Formale Systeme II: Theorie

Theories

SS 2022

Prof. Dr. Bernhard Beckert · Dr. Mattias Ulbrich

Theories and Satisfiability – Introduction

Different Questions to Ask

Deciding logics

Question: Is formula ϕ valid, i.e., ϕ satisfied in all possible structures.

- $(\forall x. p(x)) \to p(f(x))$ is valid.
- $x > y \to y < x$ not valid (uninterpreted symbols!)

Deciding theories

Question: Is formula ϕ satisfied structures with fixed interpretation for symbols.

- $\exists x.\ 2 \cdot x^2 - x - 1 = 0 \land x < 0$ holds in $\mathbb{R}$, ...
- ... but not in $\mathbb{Z}$.

Theories

Given a FOL signature Σ
Fml_Σ ...set of closed FOL-formulas over Σ.

Definition: *Theory*

A theory $T \subset Fml_\Sigma$ is a set of formulas such that

1. T is **closed under consequence**: If $T \models \phi$ then $\phi \in T$
2. T is **consistent**: $false \notin T$

A FOL structure (D, I) is called a T-model of $\psi \in Fml_\Sigma$ if

1. $D, I \models \psi$ and
2. $D, I \models \phi$ for all $\phi \in T$

Theories II

- A FOL structure (D, I) is called a T-structure if $D, I \models \phi$ for all $\phi \in T$.

- A T-structure (D, I) is a T-model of $\psi \in Fml_\Sigma$ if $D, I \models \psi$.

- $\psi \in Fml_\Sigma$ is called T-satisfiable if it has a T-model.

- $\psi \in Fml_\Sigma$ is called T-valid if every T-structure is a T-model of ψ. $\iff T \models \psi \iff \psi \in T$

- T is called complete if: $\phi \in Fml_\Sigma \implies \phi \in T$ or $\neg\phi \in T$

- $\models_T$ is used instead of $T \models$: $S \models_T \phi$ defined as $S \cup T \models \phi$

Generating Theories

Axiomatisation

Theory T may be represented by a **set** $Ax \subset Fml_\Sigma$ **of axioms**.
T is the consequential closure of Ax, we write:

$$T = \mathcal{T}(Ax) := \{\phi \mid Ax \models \phi\}$$

T is "axiomatisable".

Fixing a structure

Theory T may be represented by one **particular structure** (D, I).
T is the set of true formulas in (D, I), we write:

$$T = \mathcal{T}(D, I) := \{\phi \mid (D, I) \models \phi\}$$

Discussion

- Every theory $\mathcal{T}(D, I)$ is complete.
- If Ax is recursive enumerable, then $\mathcal{T}(Ax)$ is recursive enumerable.
- If Ax is decidable, then $\mathcal{T}(Ax)$ needs not be decidable.
- $\mathcal{T}(D, I)$ needs not be recursive enumerable.
- (D, I) is not the only $\mathcal{T}(D, I)$-model.
  (In general, two $\mathcal{T}(D, I)$-models are not even isomorphic)

Free variables

When dealing with theories, formulas often have free variables.

Open and closed (reminder)

$\phi_1 = \forall x.\exists y.p(x,y)$ is closed, has no free variables,
$\phi_2 = \exists y.p(x,y)$ is open, has free variables $FV(\phi_2) = \{x\}$

$Fml^o_\Sigma \supset Fml_\Sigma$ …set of **open** formulas

Existential closure $\exists[\cdot]$

For $\phi \in Fml^o_\Sigma$ with $FV = \{x_1, ..., x_n\}$ define:

$$\exists[\phi] := \exists x_1. \ldots \exists x_n.\ \phi$$

$\phi \in Fml^o_\Sigma$ is called T-satisfiable if $\exists[\phi]$ is T-satisfiable.

Axioms for Equality

Theorem

Equality can be axiomatised in first order logic.

This means: Given signature Σ, there is a set $Eq_\Sigma \subset Fml_\Sigma$ that axiomatise equality:

$\phi^\approx$ is formula ϕ with interpreted "$=$" replaced by uninterpred "$\approx$".

$$S \models \phi \iff S^\approx \models_{\mathcal{T}(Eq_\Sigma)} \phi^\approx$$

FOL with equality cannot be more expressive than FOL without built-in equality.

Axioms for Equality

Axioms Eq_Σ:

- $\forall x.\ x \approx x$ (Reflexivity)

- $\forall x_1, x_1, \ldots, x_n, x_n'.$
  $$x_1 \approx x_1' \wedge \ldots \wedge x_n \approx x_n' \to f(x_1, ..., x_n) \approx f(x_1', \ldots, x_n')$$
  for any function f in Σ with arity n. (Congruency)

- $\forall x_1, x_1, \ldots, x_n, x_n'.$
  $$x_1 \approx x_1' \wedge \ldots \wedge x_n \approx x_n' \to p(x_1, ..., x_n) \leftrightarrow p(x_1', \ldots, x_n')$$
  for any predicate p in Σ with arity n. (Congruency)
  (This includes predicate $\approx$)

Symmetry and transitivity of $\approx$ are consequences of Eq_Σ
$\rightsquigarrow$ Exercise

Satisfiability Modulo Theories

SMT solvers

A lot of research in recent years:
(Simplify), Z3, CVC4, Yices, MathSAT, SPT, ...
Some for many theories, others only for a single theory.

(Common input format SMT-Lib 2)

$Fml^{QF} \subset Fml^{o}$ ... the set of quantifier-free formulas

Interesting questions for a theory T:

- **SAT:** Is $\phi \in Fml^{o}$ a T-satisfiable formula?
- **QF-SAT:** Is $\phi \in Fml^{QF}$ a T-satisfiable formula?

Decision Procedure

Decision Procedure

A decision procedure DP_T for a theory T is a deterministic algorithm that always terminates.
It takes a formula ϕ as input and returns SAT if ϕ is T-satisfiable, UNSAT otherwise.

N.B.:

- ϕ is T-valid $\iff$ $\neg\phi$ is not T-satisfiable.
- DP_T can also be used to decide validity!

Decision Procedures

Theory	**QF-SAT**	**SAT**
Equality	**YES**	**YES**
Uninterpreted functions	**YES**	co-**SEMI**
Integer arithmetic		
Linear arithmetic		
Real arithmetic		
Bitvectors	**YES**	**YES**
Floating points	**YES**	**YES**

Natural Arithmetic – Goedel's (First) Incompleteness Theorem

Natural Numbers

Standard model of natural numbers

Let $\Sigma_{\mathcal{N}} = (\{+, *, 0, 1\}, \{<\})$.

$\mathcal{N} = (\mathbb{N}, I_{\mathcal{N}})$ with "obvious" meaning:

$I_{\mathcal{N}}(\left\{\begin{smallmatrix}+\\ *\\ <\end{smallmatrix}\right\})(a, b) = a \left\{\begin{smallmatrix}+\\ \cdot\\ <\end{smallmatrix}\right\} b, I_{\mathcal{N}}(0) = 0, I_{\mathcal{N}}(1) = 1$

$\mathcal{T}(\mathcal{N})$ is the set of all sentences over $\Sigma_{\mathcal{N}}$ which are true in the natural numbers.

Gödel's Incompleteness Theorem

"Any consistent formal system within which a certain amount of elementary arithmetic can be carried out is incomplete."

Peano Arithmetic

Natural number arithmetic is not axiomatisable (with a r.e. set)
Let's **approximate**.

The Peano Axioms PA

1. $\forall x(x + 1 \not\doteq 0)$
2. $\forall x \forall y(x + 1 \doteq y + 1 \to x \doteq y)$
3. $\forall x(x + 0 \doteq x)$
4. $\forall x \forall y(x + (y + 1) \doteq (x + y) + 1)$
5. $\forall x(x * 0 \doteq 0)$
6. $\forall x \forall y(x * (y + 1) \doteq (x * y) + x)$
7. For any $\phi \in Fml_{\Sigma_{\mathcal{N}}}$
   $$(\phi(0) \wedge \forall x(\phi(x) \to \phi(x + 1))) \to \forall x(\phi)$$

That's an infinite (yet recursive) set of Axioms.

Peano Arithmetic

- Peano arithmetic approximates natural arithmetic.
- More $\mathcal{T}(PA)$-models than $\mathcal{T}(\mathcal{N})$-models
- $\mathcal{T}(PA)$ is not complete.

$\Longrightarrow$ There are $\mathcal{T}(\mathcal{N})$-valid formulas that are **not** $\mathcal{T}(PA)$-valid formulas.

There are artificial examples in $\mathcal{T}(\mathcal{N}) \setminus \mathcal{T}(PA)$,
but also actual mathematical theorems:

The first result is an improvement of a theorem of Goodstein [2]. Let m and n be natural numbers, $n > 1$. We define the *base n representation* of m as follows:

First write m as the sum of powers of n. (For example, if $m = 266$, $n = 2$, write $266 = 2^8 + 2^3 + 2^1$.) Now write each exponent as the sum of powers of n. (For example, $266 = 2^{2^3} + 2^{2+1} + 2^1$.) Repeat with exponents of exponents and so on until the representation stabilizes. For example, 266 stabilizes at the representation $2^{2^{2+1}} + 2^{2+1} + 2^1$.

We now define the number $G_n(m)$ as follows. If $m = 0$ set $G_n(m) = 0$. Otherwise set $G_n(m)$ to be the number produced by replacing every n in the base n representation of m by $n+1$ and then subtracting 1. (For example, $G_2(266) = 3^{3^{3+1}} + 3^{3+1} + 2$).

Now define the Goodstein sequence for m starting at 2 by

$$m_0 = m,\ m_1 = G_2(m_0),\ m_2 = G_3(m_1),\ m_3 = G_4(m_2),\ \ldots .$$

So, for example,

$$266_0 = 266 = 2^{2^{2+1}} + 2^{2+1} + 2$$

$$266_1 = 3^{3^{3+1}} + 3^{3+1} + 2 \sim 10^{38}$$

$$266_2 = 4^{4^{4+1}} + 4^{4+1} + 1 \sim 10^{616}$$

$$266_3 = 5^{5^{5+1}} + 5^{5+1} \sim 10^{10,000}.$$

Similarly we can define the Goodstein sequence for m starting at n for any $n > 1$.

THEOREM 1. (i) (Goodstein [**2**]) $\forall m\, \exists k\, m_k = 0$. *More generally for any $m, n > 1$ the Goodstein sequence for m starting at n eventually hits zero.*

(ii) $\forall m\, \exists k\, m_k = 0$ (*formalized in the language of first order arithmetic*) *is not provable in P.*

from: L. KIRBY and J. PARIS, 'Accessible Independence Results for Peano Arithmetic' (1982)
[2] R. L. GOODSTEIN, 'On the restricted ordinal theorem', J. Symbolic Logic (1944)

Decision Procedures

Theory	QF-SAT	SAT
Equality	**YES**	**YES**
Uninterpreted functions	**YES**	co-**SEMI**
Integer arithmetic	**NO**[1]	**NO**
Linear arithmetic		
Real arithmetic		
Bitvectors	**YES**	**YES**
Floating points	**YES**	**YES**

[1] Yuri Matiyasevich. Enumerable sets are diophantine. Journal of Sovietic Mathematics, 1970.

Natural Arithmetic – Presburger Arithmetic and its Decidability

Presburger Arithmetic

Let $\Sigma_P = (\{0, 1, +\}, \{<\})$, the signature w/o multiplication.

The Presburger Axioms P

1. $\forall x(x + 1 \not\doteq 0)$
2. $\forall x \forall y(x + 1 \doteq y + 1 \rightarrow x \doteq y)$
3. $\forall x(x + 0 \doteq x)$
4. $\forall x \forall y(x + (y + 1) \doteq (x + y) + 1)$
5. For any $\phi \in Fml_{\Sigma_\mathcal{N}}$
   $(\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x + 1))) \rightarrow \forall x(\phi)$

A subset of the Peano axioms (w/o those for multiplication).

Conventions:

$3 \stackrel{def}{=} 1 + 1 + 1, \qquad 3x \stackrel{def}{=} x + x + x, \qquad$ etc.

Presburger Arithmetic

Mojżesz Presburger. *Über die Vollständigkeit eines gewissen Systems der Arithmetik*, Warsaw 1929

Theorem

He proved Presburger arithmetic to be

- consistent,
- complete, and
- decidable.

We are interested in the 3rd property!

Quantifier Elimination

Definition

A theory T admits **quantifier elimination** (QE) if any formula

$$Q_1 x_1 \dots Q_n x_n .\ \phi(x_1, \dots, x_n, y_1, \dots, y_m) \in Fml^o$$

is T-equivalent to a quantifier-free formula

$$\psi(y_1, \dots, y_m) \in Fml^o \quad .$$

$Q_i \in \{\forall, \exists\}$

If T-ground instances in $Fml^{QF} \cap Fml$ can be decided, QE gives us a decision procedure for T.

Quantifier Elimination

Lemma

If T admits QE for any formula

$$\exists x.\ \phi_1(x, y_1, \ldots, y_m) \wedge \ldots \wedge \phi_n(x, y_1, \ldots, y_m) \in Fml^o$$

with ϕ_i literals, then T admits QE for any formula in Fml^o.

Literal: atomic formula or a negation of one.

Proof: (Easy) exercise.

Presburger and Quantifier Elimination

Does Presburger Arithmetic admits QE?

Almost … However

$$\exists x . y = x + x \text{ has no quantifier-free } P\text{-equivalent}$$

Add predicates: $\{k|\cdot : k \in \mathbb{N}_{>0}\}$ “k divides …”

$$\exists x . y = x + x \;\leftrightarrow\; 2|y \qquad \text{is } P\text{-valid}$$

Presburger Arithmetic with divisibility admits QE.

$\leadsto$ Cooper's algorithm … Blackboard

Decision Procedures

Theory	QF-SAT	SAT
Equality	YES	YES
Uninterpreted functions	YES	co-SEMI
Integer arithmetic	NO	NO
Linear arithmetic	YES	YES
Real arithmetic		
Bitvectors	YES	YES
Floating points	YES	YES

Real Arithmetic

Real arithmetic is decidable

$\Sigma = (\{+, -, \cdot, 0, 1\}, \{\leq\}), \qquad \varphi \in \mathit{Fml}_\Sigma$

Reminder:

$\mathbb{N} \models \varphi$ is not decidable, not even recursive enumerable (Gödel).

Tarski-Seidenberg theorem (c. 1948)

$\mathbb{R} \models \varphi$ **is** decidable.
Complexity is double exponential (c. 1988).

Idea: *Quantifier elimination*

Find formula ψ such that $(\exists x.\varphi(x, y)) \leftrightarrow \psi(y)$.
Computer algebra systems do this: Redlog, Mathematica, (Z3)

Real arithmetic – Axioms

Real arithmetic has a recursive axiomatisation R

- $+$ is an Abelian group, $\cdot$ is an Abelian semigroup:

  $$\begin{array}{ll} \forall x, y, z.\ (x + y) + z = x + (y + z) & \forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ \forall x, y.\ x + y = y + x & \forall x, y.\ x \cdot y = y \cdot x \\ \forall x.\ x + 0 = x \land 0 + x = x & \forall x.\ x \cdot 1 = x \land 1 \cdot x = x \\ \forall x.\ x + (-x) = 0 \land (-x) + x = 0 & \end{array}$$

- Distributive Laws
  $\forall x, y, z.\ (x + y) \cdot z = x \cdot z + y \cdot z \quad \land \quad z \cdot (x + y) = z \cdot x + z \cdot y$

- Ordering
  $\forall x, y, z.\ x \leq y \to x + z \leq y + z$
  $\forall x, y.\ 0 \leq x \land 0 \leq y \to 0 \leq xy$

- Roots
  $\forall x \exists y.\ (y \cdot y = x \lor y \cdot y = -x)$
  $\forall a_0 \ldots \forall a_n.\ a_n \neq 0 \to \exists x.\ (a_n x^n + \ldots + a_0 = 0)$ for all odd $n \in \mathbb{N}$

Real closed fields

$\mathcal{T}(\mathbb{R}) = \mathcal{T}(R)$ is the set of FOL sentences that are true in $\mathbb{R}$.

But there are also other interesting models of $\mathcal{T}(R)$:

- Real numbers $\mathbb{R}$,
- Real algebraic numbers $\mathbb{R} \cap \bar{\mathbb{Q}}$
  (real numbers that are roots of polynomials with integer coeffs.)
- Computable numbers
  (real numbers that can be approximated arbitrarily precisely.)
- ...

Semialgebraic sets

Semialgebraic set

$S \subseteq \mathbb{R}^n$ is called *semialgebraic* if it defined by a boolean combination of polynomial equations and inequalitites.

Boolean combination means: $\cup, \cap, \complement$

Observation:

S is semialgebaric iff there is a quantifier-free FOL-formula $\varphi(S)$ with n free variables $x_1, \ldots, x_n$ such that

$$(s_1, \ldots, s_n) \in S \iff \mathbb{R}, [x_1 \mapsto s_1, \ldots, x_n \mapsto s_n] \models \varphi(S)$$

Tarski-Seidenberg Theorem

Definition: *Projection* $\pi_n : \mathbb{R}^n \to \mathbb{R}^{n-1}$

$$\pi_n((s_1, \dots, s_n)) := (s_1, \dots, s_{n-1})$$

$$\pi_n(S) := \{\pi_n(\bar{s}) \mid \bar{s} \in S\} \qquad \text{(extended to } 2^{\mathbb{R}}\text{)}$$

$$(s_1, \dots, s_{n-1}) \in \pi_n(S) \iff \mathbb{R}, [x_1 \mapsto s_1, \dots, x_{n-1} \mapsto s_{n-1}] \models \exists x_n.\, \varphi(S)$$

Tarski-Seidenberg Theorem (*Projektionssatz*)

Let $S \subseteq \mathbb{R}^n$ be semialgebraic.
Then $\pi_n(S) \in \mathbb{R}^{n-1}$ is also semialgebraic.

Example

Single variable, single quadratic equation

Let S_{quad} be the solutions of $ax^2 + bx + c = 0$.
(is semialgebraic: $ax^2 + bx + c \in \mathbb{R}[a, b, c, x]$)

Due to Tarski-Seidenberg, there must be an equiv. quantifier-free formula $\varphi(\pi_4(S_{quad}))$ with free variables a, b, c.

$$\exists x. ax^2 + bx + c = 0$$

$$\iff$$

$$(a \neq 0 \wedge b^2 - 4ac \geq 0)$$
$$\vee\ (a = 0 \wedge (b = 0 \rightarrow c = 0))$$

$\big(\exists x. x^3 + a_2x^2 + a_1x + a_0 = 0$ is trivally equivalent to true.$\big)$

Quantifier Elimination – Algorithm

1. Sufficient to look at $\exists x. \bigwedge_i \phi_i(\bar{y}, x)$ for atomic ϕ_i. $\rightarrow$ Excercise
2. Sufficient to consider ϕ_i of shape $p(\bar{y}, x) \begin{Bmatrix} < \\ > \\ = \end{Bmatrix} 0$ for $p \in \mathbb{R}[\bar{y}][x]$ $\rightarrow$ Why?
3. Every polynomial $p \in R[x]$ has finitely many connected regions with same sign. $\rightarrow$ Board
   Choose a set *Rep* of representatives.
4. $\exists x. \bigwedge\limits_i \phi_i(x, \bar{y}) \leftrightarrow \bigvee\limits_{r \in Rep} \bigwedge\limits_i \phi_i(r, \bar{y})$

Decision Technique

Cylindrical Algebraic Decomposition (CAD)

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x. x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$
- Interesting intervals: $(-\infty, 2)$, $(2, 3)$, $(3, \infty)$, $(2, z)$, ...
- Representatives:

$$\begin{aligned} Rep &= \left\{2, 3, z, \text{“}-\infty\text{”}, \text{“}+\infty\text{”}, \tfrac{2+3}{2}, \tfrac{2+z}{2}, \tfrac{3+z}{2}\right\} \\ &= \left\{\tfrac{i_1+i_2}{2} \mid i_1, i_2 \in I\right\} \cup \{\text{“}-\infty\text{”}, \text{“}+\infty\text{”}\} \end{aligned}$$

For the example:

$$\begin{aligned} \psi \quad &\leftrightarrow \quad \bigvee_{r \in Rep} r > 2 \land r < 3 \land r > z \\ &\leftrightarrow \quad 2.5 > z \lor (z > 2 \land z < 4 \land 2 > z) \lor (z > 1 \land z < 3 \land 3 > z) \\ &\leftrightarrow \quad z < 3 \end{aligned}$$

Decision Procedures

Theory	**QF-SAT**	**SAT**
Equality	**YES**	**YES**
Uninterpreted functions	**YES**	co-**SEMI**
Integer arithmetic	**NO**	**NO**
Linear arithmetic	**YES**	**YES**
Real arithmetic	**YES**	**YES**
Bitvectors	**YES**	**YES**
Floating points	**YES**	**YES**

Divison

Karlsruhe Institute of Technology

Adding division (the inverse $\cdot^{-1}$) does not increase expressive power.

Consider $\Sigma_{div} = \Sigma \cup \{\cdot^{-1}\}$.
Let quantifier-free $\varphi \in \mathit{Fml}^{qf}_{\Sigma_{div}}$ contain a division by t:

$$\varphi[t^{-1}] \;\leftrightarrow\; \big((\exists y. y = t^{-1} \land \varphi[y]) \lor (t = 0 \land \varphi[n])\big) \tag{1}$$

n is a fresh free variable for the value of "0^{-1}"

Let $\psi \in \mathit{Fml}_{\Sigma_{div}}$ contain divisions.
Obtain $\psi' \in \mathit{Fml}_{\Sigma}$ by applying (1) to literals in ψ.

$$\mathbb{R} \models \psi \iff \mathbb{R} \models \forall n. \psi'$$

Underspecification: ψ is true in $\mathbb{R}$ if it is true for all possible valuations of "0^{-1}": $\mathbb{R} \models \frac{1}{0} = \frac{1}{0}$, $\mathbb{R} \not\models \frac{1}{0} = \frac{2}{0}$