Verification

Lecture 21

Bernd Finkbeiner
Peter Faymonville
Michael Gerke

UNIVERSITÄT
DES
SAARLANDES

Propositional Logic (PL)

PL Syntax

Atom	truth symbols $\top$("true") and $\bot$("false")
	propositional variables $P, Q, R, P_1, Q_1, R_1, \cdots$
Literal	atom α or its negation $\neg\alpha$
Formula	literal or application of a
	logical connective to formulae F, F_1, F_2

$\neg F$	"not"	(negation)
$F_1 \wedge F_2$	"and"	(conjunction)
$F_1 \vee F_2$	"or"	(disjunction)
$F_1 \rightarrow F_2$	"implies"	(implication)
$F_1 \leftrightarrow F_2$	"if and only if"	(iff)

PL Semantics

Formula F + Interpretation I = Truth value (true, false)

Interpretation

$$I : \{P \mapsto \text{true}, Q \mapsto \text{false}, \cdots\}$$

Evaluation of F under I:

F	$\neg F$
0	1
1	0

where 0 corresponds to value false
1 true

F_1	F_2	$F_1 \wedge F_2$	$F_1 \vee F_2$	$F_1 \rightarrow F_2$	$F_1 \leftrightarrow F_2$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Satisfiability and Validity

F is satisfiable iff there exists an interpretation I such that $I \models F$.
F is valid iff for all interpretations I, $I \models F$.

F is valid iff $\neg F$ is unsatisfiable

Satisifability and validity are decidable (truth tables, BDDs, DPLL, ...)

Example $\quad F : P \wedge Q \rightarrow P \vee \neg Q$

P Q	$P \wedge Q$	$\neg Q$	$P \vee \neg Q$	F
0 0	0	1	1	1
0 1	0	0	0	1
1 0	0	1	1	1
1 1	1	0	1	1

Thus F is valid.

First-Order Logic (FOL)

Also called Predicate Logic or Predicate Calculus

FOL Syntax

variables	$x, y, z, \cdots$
constants	$a, b, c, \cdots$
functions	$f, g, h, \cdots$
terms	variables, constants or n-ary function applied to n terms as arguments $a, x, f(a), g(x, b), f(g(x, g(b)))$
predicates	$p, q, r, \cdots$
atom	$\top$, $\bot$, or an n-ary predicate applied to n terms
literal	atom or its negation $p(f(x), g(x, f(x))), \quad \neg p(f(x), g(x, f(x)))$

Note: 0-ary functions: constant
0-ary predicates: $P, Q, R, \ldots$

Quantifiers

existential quantifier $\exists x.F[x]$
"there exists an x such that $F[x]$"

universal quantifier $\forall x.F[x]$
"for all x, $F[x]$"

FOL formula literal, application of logical connectives ($\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$) to formulae,
or application of a quantifier to a formula

Example: FOL formula

$$\forall x.\ \underbrace{p(f(x),x) \rightarrow (\exists y.\ \underbrace{p(f(g(x,y)),g(x,y))}_{G}) \wedge q(x,f(x))}_{F}$$

The scope of $\forall x$ is F.
The scope of $\exists y$ is G.
The formula reads:

"for all x,
if $p(f(x),x)$
then there exists a y such that
$p(f(g(x,y)),g(x,y))$ and $q(x,f(x))$"

FOL Semantics

An interpretation $I : (D_I, \alpha_I)$ consists of:

- Domain D_I
  non-empty set of values or objects
  cardinality $|D_I|$ finite (eg, 52 cards),
  countably infinite (eg, integers), or
  uncountably infinite (eg, reals)
- Assignment α_I
  - each variable x assigned value $x_I \in D_I$
  - each n-ary function f assigned

    $$f_I : D_I^n \to D_I$$

    In particular, each constant a (0-ary function) assigned value $a_I \in D_I$
  - each n-ary predicate p assigned

    $$p_I : D_I^n \to \{\text{true}, \text{false}\}$$

    In particular, each propositional variable P (0-ary predicate) assigned truth value (true, false)

Example:

$$F : p(f(x,y),z) \rightarrow p(y,g(z,x))$$

Interpretation $I : (D_I, \alpha_I)$

$D_I = \mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ integers

$\alpha_I : \{f \mapsto +, g \mapsto -, p \mapsto >\}$

Therefore, we can write

$$F_I : x + y > z \rightarrow y > z - x$$

(This is the way we'll write it in the future!)

Also

$\alpha_I : \{x \mapsto 13, y \mapsto 42, z \mapsto 1\}$

Thus

$$F_I : 13 + 42 > 1 \rightarrow 42 > 1 - 13$$

Compute the truth value of F under I

1.	I	$\models$	$x + y > z$	since $13 + 42 > 1$
2.	I	$\models$	$y > z - x$	since $42 > 1 - 13$
3.	I	$\models$	F	by 1, 2, and $\rightarrow$

F is true under I

Semantics: Quantifiers

x variable.

x-variant of interpretation I is an interpretation $J : (D_J, \alpha_J)$ such that

- $D_I = D_J$
- $\alpha_I[y] = \alpha_J[y]$ for all symbols y, except possibly x

That is, I and J agree on everything except possibly the value of x

Denote $J : I \lhd \{x \mapsto \mathsf{v}\}$ the x-variant of I in which $\alpha_J[x] = \mathsf{v}$ for some $\mathsf{v} \in D_I$. Then

- $I \models \forall x.\, F$ iff for all $\mathsf{v} \in D_I$, $I \lhd \{x \mapsto \mathsf{v}\} \models F$
- $I \models \exists x.\, F$ iff there exists $\mathsf{v} \in D_I$ s.t. $I \lhd \{x \mapsto \mathsf{v}\} \models F$

Example

For $\mathbb{Q}$, the set of rational numbers, consider

$$F : \forall x.\ \exists y.\ 2 \times y = x$$

Compute the value of F_I (F under I):

Let

$J_1 : I \lhd \{x \mapsto \mathsf{v}\}$	$J_2 : J_1 \lhd \{y \mapsto \frac{\mathsf{v}}{2}\}$
x-variant of I	y-variant of J_1

for $\mathsf{v} \in \mathbb{Q}$.

Then

1.	J_2	$\models$	$2 \times y = x$	since $2 \times \frac{\mathsf{v}}{2} = v$
2.	J_1	$\models$	$\exists y.\ 2 \times y = x$	
3.	I	$\models$	$\forall x.\ \exists y.\ 2 \times y = x$	since $\mathsf{v} \in \mathbb{Q}$ is arbitrary

Satisfiability and Validity

F is satisfiable iff there exists I s.t. $I \models F$
F is valid iff for all I, $I \models F$

F is valid iff $\neg F$ is unsatisfiable

- FOL is undecidable (Turing & Church)
  There does not exist an algorithm for deciding if a FOL formula F is valid, i.e. always halt and says "yes" if F is valid or say "no" if F is invalid.
- FOL is semi-decidable
  There is a procedure that always halts and says "yes" if F is valid, but may not halt if F is invalid.

Semantic Argument Method

Proof rules for propositional logic

$$\begin{array}{l} I \models \neg F \\ \hline I \not\models F \end{array} \qquad \begin{array}{l} I \not\models \neg F \\ \hline I \models F \end{array}$$

$$\begin{array}{l} I \models F \wedge G \\ \hline I \models F \\ I \models G \end{array} \leftarrow \text{and} \qquad \begin{array}{c} I \not\models F \wedge G \\ \hline I \not\models F \quad \mid \quad I \not\models G \end{array}$$

$$\nwarrow \text{or}$$

$$\begin{array}{c} I \models F \vee G \\ \hline I \models F \quad \mid \quad I \models G \end{array} \qquad \begin{array}{l} I \not\models F \vee G \\ \hline I \not\models F \\ I \not\models G \end{array}$$

$$\begin{array}{c} I \models F \rightarrow G \\ \hline I \not\models F \quad \mid \quad I \models G \end{array} \qquad \begin{array}{l} I \not\models F \rightarrow G \\ \hline I \models F \\ I \not\models G \end{array}$$

$$\begin{array}{c} I \models F \leftrightarrow G \\ \hline I \models F \wedge G \quad \mid \quad I \not\models F \vee G \end{array} \qquad \begin{array}{c} I \not\models F \leftrightarrow G \\ \hline I \models F \wedge \neg G \quad \mid \quad I \models \neg F \wedge G \end{array}$$

$$\begin{array}{l} I \models F \\ I \not\models F \\ \hline I \models \bot \end{array}$$

Semantic Argument Method

Proof rules for quantifiers

$$\frac{I \models \forall x.\, F}{I \lhd \{x \mapsto \mathsf{v}\} \models F} \qquad \frac{I \not\models \exists x.\, F}{I \lhd \{x \mapsto \mathsf{v}\} \not\models F}$$

$$\frac{I \models \exists x.F}{I \lhd \{x \mapsto \mathsf{v}\} \models F} \text{ for a } \textit{fresh } \mathsf{v} \in D_I \qquad \frac{I \not\models \forall x.F}{I \lhd \{x \mapsto \mathsf{v}\} \not\models F} \text{ for a } \textit{fresh } \mathsf{v} \in D_I$$

$$\frac{\begin{array}{l} J : I \lhd \{\cdots \mapsto \cdots\} \models p(s_1, \ldots, s_n) \\ K : I \lhd \{\cdots \mapsto \cdots\} \not\models p(t_1, \ldots, t_n) \end{array}}{I \models \bot} \text{ for all } i \in \{1, \ldots, n\}, \alpha_J[s_i] = \alpha_K[t_i]$$

First-Order Theories

First-order theory T defined by

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

Σ-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

A Σ-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 Σ-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 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.

Theory of Equality T_E

Signature

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

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

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.

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 $+, -, >$

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

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

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 Σ_{PA} as

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

We have $>$ and $\geq$ since

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

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

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 Σ_{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

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

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

Axioms $T_{\mathbb{N}}$:

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)

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

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

where

- $\ldots, -2, -1, 0, 1, 2, \ldots$ are constants
- $\ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots$ are unary functions
  (intended $2 \cdot x$ 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 $>$

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

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

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

- 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.

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.

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_{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. Congruence axiom for atom

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

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

2. Lists + equality

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

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

(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

Theory of Arrays

1. 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,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)

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