Decision Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Winter Term 2019/2020

Theories

Theories

In first-order logic function symbols have no predefined meaning:

The formula $1 + 1 = 3$ is satisfiable.

We want to fix the meaning for some function symbols.
Examples:

- Equality theory
- Theory of natural numbers
- Theory of rational numbers
- Theory of arrays or lists

First-Order Theories

Definition (First-order theory)

A First-order theory T consists of

- A Signature Σ - set of constant, function, and predicate symbols
- A set of axioms A_T - set of closed (no free variables) Σ-formulae

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

- The symbols of Σ are just symbols without prior meaning
- The axioms of T provide their meaning

Theory of Equality T_E

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

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

Axiom Schemata

Congruence and Equivalence are axiom schemata.

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

For every function symbol there is an instance of the congruence axiom schemata.

Example: Congruence axiom for binary function f_2:
$\forall x_1, x_2, y_1, y_2.\ x_1 = y_1 \land x_2 = y_2 \rightarrow f_2(x_1, x_2) = f_2(y_1, y_2)$

A_{T_E} contains an infinite number of these axioms.

T-Validity and T-Satisfiability

Definition (T-interpretation)

An interpretation I is a T-interpretation, if it satisfies all the axioms of T.

Definition (T-valid)

A Σ-formula F is valid in theory T (T-valid, also $T \models F$),
if every T-interpretation satisfies F.

Definition (T-satisfiable)

A Σ-formula F is satisfiable in T (T-satisfiable),
if there is a T-interpretation that satisfies F

Definition (T-equivalent)

Two Σ-formulae F_1 and F_2 are equivalent in T (T-equivalent),
if $F_1 \leftrightarrow F_2$ is T-valid,

Example: T_E-validity

Semantic argument method can be used for T_E

Prove

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

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.	$I \models \forall x, y, z.\ x = y \wedge y = z \rightarrow x = z$	transitivity
5.	$I \models a = b \wedge b = c \rightarrow a = c$	4, 3 $\times\ \forall\{x \mapsto a, y \mapsto b, z \mapsto c\}$
6a	$I \not\models a = b \wedge b = c$	5, $\rightarrow$
7a	$I \models \bot$	2 and 6a contradictory
6b.	$I \models a = c$	4, 5, (5, $\rightarrow$)
7b.	$I \models a = c \rightarrow f(a) = f(c)$	(congruence), 2 $\times\ \forall$
8ba.	$I \not\models a = c \quad \cdots I \models \bot$	
8bb.	$I \models f(a) = f(c)$	7b, $\rightarrow$
9bb.	$I \models a = b$	2, $\wedge$
10bb.	$I \models a = b \rightarrow b = a$	(symmetry), 2 $\times\ \forall$
11bba.	$I \not\models a = b \quad \cdots I \models \bot$	
11bbb.	$I \models b = a$	10bb, $\rightarrow$
12bbb.	$I \models f(a) = f(c) \wedge b = a \rightarrow g(f(a), b) = g(f(c), a)$	(congruence), 4 $\times\ \forall$
...13	$I \models g(f(a), b) = g(f(c), a)$	8bb, 11bbb, 12bbb

3 and 13 are contradictory. Thus, F is T_E-valid.

Decidability of T_E

Is it possible to decide T_E-validity?

T_E-validity is undecidable.

If we restrict ourself to quantifier-free formulae we get decidability:

For a quantifier-free formula T_E-validity is decidable.

Fragments of Theories

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

Example: 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-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-formula F in the fragment.

Natural Numbers and Integers

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

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 $+, -, >$

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

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

Axioms of T_{PA}: axioms of T_E,

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.

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

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

We can define $>$ and $\geq$: $3x + 5 > 2y$ write as $\exists z.\ z \neq 0 \land 3x + 5 = 2y + z$

$3x + 5 \geq 2y$ write as $\exists z.\ 3x + 5 = 2y + z$

Examples for valid formulae:

- Pythagorean Theorem is T_{PA}-valid
  $$\exists x, y, z.\ x \neq 0 \land y \neq 0 \land z \neq 0 \land xx + yy = zz$$
- Fermat's Last Theorem is T_{PA}-valid (Andrew Wiles, 1994)
  $$\forall n.\ n > 2 \rightarrow \neg \exists x, y, z.\ x \neq 0 \land y \neq 0 \land z \neq 0 \land x^n + y^n = z^n$$

In Fermat's theorem we used x^n, which is not a valid term in Σ_{PA}.
However, there is the Σ_{PA}-formula $EXP[x, n, r]$ with

1. $EXP[x, 0, r] \leftrightarrow r = 1$
2. $EXP[x, i+1, r] \leftrightarrow \exists r_1.\ EXP[x, i, r_1] \land r = r_1 \cdot x$

$$
\begin{aligned}
EXP[x, n, r] :\ & \exists d, m.\ (\exists z.\ d = (m+1)z + 1) \land \\
& (\forall i, r_1.\ i < n \land r_1 < m \land (\exists z.\ d = ((i+1)m+1)z + r_1) \to \\
& \qquad r_1 x < m \land (\exists z.\ d = ((i+2)m+1)z + r_1 \cdot x)) \land \\
& r < m \land (\exists z.\ d = ((n+1)m+1)z + r)
\end{aligned}
$$

Fermat's theorem can be stated as:

$$
\begin{aligned}
\forall n.\ n > 2 \to \neg\exists x, y, z, rx, ry.\ x \neq 0 \land y \neq 0 \land z \neq 0 \land \\
EXP[x, n, rx] \land EXP[y, n, ry] \land EXP[z, n, rx + ry]
\end{aligned}
$$

Decidability of Peano Arithmetic

Gödel showed that for every recursive function $f : \mathbb{N}^n \to \mathbb{N}$ there is a Σ_{PA}-formula $F[x_1, \ldots, x_n, r]$ with

$$F[x_1, \ldots, x_n, r] \leftrightarrow r = f(x_1, \ldots, x_n)$$

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

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

Signature: $\Sigma_{\mathbb{N}}$: $\{0,\ 1,\ +,\ =\}$ no multiplication!

Axioms of $T_{\mathbb{N}}$: axioms of T_E,

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)

3 is an axiom schema.

$T_{\mathbb{N}}$-satisfiability and $T_{\mathbb{N}}$-validity are decidable. (Presburger 1929)

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 $x + x$)
- $+, -, =, >$ 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:

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

Example: $\Sigma_{\mathbb{N}}$-formula to $\Sigma_{\mathbb{Z}}$-formula.

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

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

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

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

Example: $\Sigma_{\mathbb{Z}}$-formula to $\Sigma_{\mathbb{N}}$-formula

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

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

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

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

Eliminate $>$ and numbers:

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

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

Reducing $T_{\mathbb{Z}}$ to $T_{\mathbb{N}}$.

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.

Rationals and Reals

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

- 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

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

can be expressed as

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

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

UNI FREIBURG

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

Axioms of $T_{\mathbb{R}}$: axioms of T_E,

1. $\forall x, y, z.\ (x + y) + z = x + (y + z)$ (+ associativity)
2. $\forall x, y.\ x + y = y + x$ (+ commutativity)
3. $\forall x.\ x + 0 = x$ (+ identity)
4. $\forall x.\ x + (-x) = 0$ (+ inverse)
5. $\forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (· associativity)
6. $\forall x, y.\ x \cdot y = y \cdot x$ (· commutativity)
7. $\forall x.\ x \cdot 1 = x$ (· identity)
8. $\forall x.\ x \neq 0 \rightarrow \exists y.\ x \cdot y = 1$ (· inverse)
9. $\forall x, y, z.\ x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivity)
10. $0 \neq 1$ (separate identies)
11. $\forall x, y.\ x \geq y \land y \geq x \rightarrow x = y$ (antisymmetry)
12. $\forall x, y, z.\ x \geq y \land y \geq z \rightarrow x \geq z$ (transitivity)
13. $\forall x, y.\ x \geq y \lor y \geq x$ (totality)
14. $\forall x, y, z.\ x \geq y \rightarrow x + z \geq y + z$ (+ ordered)
15. $\forall x, y.\ x \geq 0 \land y \geq 0 \rightarrow x \cdot y \geq 0$ (· ordered)
16. $\forall x.\ \exists y.\ x = y \cdot y \lor x = -y \cdot y$ (square root)
17. for each odd integer n,
    $\forall x_0, \ldots, x_{n-1}.\ \exists y.\ y^n + x_{n-1} y^{n-1} \cdots + x_1 y + x_0 = 0$ (at least one root)

Example

F: $\forall x.\ x \cdot 0 = 0$ is $T_{\mathbb{R}}$-valid.

1.	$I \not\models \forall x.\ x \cdot 0 = 0$	assumption
2.	$I \not\models a \cdot 0 = 0$	$\forall$, a fresh
3.	$I \models a = a$	reflexivity, $\{x \mapsto a\}$
4.	$I \models (0 + 0) = 0$	$+$-identity $\{x \mapsto 0\}$
5.	$I \models a \cdot (0 + 0) = a \cdot 0$	3,4,congruence
6.	$I \models a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$	distributivity
7.	$I \models a \cdot 0 + a \cdot 0 = a \cdot (0 + 0)$	6,symmetry
8.	$I \models a \cdot 0 + a \cdot 0 = a \cdot 0$	7,5,transitivity
9.	$I \models (a \cdot 0 + a \cdot 0) + -(a \cdot 0) = a \cdot 0 + -(a \cdot 0)$	8,congruence
10.	$I \models a \cdot 0 + -(a \cdot 0) = 0$	$+$-inverse
11.	$I \models (a \cdot 0 + a \cdot 0) + -(a \cdot 0) = a \cdot 0 + (a \cdot 0 + -(a \cdot 0))$	$+$-associativity
12.	$I \models a \cdot 0 + (a \cdot 0 + -(a \cdot 0)) = a \cdot 0 + 0$	10, congruence
13.	$I \models a \cdot 0 + 0 = a \cdot 0$	$+$-identity
14.	$I \models (a \cdot 0 + a \cdot 0) + -(a \cdot 0) = a \cdot 0$	11,12,13,transitivity
15.	$I \models a \cdot 0 = (a \cdot 0 + a \cdot 0) + -(a \cdot 0)$	14,symmetry
16.	$I \models a \cdot 0 = 0$	15,9,10,transitivity
17.	$I \models \bot$	16,2,contradiction

Example

F: $\forall a, b, c.\ b^2 - 4ac \geq 0 \leftrightarrow \exists x.\ ax^2 + bx + c = 0$ is $T_{\mathbb{R}}$-valid.
As usual: x^2 abbreviates $x \cdot x$, we omit $\cdot$, e.g. in $4ac$,
4 abbreviate $1 + 1 + 1 + 1$ and $a - b$ abbreviates $a + (-b)$.

1.	$I \not\models F$	assumption
2a.	$I \models bb - 4ac \geq 0$	1, $\leftrightarrow$
3a.	$I \not\models \exists x. axx + bx + c = 0$	1, $\leftrightarrow$
4a.	$I \models \exists y.\ bb - 4ac = y^2 \vee bb - 4ac = -y^2$	square root, $\forall$
5a.	$I \models d^2 = bb - 4ac \vee d^2 = -(bb - 4ac)$	2, $\exists$
6a.	$I \models 2a \cdot e = 1$	$\cdot$ inverse, $\forall$, $\exists$
7a.	$I \not\models a((-b + d)e)^2 + b(-b + d)e + c = 0$	6a, $\exists$
8a.	$I \not\models ab^2e^2 - 2abde^2 + ad^2e^2$ $-b^2e + bde + c = 0$	distributivity
9a.	$I \models d^2 \geq 0$	see exercise
10a.	$I \models dd = bb - 4ac$	$\vee$ on 4a, 2a, 9a
11a.	$I \not\models ab^2e^2 - bde + a(b^2 - 4ac)e^2$ $-b^2e + bde + c = 0$	8a,6a, 10a, congruence
12a.	$I \not\models 0 = 0$	11a, distributivity, inverse
13a.	$I \models \bot$	12a, reflexivity

Example

F: $\forall a, b, c.\ bb - 4ac \geq 0 \leftrightarrow \exists x.\ axx + bx + c = 0$ is $T_{\mathbb{R}}$-valid.
As usual: x^2 abbreviates $x \cdot x$, we omit $\cdot$, e.g., in $4ac$,
4 abbreviate $1 + 1 + 1 + 1$ and $a - b$ abbreviates $a + (-b)$.

1.	$I \not\models F$	assumption
$2b$.	$I \not\models bb - 4ac \geq 0$	$1, \leftrightarrow$
$3b$.	$I \models \exists x. axx + bx + c = 0$	$1, \leftrightarrow$
$4b$.	$I \models aff + bf + c = 0$	$8b, \exists$
$5b$.	$I \models (2af + b)^2 = bb - 4ac$	field axioms, T_E
$6b$.	$I \models (2af + b)^2 \geq 0$	see exercise
$7b$.	$I \models bb - 4ac \geq 0$	5b, 6b, equivalence
$8b$.	$I \models \bot$	2b, 7b

Decidability of $T_{\mathbb{R}}$

$T_{\mathbb{R}}$ is decidable (Tarski, 1930)
High time complexity: $O(2^{2^{kn}})$

Signature: $\Sigma_{\mathbb{Q}} : \{0, 1, +, -, =, \geq\}$ no multiplication!

Axioms of $T_{\mathbb{Q}}$: axioms of T_E,

1. $\forall x, y, z.\ (x + y) + z = x + (y + z)$ (+ associativity)
2. $\forall x, y.\ x + y = y + x$ (+ commutativity)
3. $\forall x.\ x + 0 = x$ (+ identity)
4. $\forall x.\ x + (-x) = 0$ (+ inverse)
5. $1 \geq 0 \wedge 1 \neq 0$ (one)
6. $\forall x, y.\ x \geq y \wedge y \geq x \rightarrow x = y$ (antisymmetry)
7. $\forall x, y, z.\ x \geq y \wedge y \geq z \rightarrow x \geq z$ (transitivity)
8. $\forall x, y.\ x \geq y \vee y \geq x$ (totality)
9. $\forall x, y, z.\ x \geq y \rightarrow x + z \geq y + z$ (+ ordered)
10. For every positive integer n:
    $\forall x.\ \exists y.\ x = \underbrace{y + \cdots + y}_{n}$ (divisible)

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

$$x + x + x + y + y + y + y \geq \underbrace{1 + 1 + \cdots + 1}_{24}$$

$T_{\mathbb{Q}}$ is decidable
Efficient algorithm for quantifier free fragment

Recursive Data Structures (RDS)

- Data Structures are tuples of variables.
  Like `struct` in C, `record` in Pascal.
- In Recursive Data Structures, one of the tuple elements can be the data structure again.
  Linked lists or trees.

RDS theory of LISP-like lists, T_{cons}

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

where

$\text{cons}(a, b)$ – list constructed by adding a in front of list 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: The axioms of A_{T_E} plus

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

Axioms of Theory of Lists T_{cons}

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)

We argue that the following Σ_{cons}-formula F is T_{cons}-valid:

$$F: \quad \mathsf{car}(a) = \mathsf{car}(b) \wedge \mathsf{cdr}(a) = \mathsf{cdr}(b) \wedge \neg\mathsf{atom}(a) \wedge \neg\mathsf{atom}(b) \\ \rightarrow a = b$$

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

Lines 6 and 10 are contradictory. Therefore, F is T_{cons}-valid.

Decidability of T_{cons}

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

Theory of Arrays T_A

Signature: Σ_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,e)")

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)

Equality in T_A

Note: $=$ is only defined for array elements

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

not T_A-valid, but

$$a[i] = e \to \forall j.\ a\langle i \triangleleft e\rangle[j] = a[j]\ ,$$

is T_A-valid.

Also

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

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

T_A is undecidable
Quantifier-free fragment of T_A is decidable

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 $(T_{\mathsf{E}} \cup T_{\mathbb{Z}})$-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 $A_1 \cup A_2$

Nelson & Oppen

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 requirements are met
then satisfiability of qff of $T_1 \cup T_2$ is decidable.

Lists with equality $T_{\text{cons}}^{=}$

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

Signature: $\Sigma_{\mathsf{E}} \ \cup \ \Sigma_{\text{cons}}$

(this includes uninterpreted constants, functions, and predicates)

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

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

Example: $T_{\text{cons}}^{=}$-Validity

We argue that the following $\Sigma_{\text{cons}}^{=}$-formula F is $T_{\text{cons}}^{=}$-valid:

$$F: \quad \text{car}(a) = \text{car}(b) \wedge \text{cdr}(a) = \text{cdr}(b) \wedge \neg\text{atom}(a) \wedge \neg\text{atom}(b) \\ \to f(a) = f(b)$$

1.	$I \not\models F$	assumption
2.	$I \models \text{car}(a) = \text{car}(b)$	1, $\to$, $\wedge$
3.	$I \models \text{cdr}(a) = \text{cdr}(b)$	1, $\to$, $\wedge$
4.	$I \models \neg\text{atom}(a)$	1, $\to$, $\wedge$
5.	$I \models \neg\text{atom}(b)$	1, $\to$, $\wedge$
6.	$I \not\models f(a) = f(b)$	1, $\to$
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. Therefore, F is $T_{\text{cons}}^{=}$-valid.

First-Order Theories

	Theory	Decidable	QFF Dec.
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	–	✓
$T_{\mathsf{cons}}^{=}$	Lists with Equality	–	✓
T_{A}	Arrays	–	✓
$T_{\mathsf{A}}^{=}$	Arrays with Extensionality	–	✓