Decision Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Summer 2012

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)
  - QFF of Equality

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)
  - QFF of Equality
  - Presburger arithmetic

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)
  - QFF of Equality
  - Presburger arithmetic
  - (QFF of) Linear integer arithmetic

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)
  - QFF of Equality
  - Presburger arithmetic
  - (QFF of) Linear integer arithmetic
  - Real arithmetic

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

- Quantifier Free Fragment (QFF)
- QFF of Equality
- Presburger arithmetic
- (QFF of) Linear integer arithmetic
- Real arithmetic
- (QFF of) Linear real/rational arithmetic

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)
  - QFF of Equality
  - Presburger arithmetic
  - (QFF of) Linear integer arithmetic
  - Real arithmetic
  - (QFF of) Linear real/rational arithmetic
  - QFF of Recursive Data Structures

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

$\Longrightarrow$ Restrictions to decidable fragments of FOL

  - Quantifier Free Fragment (QFF)
  - QFF of Equality
  - Presburger arithmetic
  - (QFF of) Linear integer arithmetic
  - Real arithmetic
  - (QFF of) Linear real/rational arithmetic
  - QFF of Recursive Data Structures
  - QFF of Arrays

Further route of this lecture

- Syntax and Semantics of First Order Logic (FOL)
- Semantic Tableaux for FOL
- FOL is only semi-decidable

⟹ Restrictions to decidable fragments of FOL

- Quantifier Free Fragment (QFF)
- QFF of Equality
- Presburger arithmetic
- (QFF of) Linear integer arithmetic
- Real arithmetic
- (QFF of) Linear real/rational arithmetic
- QFF of Recursive Data Structures
- QFF of Arrays
- Putting it all together (Nelson-Oppen).

First-Order Logic

Also called Predicate Logic or Predicate Calculus

FOL Syntax

variables	$x, y, z, \cdots$
constants	$a, b, c, \cdots$
functions	$f, g, h, \cdots$ with arity $n > 0$

Also called Predicate Logic or Predicate Calculus

FOL Syntax

variables	$x, y, z, \cdots$
constants	$a, b, c, \cdots$
functions	$f, g, h, \cdots$ with arity $n > 0$
terms	variables, constants or
	n-ary function applied to n terms as arguments
	$a, x, f(a), g(x, b), f(g(x, f(b)))$

Also called Predicate Logic or Predicate Calculus

FOL Syntax

variables	$x, y, z, \cdots$
constants	$a, b, c, \cdots$
functions	$f, g, h, \cdots$ with arity $n > 0$
terms	variables, constants or
	n-ary function applied to n terms as arguments
	$a, x, f(a), g(x, b), f(g(x, f(b)))$
predicates	$p, q, r, \cdots$ with arity $n \geq 0$

Also called Predicate Logic or Predicate Calculus

FOL Syntax

variables	$x, y, z, \cdots$
constants	$a, b, c, \cdots$
functions	$f, g, h, \cdots$ with arity $n > 0$
terms	variables, constants or
	n-ary function applied to n terms as arguments
	$a, x, f(a), g(x, b), f(g(x, f(b)))$
predicates	$p, q, r, \cdots$ with arity $n \geq 0$
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: $P, Q, R, \ldots$

Syntax of First-Order Logic (2)

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.

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 $q(x, f(x))$"

Famous theorems in FOL

- The length of one side of a triangle is less than the sum of the lengths of the other two sides

Famous theorems in FOL

- The length of one side of a triangle is less than the sum of the lengths of the other two sides

$$\forall x, y, z.\ \mathit{triangle}(x, y, z) \rightarrow \mathit{length}(x) < \mathit{length}(y) + \mathit{length}(z)$$

Famous theorems in FOL

- The length of one side of a triangle is less than the sum of the lengths of the other two sides

$$\forall x, y, z.\ \mathit{triangle}(x, y, z) \rightarrow \mathit{length}(x) < \mathit{length}(y) + \mathit{length}(z)$$

- Fermat's Last Theorem.

Famous theorems in FOL

- The length of one side of a triangle is less than the sum of the lengths of the other two sides

$$\forall x, y, z.\ triangle(x, y, z) \rightarrow length(x) < length(y) + length(z)$$

- Fermat's Last Theorem.

$$\begin{aligned}
&\forall n.\ integer(n) \land n > 2 \\
&\quad \rightarrow \forall x, y, z. \\
&\qquad integer(x) \land integer(y) \land integer(z) \\
&\qquad \land x > 0 \land y > 0 \land z > 0 \\
&\qquad\quad \rightarrow x^n + y^n \neq z^n
\end{aligned}$$

Pumping Lemma

Pumping Lemma

For every regular Language L there is some $n \geq 0$, such that for all words $z \in L$ with $|z| \geq n$ there is a decomposition $z = uvw$ with $|v| \geq 1$ and $|uv| \leq n$, such that for all $i \geq 0$: $uv^i w \in L$.

Pumping Lemma

For every regular Language L there is some $n \geq 0$, such that for all words $z \in L$ with $|z| \geq n$ there is a decomposition $z = uvw$ with $|v| \geq 1$ and $|uv| \leq n$, such that for all $i \geq 0$: $uv^i w \in L$.

$$\begin{array}{l}
\forall L.\ regularlanguage(L) \rightarrow \\
\quad \exists n.\ integer(n) \land n \geq 0 \land \\
\quad\quad \forall z.\ z \in L \land |z| \geq n \rightarrow \\
\quad\quad\quad \exists u, v, w.\ word(u) \land word(v) \land word(w) \land \\
\quad\quad\quad\quad z = uvw \land |v| \geq 1 \land |uv| \leq n \land \\
\quad\quad\quad\quad \forall i.\ integer(i) \land i \geq 0 \rightarrow uv^i w \in L
\end{array}$$

Pumping Lemma

For every regular Language L there is some $n \geq 0$, such that for all words $z \in L$ with $|z| \geq n$ there is a decomposition $z = uvw$ with $|v| \geq 1$ and $|uv| \leq n$, such that for all $i \geq 0$: $uv^i w \in L$.

$$
\begin{array}{l}
\forall L.\ \mathit{regularlanguage}(L) \rightarrow \\
\quad \exists n.\ \mathit{integer}(n) \land n \geq 0 \land \\
\quad\quad \forall z.\ z \in L \land |z| \geq n \rightarrow \\
\quad\quad\quad \exists u, v, w.\ \mathit{word}(u) \land \mathit{word}(v) \land \mathit{word}(w) \land \\
\quad\quad\quad\quad z = uvw \land |v| \geq 1 \land |uv| \leq n \land \\
\quad\quad\quad\quad \forall i.\ \mathit{integer}(i) \land i \geq 0 \rightarrow uv^i w \in L
\end{array}
$$

Predicates: $\mathit{regularlanguage}$, $\mathit{integer}$, word, $\cdot \in \cdot$, $\cdot \leq \cdot$, $\cdot \geq \cdot$, $\cdot = \cdot$

Pumping Lemma

For every regular Language L there is some $n \geq 0$, such that for all words $z \in L$ with $|z| \geq n$ there is a decomposition $z = uvw$ with $|v| \geq 1$ and $|uv| \leq n$, such that for all $i \geq 0$: $uv^i w \in L$.

$$\begin{array}{l}
\forall L.\ \mathit{regularlanguage}(L) \rightarrow \\
\quad \exists n.\ \mathit{integer}(n) \land n \geq 0 \land \\
\quad\quad \forall z.\ z \in L \land |z| \geq n \rightarrow \\
\quad\quad\quad \exists u, v, w.\ \mathit{word}(u) \land \mathit{word}(v) \land \mathit{word}(w) \land \\
\quad\quad\quad\quad z = uvw \land |v| \geq 1 \land |uv| \leq n \land \\
\quad\quad\quad\quad \forall i.\ \mathit{integer}(i) \land i \geq 0 \rightarrow uv^i w \in L
\end{array}$$

Predicates: *regularlanguage*, *integer*, *word*, $\cdot \in \cdot$, $\cdot \leq \cdot$, $\cdot \geq \cdot$, $\cdot = \cdot$
Constants: 0, 1
Functions: $|\cdot|$ (word length), concatenation, iteration

FOL Semantics

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

- Domain D_I
  non-empty set of values or objects

FOL Semantics

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

- Domain D_I
  non-empty set of values or objects
  for example $D_I =$ playing cards (finite),

FOL Semantics

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

- Domain D_I
  non-empty set of values or objects
  for example $D_I =$ playing cards (finite),
  integers (countable infinite), or

FOL Semantics

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

- Domain D_I
  non-empty set of values or objects
  for example $D_I =$ playing cards (finite),
  integers (countable infinite), or
  reals (uncountable infinite)

FOL Semantics

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

- Domain D_I

  non-empty set of values or objects

  for example $D_I =$ playing cards (finite),
  integers (countable infinite), or
  reals (uncountable infinite)

- Assignment α_I
  - each variable x assigned value $\alpha_I[x] \in D_I$

FOL Semantics

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

- Domain D_I
  non-empty set of values or objects
  for example $D_I =$ playing cards (finite),
  integers (countable infinite), or
  reals (uncountable infinite)
- Assignment α_I
  - each variable x assigned value $\alpha_I[x] \in D_I$
  - each n-ary function f assigned

$$\alpha_I[f] : D_I^n \rightarrow D_I$$

  In particular, each constant a (0-ary function) assigned value $\alpha_I[a] \in D_I$

FOL Semantics

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

- Domain D_I
  non-empty set of values or objects
  for example $D_I =$ playing cards (finite),
  integers (countable infinite), or
  reals (uncountable infinite)
- Assignment α_I
  - each variable x assigned value $\alpha_I[x] \in D_I$
  - each n-ary function f assigned

    $$\alpha_I[f] : D_I^n \to D_I$$

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

    $$\alpha_I[p] : D_I^n \to \{\top, \bot\}$$

    In particular, each propositional variable P (0-ary predicate) assigned truth value ($\top$, $\bot$)

Example

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

Interpretation $I : (D_I, \alpha_I)$

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

$\alpha_I[f] : D_I^2 \to D_I$, $(x,y) \mapsto x + y$

$\alpha_I[g] : D_I^2 \to D_I$, $(x,y) \mapsto x - y$

$$\alpha_I[p] : D_I^2 \to \{\top, \bot\}$$

$$(x,y) \mapsto \begin{cases} \top & \text{if } x < y \\ \bot & \text{otherwise} \end{cases}$$

Example

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

Interpretation $I : (D_I, \alpha_I)$

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

$$\alpha_I[f] : \; D_I^2 \rightarrow D_I \qquad \alpha_I[g] : \; D_I^2 \rightarrow D_I$$

$$(x,y) \mapsto x + y \qquad (x,y) \mapsto x - y$$

$$\alpha_I[p] : \; D_I^2 \rightarrow \{\top, \bot\}$$

$$(x,y) \mapsto \begin{cases} \top & \text{if } x < y \\ \bot & \text{otherwise} \end{cases}$$

Also $\alpha_I[x] = 13, \alpha_I[y] = 42, \alpha_I[z] = 1$

Compute the truth value of F under I

Example

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

Interpretation $I \;:\; (D_I, \alpha_I)$

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

$$\alpha_I[f] \;:\; D_I^2 \rightarrow D_I \qquad\qquad \alpha_I[g] \;:\; D_I^2 \rightarrow D_I$$

$$(x,y) \mapsto x + y \qquad\qquad (x,y) \mapsto x - y$$

$$\alpha_I[p] \;:\; D_I^2 \rightarrow \{\top, \bot\}$$

$$(x,y) \mapsto \begin{cases} \top & \text{if } x < y \\ \bot & \text{otherwise} \end{cases}$$

Also $\alpha_I[x] = 13, \alpha_I[y] = 42, \alpha_I[z] = 1$

Compute the truth value of F under I

1.	$I \not\models p(f(x,y),z)$	since $13 + 42 \geq 1$
2.	$I \not\models p(y,g(z,x))$	since $42 \geq 1 - 13$
3.	$I \models F$	by 1, 2, and $\rightarrow$

F is true under I

For a variable x:

Definition (x-variant)

An 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

Semantics: Quantifiers

For a variable x:

Definition (x-variant)

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

For a variable x:

Definition (x-variant)

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

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

Example

Consider

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

Here $2 \cdot y$ is the infix notatation of the term $\cdot(2, y)$,
and $2 \cdot y = x$ is the infix notatation of the atom $= (\cdot(2, y), x)$.

- 2 is a 0-ary function symbol (a constant).
- $\cdot$ is a 2-ary function symbol.
- $=$ is a 2-ary predicate symbol.
- x, y are variables.

Example

Consider

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

Here $2 \cdot y$ is the infix notatation of the term $\cdot(2, y)$,
and $2 \cdot y = x$ is the infix notatation of the atom $= (\cdot(2, y), x)$.

- 2 is a 0-ary function symbol (a constant).
- $\cdot$ is a 2-ary function symbol.
- $=$ is a 2-ary predicate symbol.
- x, y are variables.

What is the truth-value of F?

Example ($\mathbb{Z}$)

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

Let I be the standard interpration for integers, $D_I = \mathbb{Z}$.
Compute the value of F under I:

Example ($\mathbb{Z}$)

$$F : \forall x.\, \exists y.\, 2 \cdot y = x$$

Let I be the standard interpration for integers, $D_I = \mathbb{Z}$.
Compute the value of F under I:

$$I \models \forall x.\, \exists y.\, 2 \cdot y = x$$

iff

$$\text{for all v} \in D_I,\ I \triangleleft \{x \mapsto \text{v}\} \models \exists y.\, 2 \cdot y = x$$

iff

for all v $\in D_I$, there exists $\text{v}_1 \in D_I$, $I \triangleleft \{x \mapsto \text{v}\} \triangleleft \{y \mapsto \text{v}_1\} \models 2 \cdot y = x$

The latter is false since for $1 \in D_I$ there is no number v_1 with $2 \cdot v_1 = 1$.

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

Let I be the standard interpration for rational numbers, $D_I = \mathbb{Q}$.
Compute the value of F under I:

Example ($\mathbb{Q}$)

$$F : \forall x.\, \exists y.\, 2 \cdot y = x$$

Let I be the standard interpration for rational numbers, $D_I = \mathbb{Q}$.
Compute the value of F under I:

$$I \models \forall x.\, \exists y.\, 2 \cdot y = x$$

iff

$$\text{for all } \mathsf{v} \in D_I,\ I \triangleleft \{x \mapsto \mathsf{v}\} \models \exists y.\, 2 \cdot y = x$$

iff

for all $\mathsf{v} \in D_I$, there exists $\mathsf{v}_1 \in D_I$, $I \triangleleft \{x \mapsto \mathsf{v}\} \triangleleft \{y \mapsto \mathsf{v}_1\} \models 2 \cdot y = x$

The latter is true since for $\mathsf{v} \in D_I$ we can choose $\mathsf{v}_1 = \frac{\mathsf{v}}{2}$.

Satisfiability and Validity

Definition (Satisfiability)

F is satisfiable iff there exists an interpretation I such that $I \models F$.

Definition (Validity)

F is valid iff for all interpretations I, $I \models F$.

Satisfiability and Validity

Definition (Satisfiability)

F is satisfiable iff there exists an interpretation I such that $I \models F$.

Definition (Validity)

F is valid iff for all interpretations I, $I \models F$.

Note

F is valid iff $\neg F$ is unsatisfiable

Substitution

Suppose, we want to replace terms with other terms in formulas, e.g.

$$F \; : \; \forall y.\; (p(x, y) \rightarrow p(y, x))$$

should be transformed to

$$G \; : \; \forall y.\; (p(a, y) \rightarrow p(y, a))$$

Substitution

Suppose, we want to replace terms with other terms in formulas, e.g.

$$F \; : \; \forall y. \; (p(x, y) \rightarrow p(y, x))$$

should be transformed to

$$G \; : \; \forall y. \; (p(a, y) \rightarrow p(y, a))$$

We call the mapping from x to a a substituion denoted as $\sigma : \{x \mapsto a\}$.

Substitution

Suppose, we want to replace terms with other terms in formulas, e.g.

$$F\ :\ \forall y.\ (p(x,y) \rightarrow p(y,x))$$

should be transformed to

$$G\ :\ \forall y.\ (p(a,y) \rightarrow p(y,a))$$

We call the mapping from x to a a substituion denoted as $\sigma : \{x \mapsto a\}$.
We write $F\sigma$ for the formula G.

Substitution

Suppose, we want to replace terms with other terms in formulas, e.g.

$$F \ : \forall y. \ (p(x, y) \rightarrow p(y, x))$$

should be transformed to

$$G \ : \forall y. \ (p(a, y) \rightarrow p(y, a))$$

We call the mapping from x to a a substituion denoted as $\sigma : \{x \mapsto a\}$.
We write $F\sigma$ for the formula G.
Another convenient notation is $F[x]$ for a formula containing the variable x and $F[a]$ for $F\sigma$.

Substitution

Definition (Substitution)

A substitution is a mapping from terms to terms, e.g.

$$\sigma : \{t_1 \mapsto s_1, \ldots, t_n \mapsto s_n\}$$

By $F\sigma$ we denote the application of σ to formula F, i.e., the formula F where all occurences of $t_1, \ldots, t_n$ are replaced by $s_1, \ldots, s_n$.

For a formula named $F[x]$ we write $F[t]$ as shorthand for $F[x]\{x \mapsto t\}$.

Safe Substitution

Care has to be taken in the presence of quantifiers:

$$F[x] \, : \, \exists y.\ y = Succ(x)$$

What is $F[y]$?

Safe Substitution

Care has to be taken in the presence of quantifiers:

$$F[x] : \exists y.\ y = Succ(x)$$

What is $F[y]$?
We need to rename bounded variables occuring in the substitution:

$$F[y] : \exists y'.\ y' = Succ(y)$$

Safe Substitution

Care has to be taken in the presence of quantifiers:

$$F[x] : \exists y.\ y = Succ(x)$$

What is $F[y]$?
We need to rename bounded variables occuring in the substitution:

$$F[y] : \exists y'.\ y' = Succ(y)$$

Bounded renaming does not change the models of a formula:

$$(\exists y.\ y = Succ(x)) \Leftrightarrow (\exists y'.\ y' = Succ(x))$$

Recursive Definition of Substitution

$$t\sigma = \begin{cases} \sigma(t) & t \in \mathrm{dom}(\sigma) \\ f(t_1\sigma, \ldots, t_n\sigma) & t \notin \mathrm{dom}(\sigma) \wedge t = f(t_1, \ldots, t_n) \\ x & t \notin \mathrm{dom}(\sigma) \wedge t = x \end{cases}$$

$$\begin{aligned} p(t_1, \ldots, t_n)\sigma &= p(t_1\sigma, \ldots, t_n\sigma) \\ (\neg F)\sigma &= \neg(F\sigma) \\ (F \wedge G)\sigma &= (F\sigma) \wedge (G\sigma) \\ &\ldots \end{aligned}$$

$$(\forall x.\ F)\sigma = \begin{cases} \forall x.\ F\sigma & x \notin \mathit{Vars}(\sigma) \\ \forall x'.\ ((F\{x \mapsto x'\})\sigma) & \text{otherwise and } x' \text{ is fresh} \end{cases}$$

$$(\exists x.\ F)\sigma = \begin{cases} \exists x.\ F\sigma & x \notin \mathit{Vars}(\sigma) \\ \exists x'.\ ((F\{x \mapsto x'\})\sigma) & \text{otherwise and } x' \text{ is fresh} \end{cases}$$

$$F : (\forall x.\ \underset{\text{bound by } \forall x \nearrow}{p(x},\underset{\nwarrow \text{ free}}{y))} \rightarrow\ q(f(\underset{\text{free} \nearrow}{y}),\ \underset{\nwarrow \text{ free}}{x})$$

$$\sigma : \{x \mapsto g(x),\ y \mapsto f(x),\ f(y) \mapsto h(x,y)\}$$

$F\sigma$?

Example: Safe Substitution $F\sigma$

$$F \;:\; (\forall x.\ p(x, y)) \rightarrow\ q(f(y),\ x)$$

bound by $\forall x$ $\nearrow$ $\nwarrow$ free free $\nearrow$ $\nwarrow$ free

$$\sigma \;:\; \{x \mapsto g(x),\ y \mapsto f(x),\ f(y) \mapsto h(x, y)\}$$

$F\sigma$?

1. Rename

$$F' \;:\; \forall x'.\ p(x', y) \rightarrow q(f(y), x)$$

$\uparrow$ $\uparrow$

where x' is a fresh variable

2. $F\sigma \;:\; \forall x'.\ p(x', f(x)) \rightarrow q(h(x, y), g(x))$

Semantic Tableaux

Recall rules from propositional logic:

$$\frac{I \models \neg F}{I \not\models F} \qquad \frac{I \not\models \neg F}{I \models F}$$

$$\frac{I \models F \wedge G}{\begin{array}{l} I \models F \\ I \models G \end{array}} \leftarrow \text{and} \qquad \frac{I \not\models F \wedge G}{I \not\models F \mid I \not\models G} \;\; (\nwarrow \text{or})$$

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

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

$$\frac{I \models F \leftrightarrow G}{I \models F \wedge G \mid I \not\models F \vee G} \qquad \frac{I \not\models F \leftrightarrow G}{I \models F \wedge \neg G \mid I \models \neg F \wedge G}$$

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

Semantic Tableaux for FOL

The following additional rules are used for quantifiers:

$$\frac{I \models \forall x. F[x]}{I \models F[t]} \text{ for any term } t \qquad \frac{I \not\models \forall x. F[x]}{I \not\models F[a]} \text{ for a fresh constant } a$$

$$\frac{I \models \exists x. F[x]}{I \models F[a]} \text{ for a fresh constant } a \qquad \frac{I \not\models \exists x. F[x]}{I \not\models F[t]} \text{ for any term } t$$

(We assume that there are infinitely many constant symbols.)

The formula $F[t]$ is created from the formula $F[x]$ by the substitution $\{x \mapsto t\}$ (roughly, replace every x by t).

Example

Show that $(\exists x.\ \forall y.\ p(x, y)) \rightarrow (\forall x.\ \exists y.\ p(y, x))$ is valid.

Example

Show that $(\exists x.\ \forall y.\ p(x,y)) \rightarrow (\forall x.\ \exists y.\ p(y,x))$ is valid.

Assume otherwise.

1.	$I \not\models (\exists x.\ \forall y.\ p(x,y)) \rightarrow (\forall x.\ \exists y.\ p(y,x))$		assumption
2.	$I \models \exists x.\ \forall y.\ p(x,y)$		1 and $\rightarrow$
3.	$I \not\models \forall x.\ \exists y.\ p(y,x)$		1 and $\rightarrow$
4.	$I \models \forall y.\ p(a,y)$		2, $\exists$ ($x \mapsto a$ fresh)
5.	$I \not\models \exists y.\ p(y,b)$		3, $\forall$ ($x \mapsto b$ fresh)
6.	$I \models p(a,b)$		4, $\forall$ ($y \mapsto b$)
7.	$I \not\models p(a,b)$		5, $\exists$ ($y \mapsto a$)
8.	$I \models \bot$		6,7 contradictory

Thus, the formula is valid.

Example

Is $F \; : \; (\forall x.\ p(x, x)) \rightarrow (\exists x.\ \forall y.\ p(x, y))$ valid?.

Example

Is F : $(\forall x.\ p(x, x)) \rightarrow (\exists x.\ \forall y.\ p(x, y))$ valid?.

Assume I is a falsifying interpretation for F and apply semantic argument:

1.	$I \not\models (\forall x.\ p(x, x)) \rightarrow (\exists x.\ \forall y.\ p(x, y))$	
2.	$I \models \forall x.\ p(x, x)$	1 and $\rightarrow$
3.	$I \not\models \exists x.\ \forall y.\ p(x, y)$	1 and $\rightarrow$
4.	$I \models p(a_1, a_1)$	2, $\forall$
5.	$I \not\models \forall y. p(a_1, y)$	3, $\exists$
6.	$I \not\models p(a_1, a_2)$	5, $\forall$
7.	$I \models p(a_2, a_2)$	2, $\forall$
8.	$I \not\models \forall y. p(a_2, y)$	3, $\exists$
9.	$I \not\models p(a_2, a_3)$	8, $\forall$
$\vdots$		

No contradiction.

Example

Is F : $(\forall x.\ p(x,x)) \rightarrow (\exists x.\ \forall y.\ p(x,y))$ valid?.

Assume I is a falsifying interpretation for F and apply semantic argument:

1.	$I \not\models (\forall x.\ p(x,x)) \rightarrow (\exists x.\ \forall y.\ p(x,y))$	
2.	$I \models \forall x.\ p(x,x)$	1 and $\rightarrow$
3.	$I \not\models \exists x.\ \forall y.\ p(x,y)$	1 and $\rightarrow$
4.	$I \models p(a_1,a_1)$	2, $\forall$
5.	$I \not\models \forall y. p(a_1,y)$	3, $\exists$
6.	$I \not\models p(a_1,a_2)$	5, $\forall$
7.	$I \models p(a_2,a_2)$	2, $\forall$
8.	$I \not\models \forall y. p(a_2,y)$	3, $\exists$
9.	$I \not\models p(a_2,a_3)$	8, $\forall$

$\vdots$

No contradiction. Falsifying interpretation I can be “read” from proof:

$$D_I = \mathbb{N}, \quad p_I(x,y) = \begin{cases} \text{true} & y = x, \\ \text{false} & y = x+1, \\ \text{arbitrary} & \text{otherwise.} \end{cases}$$

Semantic Argument Proof

To show FOL formula F is valid, assume $I \not\models F$ and derive a contradiction $I \models \bot$ in all branches

Semantic Argument Proof

To show FOL formula F is valid, assume $I \not\models F$ and derive a contradiction $I \models \perp$ in all branches

- Soundness
  If every branch of a semantic argument proof reach $I \models \perp$, then F is valid

To show FOL formula F is valid, assume $I \not\models F$ and derive a contradiction $I \models \bot$ in all branches

- Soundness
  If every branch of a semantic argument proof reach $I \models \bot$, then F is valid
- Completeness
  Each valid formula F has a semantic argument proof in which every branch reach $I \models \bot$

Semantic Argument Proof

To show FOL formula F is valid, assume $I \not\models F$ and derive a contradiction $I \models \bot$ in all branches

- Soundness
  If every branch of a semantic argument proof reach $I \models \bot$, then F is valid
- Completeness
  Each valid formula F has a semantic argument proof in which every branch reach $I \models \bot$
- Non-termination
  For an invalid formula F the method is not guaranteed to terminate.
  Thus, the semantic argument is not a decision procedure for validity.

Soundness (proof sketch)

If for interpretation I the assumption of the proof hold
then there is an interpretation I' and a branch
such that all statements on that branch hold.

Soundness (proof sketch)

If for interpretation I the assumption of the proof hold
then there is an interpretation I' and a branch
such that all statements on that branch hold.

I' differs from I in the values $\alpha_I[a_i]$ of fresh constants a_i.

Soundness (proof sketch)

If for interpretation I the assumption of the proof hold
then there is an interpretation I' and a branch
such that all statements on that branch hold.

I' differs from I in the values $\alpha_I[a_i]$ of fresh constants a_i.

If all branches of the proof end with $I \models \bot$, then the assumption was wrong.

Soundness (proof sketch)

If for interpretation I the assumption of the proof hold
then there is an interpretation I' and a branch
such that all statements on that branch hold.

I' differs from I in the values $\alpha_I[a_i]$ of fresh constants a_i.

If all branches of the proof end with $I \models \bot$, then the assumption was wrong. Thus, if the assumption was $I \not\models F$, then F must be valid.

Completeness (proof sketch)

Consider (finite or infinite) proof trees starting with $I \not\models F$. We assume that

- all possible proof rules were applied in all non-closed branches.
- the $\forall$ and $\exists$ rules were applied for all terms.
  This is possible since the terms are countable.

If every branch is closed, the tree is finite (Kőnig's Lemma) and we have a finite proof for F.

Completeness (proof sketch, continued)

Otherwise, the proof tree has at least one open branch P. We show that F is not valid.

Completeness (proof sketch, continued)

Otherwise, the proof tree has at least one open branch P. We show that F is not valid.

1. The statements on that branch P form a Hintikka set:
   - $I \models F \wedge G \in P$ implies $I \models F \in P$ and $I \models G \in P$.
   - $I \not\models F \wedge G \in P$ implies $I \not\models F \in P$ or $I \not\models G \in P$.
   - $I \models \forall x.\ F[x] \in P$ implies for all terms t, $I \models F[t] \in P$.
   - $I \not\models \forall x.\ F[x] \in P$ implies for some term a, $I \not\models F[a] \in P$.
   - Similarly for $\vee, \rightarrow, \leftrightarrow, \exists$.

Completeness (proof sketch, continued)

Otherwise, the proof tree has at least one open branch P. We show that F is not valid.

1. The statements on that branch P form a Hintikka set:
   - $I \models F \land G \in P$ implies $I \models F \in P$ and $I \models G \in P$.
   - $I \not\models F \land G \in P$ implies $I \not\models F \in P$ or $I \not\models G \in P$.
   - $I \models \forall x.\ F[x] \in P$ implies for all terms t, $I \models F[t] \in P$.
   - $I \not\models \forall x.\ F[x] \in P$ implies for some term a, $I \not\models F[a] \in P$.
   - Similarly for $\lor, \rightarrow, \leftrightarrow, \exists$.
2. Choose $D_I := \{t \mid t \text{ is term}\}$, $\alpha_I[f](t_1, \dots, t_n) = f(t_1, \dots t_n)$,

$$\alpha_I[x] = x, \quad \alpha_I[p](t_1, \dots, t_n) = \begin{cases} \text{true} & I \models p(t_1, \dots, t_n) \in P \\ \text{false} & \text{otherwise} \end{cases}$$

Completeness (proof sketch, continued)

Otherwise, the proof tree has at least one open branch P. We show that F is not valid.

1. The statements on that branch P form a Hintikka set:
   - $I \models F \wedge G \in P$ implies $I \models F \in P$ and $I \models G \in P$.
   - $I \not\models F \wedge G \in P$ implies $I \not\models F \in P$ or $I \not\models G \in P$.
   - $I \models \forall x.\ F[x] \in P$ implies for all terms t, $I \models F[t] \in P$.
   - $I \not\models \forall x.\ F[x] \in P$ implies for some term a, $I \not\models F[a] \in P$.
   - Similarly for $\vee, \rightarrow, \leftrightarrow, \exists$.
2. Choose $D_I := \{t \mid t \text{ is term}\}$, $\alpha_I[f](t_1, \ldots, t_n) = f(t_1, \ldots t_n)$,

$$\alpha_I[x] = x, \quad \alpha_I[p](t_1, \ldots, t_n) = \begin{cases} \text{true} & I \models p(t_1, \ldots, t_n) \in P \\ \text{false} & \text{otherwise} \end{cases}$$

3. I satisfies all statements on the branch.
   In particular, I is a falsifying interpretation of F, thus F is not valid.

Normal Forms

Also in first-order logic normal forms can be used:

- Devise an algorithm to convert a formula to a normal form.
- Then devise an algorithm for satisfiability/validity that only works on the normal form.

Negation Normal Forms (NNF)

Negations appear only in literals. (only $\neg, \wedge, \vee, \exists, \forall$)

To transform F to equivalent F' in NNF use recursively the following template equivalences (left-to-right):

$$\neg\neg F_1 \Leftrightarrow F_1 \qquad \neg\top \Leftrightarrow \bot \qquad \neg\bot \Leftrightarrow \top$$

$$\left.\begin{array}{l} \neg(F_1 \wedge F_2) \Leftrightarrow \neg F_1 \vee \neg F_2 \\ \neg(F_1 \vee F_2) \Leftrightarrow \neg F_1 \wedge \neg F_2 \end{array}\right\} \text{De Morgan's Law}$$

$$F_1 \rightarrow F_2 \Leftrightarrow \neg F_1 \vee F_2$$

$$F_1 \leftrightarrow F_2 \Leftrightarrow (F_1 \rightarrow F_2) \wedge (F_2 \rightarrow F_1)$$

Negation Normal Forms (NNF)

Negations appear only in literals. (only $\neg, \wedge, \vee, \exists, \forall$)

To transform F to equivalent F' in NNF use recursively the following template equivalences (left-to-right):

$$\neg\neg F_1 \Leftrightarrow F_1 \qquad \neg\top \Leftrightarrow \bot \qquad \neg\bot \Leftrightarrow \top$$

$$\left.\begin{array}{l}\neg(F_1 \wedge F_2) \Leftrightarrow \neg F_1 \vee \neg F_2 \\ \neg(F_1 \vee F_2) \Leftrightarrow \neg F_1 \wedge \neg F_2\end{array}\right\}\text{De Morgan's Law}$$

$$F_1 \to F_2 \Leftrightarrow \neg F_1 \vee F_2$$

$$F_1 \leftrightarrow F_2 \Leftrightarrow (F_1 \to F_2) \wedge (F_2 \to F_1)$$

$$\neg\forall x.\ F[x] \Leftrightarrow \exists x.\ \neg F[x]$$

$$\neg\exists x.\ F[x] \Leftrightarrow \forall x.\ \neg F[x]$$

Example: Conversion to NNF

$$G \;:\; \forall x.\ (\exists y.\ p(x,y) \land p(x,z)) \to \exists w. p(x,w)\ .$$

Example: Conversion to NNF

$$G \; : \; \forall x.\; (\exists y.\; p(x,y) \wedge p(x,z)) \rightarrow \exists w. p(x,w) \; .$$

1. $\forall x.\; (\exists y.\; p(x,y) \wedge p(x,z)) \rightarrow \exists w.\; p(x,w)$
2. $\forall x.\; \neg(\exists y.\; p(x,y) \wedge p(x,z)) \vee \exists w.\; p(x,w)$

   $$F_1 \rightarrow F_2 \Leftrightarrow \neg F_1 \vee F_2$$

3. $\forall x.\; (\forall y.\; \neg(p(x,y) \wedge p(x,z))) \vee \exists w.\; p(x,w)$

   $$\neg \exists x.\; F[x] \Leftrightarrow \forall x.\; \neg F[x]$$

4. $\forall x.\; (\forall y.\; \neg p(x,y) \vee \neg p(x,z)) \vee \exists w.\; p(x,w)$

Prenex Normal Form (PNF)

All quantifiers appear at the beginning of the formula

$$Q_1 x_1 \cdots Q_n x_n.\ F[x_1, \cdots, x_n]$$

where $Q_i \in \{\forall, \exists\}$ and F is quantifier-free.

Every FOL formula F can be transformed to formula F' in PNF s.t. $F' \Leftrightarrow F$:

Prenex Normal Form (PNF)

All quantifiers appear at the beginning of the formula

$$Q_1 x_1 \cdots Q_n x_n.\ F[x_1, \cdots, x_n]$$

where $Q_i \in \{\forall, \exists\}$ and F is quantifier-free.

Every FOL formula F can be transformed to formula F' in PNF s.t. $F' \Leftrightarrow F$:

1. Write F in NNF

Prenex Normal Form (PNF)

All quantifiers appear at the beginning of the formula

$$Q_1 x_1 \cdots Q_n x_n.\ F[x_1, \cdots, x_n]$$

where $Q_i \in \{\forall, \exists\}$ and F is quantifier-free.

Every FOL formula F can be transformed to formula F' in PNF s.t. $F' \Leftrightarrow F$:

1. Write F in NNF
2. Rename quantified variables to fresh names

Prenex Normal Form (PNF)

All quantifiers appear at the beginning of the formula

$$Q_1 x_1 \cdots Q_n x_n.\ F[x_1, \cdots, x_n]$$

where $Q_i \in \{\forall, \exists\}$ and F is quantifier-free.

Every FOL formula F can be transformed to formula F' in PNF s.t. $F' \Leftrightarrow F$:

1. Write F in NNF
2. Rename quantified variables to fresh names
3. Move all quantifiers to the front

Example: PNF

Find equivalent PNF of

$$F \; : \; \forall x. \; ((\exists y. \; p(x,y) \wedge p(x,z)) \rightarrow \exists y. \; p(x,y))$$

Example: PNF

Find equivalent PNF of

$$F \;:\; \forall x.\ ((\exists y.\ p(x,y) \wedge p(x,z)) \rightarrow \exists y.\ p(x,y))$$

- Write F in NNF

$$F_1 \;:\; \forall x.\ (\forall y.\ \neg p(x,y) \vee \neg p(x,z)) \vee \exists y.\ p(x,y)$$

- Rename quantified variables to fresh names

$$F_2 \;:\; \forall x.\ (\forall y.\ \neg p(x,y) \vee \neg p(x,z)) \vee \exists w.\ p(x,w)$$

$\uparrow$ in the scope of $\forall x$

Example: PNF

- Move all quantifiers to the front

$$F_3 \;:\; \forall x.\, \forall y.\, \exists w.\, \neg p(x,y) \vee \neg p(x,z) \vee p(x,w)$$

Alternately,

$$F_3' \;:\; \forall x.\, \exists w.\, \forall y.\, \neg p(x,y) \vee \neg p(x,z) \vee p(x,w)$$

Note: In F_2, $\forall y$ is in the scope of $\forall x$, therefore the order of quantifiers must be $\cdots \forall x \cdots \forall y \cdots$

$$\boxed{F_4 \Leftrightarrow F \text{ and } F_4' \Leftrightarrow F}$$

Note: However $G \not\Leftrightarrow F$

$$G \;:\; \forall y.\, \exists w.\, \forall x.\, \neg p(x,y) \vee \neg p(x,z) \vee p(x,w)$$

Decidability of FOL

Decidability of FOL

- 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.

Decidability of FOL

- 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.

Decidability of FOL

- 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.

On the other hand,

- PL is decidable
  There exists an algorithm for deciding if a PL formula F is valid, e.g., the truth-table procedure.

Similarly for satisfiability

Theories

Theories

The formula $1 + 1 = 3$ is

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

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

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

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

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

- $=$, a binary predicate, interpreted by axioms.
- all constant, function, and predicate symbols.

Theory of Equality T_E

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

- $=$, 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)

Theory of Equality T_E

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

- $=$, 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)

Theory of Equality T_E

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

- $=$, 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)

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

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

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.

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.

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

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

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

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	$I \not\models \bot$	3 and 5 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?

Decidability of T_E

Is it possible to decide T_E-validity?

T_E-validity is undecidable.

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.

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

Three variations:

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

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

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

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

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

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)

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

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

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)

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

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

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)

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. $\forall x, y.\ x + 1 = y + 1 \to x = y$ (successor)
3. $F[0] \wedge (\forall x.\ F[x] \to F[x + 1]) \to \forall x.\ F[x]$ (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)

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}

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

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

We can define $>$ and $\geq$:

Expressiveness of Peano Arithmetic

$3x + 5 = 2y$ 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 $\exists z.\, z \neq 0 \wedge 3x + 5 = 2y + z$

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

Expressiveness of Peano Arithmetic

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

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

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

$$3x + 5 \geq 2y \quad \text{write as} \quad \exists z.\ 3x + 5 = 2y + z$$

Examples for valid formulae:

- Pythagorean Theorem is T_{PA}-valid

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

Expressiveness of Peano Arithmetic

$3x + 5 = 2y$ 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
$\exists z.\, z \neq 0 \wedge 3x + 5 = 2y + z$

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

Examples for valid formulae:

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

Expressiveness of Peano Arithmetic (2)

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

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

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

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

Fermat's theorem can be stated as:

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

Decidability of Peano Arithmetic

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

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

Decidability of Peano Arithmetic

Gödel showed that for every recursive function $f : \mathbb{N}^n \rightarrow \mathbb{N}$ 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)

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)

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

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. $\forall x, y. x + 1 = y + 1 \to x = y$ (successor)
3. $F[0] \wedge (\forall x. F[x] \to F[x + 1]) \to \forall x. F[x]$ (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.

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.

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.

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

Consider the $\Sigma_{\mathbb{Z}}$-formula

$F_0 : \ \forall w, x.\ \exists y, z.\ x + 2y - z - 7 > -3w + 4$

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

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

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

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

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

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

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

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

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

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

Eliminate $>$ and numbers:

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

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

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:

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

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:

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

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

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:

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

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)

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

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)

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

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)

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

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 $T_{\mathbb{R}}$

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

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

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)

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

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. $\forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ associativity)
6. $\forall x, y.\ x \cdot y = y \cdot x$ ($\cdot$ commutativity)
7. $\forall x.\ x \cdot 1 = x$ ($\cdot$ identity)
8. $\forall x.\ x \neq 0 \rightarrow \exists y.\ x \cdot y = 1$ ($\cdot$ inverse)

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. $\forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ associativity)
6. $\forall x, y.\ x \cdot y = y \cdot x$ ($\cdot$ commutativity)
7. $\forall x.\ x \cdot 1 = x$ ($\cdot$ identity)
8. $\forall x.\ x \neq 0 \rightarrow \exists y.\ x \cdot y = 1$ ($\cdot$ inverse)
9. $\forall x, y, z.\ x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivity)

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

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)

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

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. $\forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ associativity)
6. $\forall x, y.\ x \cdot y = y \cdot x$ ($\cdot$ commutativity)
7. $\forall x.\ x \cdot 1 = x$ ($\cdot$ identity)
8. $\forall x.\ x \neq 0 \rightarrow \exists y.\ x \cdot y = 1$ ($\cdot$ inverse)
9. $\forall x, y, z.\ x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivity)
10. $0 \neq 1$ (separate identies)
11. $\forall x, y.\ x \geq y \wedge y \geq x \rightarrow x = y$ (antisymmetry)
12. $\forall x, y, z.\ x \geq y \wedge y \geq z \rightarrow x \geq z$ (transitivity)
13. $\forall x, y.\ x \geq y \vee y \geq x$ (totality)

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

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. $\forall x, y.\ x \geq y \wedge y \geq x \rightarrow x = y$ (antisymmetry)
12. $\forall x, y, z.\ x \geq y \wedge y \geq z \rightarrow x \geq z$ (transitivity)
13. $\forall x, y.\ x \geq y \vee y \geq x$ (totality)
14. $\forall x, y, z.\ x \geq y \rightarrow x + z \geq y + z$ (+ ordered)
15. $\forall x, y.\ x \geq 0 \wedge y \geq 0 \rightarrow x \cdot y \geq 0$ (· ordered)

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. $\forall x, y.\ x \geq y \wedge y \geq x \rightarrow x = y$ (antisymmetry)
12. $\forall x, y, z.\ x \geq y \wedge y \geq z \rightarrow x \geq z$ (transitivity)
13. $\forall x, y.\ x \geq y \vee y \geq x$ (totality)
14. $\forall x, y, z.\ x \geq y \rightarrow x + z \geq y + z$ (+ ordered)
15. $\forall x, y.\ x \geq 0 \wedge y \geq 0 \rightarrow x \cdot y \geq 0$ (· ordered)
16. $\forall x.\ \exists y.\ x = y \cdot y \vee x = -y \cdot y$ (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: $\forall a, b, c.\ b^2 - 4ac \geq 0 \leftrightarrow \exists x.\ ax^2 + bx + c = 0$ 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 $a + (-b)$.

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
2.	$I \models \exists y.\ bb - 4ac = y^2 \lor bb - 4ac = -y^2$		square root, $\forall$
3.	$I \models d^2 = bb - 4ac \lor d^2 = -(bb - 4ac)$		2, $\exists$
4.	$I \models d \geq 0 \lor 0 \geq d$		$\geq$ total
5.	$I \models d^2 \geq 0$		4, case distinction, $\cdot$ ordered
6.	$I \models 2a \cdot e = 1$		$\cdot$ inverse, $\forall$, $\exists$
7a.	$I \models bb - 4ac \geq 0$		1,$\leftrightarrow$
8a.	$I \not\models \exists x.axx + bx + c = 0$		1,$\leftrightarrow$
9a.	$I \not\models a((-b + d)e)^2 + b(-b + d)e + c = 0$		8a, $\exists$
10a.	$I \not\models ab^2e^2 - 2abde^2 + ad^2e^2$ $-b^2e + bde + c = 0$		distributivity
11a.	$I \models dd = bb - 4ac$		3, 5, 7a
12a.	$I \not\models ab^2e^2 - bde + a(b^2 - 4ac)e^2$ $-b^2e + bde + c = 0$		6, 11a, congruence
13a.	$I \not\models 0 = 0$		3, distributivity, inverse
14a.	$I \models \bot$		13a, 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
2.	$I \models \exists y.\ bb - 4ac = y^2 \lor bb - 4ac = -y^2$		square root, $\forall$
3.	$I \models d^2 = bb - 4ac \lor d^2 = -(bb - 4ac)$		2, $\exists$
4.	$I \models d \geq 0 \lor 0 \geq d$		$\geq$ total
5.	$I \models d^2 \geq 0$		4, case distinction, $\cdot$ ordered
6.	$I \models 2a \cdot e = 1$		$\cdot$ inverse, $\forall$,$\exists$
$7b$.	$I \not\models bb - 4ac \geq 0$		1,$\leftrightarrow$
$8b$.	$I \models \exists x. axx + bx + c = 0$		1,$\leftrightarrow$
$9b$.	$I \models aff + bf + c = 0$		8b,$\exists$
$10b$.	$I \models (2af + b)^2 = bb - 4ac$		field axioms, T_E
$11b$.	$I \models (2af + b)^2 \geq 0$		analogous to 5
$12b$.	$I \models bb - 4ac \geq 0$		10b, 11b, equivalence
$13b$.	$I \models \bot$		12b, 7b

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

$T_{\mathbb{R}}$ is decidable (Tarski, 1930)
High time complexity

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

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

Theory of Rationals $T_{\mathbb{Q}}$

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

Theory of Rationals $T_{\mathbb{Q}}$

Signature: $\Sigma_{\mathbb{Q}}$: $\{0,\ 1,\ +,\ -,\ =,\ \geq\}$ no 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. $1 \geq 0 \wedge 1 \neq 0$ (one)

Theory of Rationals $T_{\mathbb{Q}}$

Signature: $\Sigma_{\mathbb{Q}}$: $\{0, 1, +, -, =, \geq\}$ no 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. $1 \geq 0 \wedge 1 \neq 0$ (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)

Theory of Rationals $T_{\mathbb{Q}}$

UNI FREIBURG

Signature: $\Sigma_{\mathbb{Q}}$: $\{0,\ 1,\ +,\ -,\ =,\ \geq\}$ no 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. $1 \geq 0 \wedge 1 \neq 0$ (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)

Theory of Rationals $T_{\mathbb{Q}}$

Signature: $\Sigma_{\mathbb{Q}}$: $\{0,\ 1,\ +,\ -,\ =,\ \geq\}$ no 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. $1 \geq 0 \land 1 \neq 0$ (one)
6. $\forall x, y.\ x \geq y \land y \geq x \rightarrow x = y$ (antisymmetry)
7. $\forall x, y, z.\ x \geq y \land y \geq z \rightarrow x \geq z$ (transitivity)
8. $\forall x, y.\ x \geq y \lor y \geq x$ (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)

Expressiveness and Decidability of $T_{\mathbb{Q}}$

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

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

Expressiveness and Decidability of $T_{\mathbb{Q}}$

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.
- Recursive Data Structures one of the tuple element 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)

Decidability of T_{cons}

Decidability of T_{cons}

T_{cons} is undecidable

Decidability of T_{cons}

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

Example: T_{cons}-Validity

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

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

Example: T_{cons}-Validity

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

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

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.	$I \not\models a = b$	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)

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

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

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

not T_A-valid, but

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

is T_A-valid.

Equality in T_A

Note: $=$ is only defined for array elements

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

not T_A-valid, but

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

is T_A-valid.

Also

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

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

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

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.

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

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?

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 . . . ?

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

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

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

(this includes uninterpreted constants, functions, and predicates)

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

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

(this includes uninterpreted constants, functions, and predicates)

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

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

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:

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

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

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

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

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. 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	–	✓