### 3. Equivalence axiom

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

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

$T_{\text{cons}}$  is undecidable

Quantifier-free fragment of  $T_{\text{cons}}$  is efficiently decidable

## 2. Lists + equality

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

Signature:  $\Sigma_= \cup \Sigma_{\text{cons}}$

(this includes uninterpreted constants, functions, and predicates)

Axioms: union of the axioms of  $T_=$  and  $T_{\text{cons}}$

$T_{\text{cons}}^=$  is undecidable

Quantifier-free fragment of  $T_{\text{cons}}^=$  is efficiently decidable

Example: We argue that the  $\Sigma_{\text{cons}}^=$ -formula

$$F : \begin{array}{l} \text{car}(a) = \text{car}(b) \wedge \text{cdr}(a) = \text{cdr}(b) \wedge \neg \text{atom}(a) \wedge \neg \text{atom}(b) \\ \rightarrow f(a) = f(b) \end{array}$$

is  $T_{\text{cons}}^=$ -valid.

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

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

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

# Theory of Arrays

## 1. 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( $a, i$ )”)
- ▶  $a\langle i \rangle v$  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  $T_ =$
2.  $\forall a, i, j. i = j \rightarrow a[i] = a[j]$  (array congruence)
3.  $\forall a, v, i, j. i = j \rightarrow a\langle i \rangle v[j] = v$  (read-over-write 1)
4.  $\forall a, v, i, j. i \neq j \rightarrow a\langle i \rangle v[j] = a[j]$  (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.

$T_A$  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

# Combination of Theories

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  $(T_{=} \cup T_{\mathbb{Z}})$ -unsatisfiable?

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  $A_1 \cup A_2$

qff = quantifier-free fragment

Nelson & Oppen showed that

if satisfiability of qff of  $T_1$  is decidable,  
satisfiability of qff of  $T_2$  is decidable, and  
certain technical simple requirements are met  
then satisfiability of qff of  $T_1 \cup T_2$  is decidable.