CS156: The Calculus of Computation

Zohar Manna

Autumn 2008

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:

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

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

Theory of Equality T_E II

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

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

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

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

Three variations:

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

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

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

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):

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

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 $T_{\mathbb{N}}$

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

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

where

- $\ldots, -2, -1, 0,\ 1,\ 2,\ \ldots$ are constants
- $\ldots, -3\cdot, -2\cdot, 2\cdot,\ 3\cdot,\ \ldots$ 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:

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

$\Sigma_{\mathbb{Z}}$-formula to $\Sigma_{\mathbb{N}}$-formula I

Example: consider the $\Sigma_{\mathbb{Z}}$-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:

$$F_1 : \quad \begin{array}{l} \forall w_p, w_n, x_p, x_n.\ \exists y_p, y_n, z_p, z_n. \\ \quad (x_p - x_n) + 2(y_p - y_n) - (z_p - z_n) - 7 > -3(w_p - w_n) + 4 \end{array}$$

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

$$F_2 : \quad \begin{array}{l} \forall w_p, w_n, x_p, x_n.\ \exists y_p, y_n, z_p, z_n. \\ \quad x_p + 2y_p + z_n + 3w_p > x_n + 2y_n + z_p + 7 + 3w_n + 4 \end{array}$$

$\Sigma_{\mathbb{Z}}$-formula to $\Sigma_{\mathbb{N}}$-formula II

Eliminate $>$ and numbers:

$$F_3: \quad \begin{array}{l} \forall w_p, w_n, x_p, x_n.\ \exists y_p, y_n, z_p, z_n.\ \exists u. \\ \quad \neg(u = 0) \ \wedge \ x_p + y_p + y_p + z_n + w_p + w_p + w_p \\ \qquad\qquad\qquad = x_n + y_n + y_n + z_p + w_n + w_n + w_n + u \\ \qquad\qquad\qquad\quad + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \end{array}$$

which is a $\Sigma_{\mathbb{N}}$-formula equisatisfiable to F_0.

To decide $T_{\mathbb{Z}}$-validity for a $\Sigma_{\mathbb{Z}}$-formula F:

- transform $\neg F$ to an equisatisfiable $\Sigma_{\mathbb{N}}$-formula $\neg G$,
- decide $T_{\mathbb{N}}$-validity of G.

$\Sigma_{\mathbb{Z}}$-formula to $\Sigma_{\mathbb{N}}$-formula III

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

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

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

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

Rationals and Reals

Signatures:

$$\begin{aligned} \Sigma_{\mathbb{Q}} &= \{0,\ 1,\ +,\ -,\ =,\ \geq\} \\ \Sigma_{\mathbb{R}} &= \Sigma_{\mathbb{Q}} \cup \{\cdot\} \end{aligned}$$

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

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

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

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

Note: strict inequality okay; simply rewrite

$$x + y > z$$

as follows:

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

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

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:

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

where

cons(a, b)– list constructed by concatenating a and b
car(x) – left projector of x: $\mathrm{car}(\mathrm{cons}(a, b)) = a$
cdr(x) – right projector of x: $\mathrm{cdr}(\mathrm{cons}(a, b)) = b$
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.

Recursive Data Structures (RDS) II

Axioms:

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

$$\forall x_1, x_2, y_1, y_2.\ x_1 = x_2 \wedge y_1 = y_2 \ \rightarrow\ \mathrm{cons}(x_1, y_1) = \mathrm{cons}(x_2, y_2)$$
$$\forall x, y.\ x = y \ \rightarrow\ \mathrm{car}(x) = \mathrm{car}(y)$$
$$\forall x, y.\ x = y \ \rightarrow\ \mathrm{cdr}(x) = \mathrm{cdr}(y)$$

3. Predicate Congruence axiom

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

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

Lists with equality

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

$$T_{\text{cons}}^{E} \quad = \quad T_{\mathrm{E}} \ \cup \ T_{\text{cons}}$$

Signature:

$$\Sigma_{\mathrm{E}} \ \cup \ \Sigma_{\text{cons}}$$

(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

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

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.

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)")

<u>Axioms</u>

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

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	–	✓

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 $(T_{\mathsf{E}} \ \cup \ T_{\mathbb{Z}})$-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

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

The <u>combined theory</u> $T_1 \ \cup \ T_2$ 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.