Satisfiability Modulo Theories

Lecture 4: First-order Theories

Lydia Kondylidou

WS 2025/26

Outline

- First-order Theories
- Satisfiability Modulo Theories
- Examples of First-order Theories

Motivation

Consider the signature $\Sigma = \langle \Sigma^S, \Sigma^F \rangle$ for a fragment of number theory:

$$\Sigma^S = \{\mathsf{Nat}\} \qquad \Sigma^F = \{0, 1, +, <\}$$

$$\mathsf{rank}(0) = \langle \mathsf{Nat} \rangle \qquad \mathsf{rank}(1) = \langle \mathsf{Nat} \rangle$$

$$\mathsf{rank}(+) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Nat} \rangle \qquad \mathsf{rank}(<) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Bool} \rangle$$

Consider the Σ-sentence

$$\forall x \in \mathbb{N}.\ \neg(x < x)$$

$$\neg\exists x \in \mathbb{N}.\ x < 0$$

$$\forall x, y, z \in \mathbb{N}.\ (x < y \wedge y < z \implies x < z)$$

Is the formula **valid**?

Motivation

Consider the signature $\Sigma = \langle \Sigma^S, \Sigma^F \rangle$ for a fragment of number theory:

$$\Sigma^S = \{\mathsf{Nat}\} \qquad \Sigma^F = \{0, 1, +, <\}$$

$$\mathsf{rank}(0) = \langle \mathsf{Nat} \rangle \qquad \mathsf{rank}(1) = \langle \mathsf{Nat} \rangle$$

$$\mathsf{rank}(+) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Nat} \rangle \qquad \mathsf{rank}(<) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Bool} \rangle$$

Consider the Σ-sentence

$$\forall x \in \mathbb{N}.\ \neg(x < x)$$

$$\neg\exists x \in \mathbb{N}.\ x < 0$$

$$\forall x, y, z \in \mathbb{N}.\ (x < y \wedge y < z \implies x < z)$$

Is the formula **valid**? *No, e.g., if we interpret* $<$ *as* ***equals*** *or as* ***divides***

Motivation

Consider the signature $\Sigma = \langle \Sigma^S, \Sigma^F \rangle$ for a fragment of number theory:

$$\Sigma^S = \{\mathsf{Nat}\} \qquad \Sigma^F = \{0, 1, +, <\}$$

$$\mathsf{rank}(0) = \langle \mathsf{Nat} \rangle \qquad \mathsf{rank}(1) = \langle \mathsf{Nat} \rangle$$

$$\mathsf{rank}(+) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Nat} \rangle \qquad \mathsf{rank}(<) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Bool} \rangle$$

Consider the Σ-sentence

$$\forall x \in \mathbb{N}.\ \neg(x < x)$$

$$\neg\exists x \in \mathbb{N}.\ x < 0$$

$$\forall x, y, z \in \mathbb{N}.\ (x < y \wedge y < z \implies x < z)$$

Is the formula **valid**? *No, e.g., if we interpret* Nat *as the set of all integers*

Motivation

Consider the signature $\Sigma = \langle \Sigma^S, \Sigma^F \rangle$ for a fragment of number theory:

$$\Sigma^S = \{\mathsf{Nat}\} \qquad \Sigma^F = \{0, 1, +, <\}$$

$$\mathsf{rank}(0) = \langle \mathsf{Nat} \rangle \qquad \mathsf{rank}(1) = \langle \mathsf{Nat} \rangle$$

$$\mathsf{rank}(+) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Nat} \rangle \qquad \mathsf{rank}(<) = \langle \mathsf{Nat}, \mathsf{Nat}, \mathsf{Bool} \rangle$$

Consider the Σ-sentence

$$\forall x \in \mathbb{N}.\ \neg(x < x)$$

$$\neg\exists x \in \mathbb{N}.\ x < 0$$

$$\forall x, y, z \in \mathbb{N}.\ (x < y \wedge y < z \implies x < z)$$

Is the formula **valid**? *No, e.g., if we interpret $<$ as the successor relation*

Motivation

Recall that **valid** means true for **all** possible interpretations

In practice, we often do **not** care about satisfiability or validity **in general** but rather with respect to a **limited class** of interpretations

Motivation

A practical reason:

When reasoning in a particular application domain, we typically have **specific** data types/structures in mind (e.g., integers, strings, lists, arrays, finite sets, ...)

More generally, we are typically **not** interested in **arbitrary** interpretations, but in **specific** in ones

Theories formalize this domain-specific reasoning:

we talk about satisfiability or validity *in a theory* or *modulo a theory*

Motivation

A computational reason:

While validity in FOL is undecidable, validity in **particular theories** can be **decidable**

It is useful for AR purposes to

identify decidable fragments of FOL and

develop efficient decision procedures for them

First-order theories

We will assume from now on an infinite set X of variables

A *theory* $\mathcal{T}$ is a pair $\langle \Sigma, M \rangle$, where:

$\Sigma = \langle \Sigma^S, \Sigma^F \rangle$ is a signature

M is a class[a] of Σ-interpretations over X that is **closed under variable re-assignment**

M is *closed under variable re-assignment* if every Σ-interpretation that differs from one in M **only** in the way it interprets the variables of X is also in M

A theory limits the interpretations of Σ-formulas to those from M

[a] In set theory, a class is a more general notion of set.

First-order theories

Example 1: the theory of Real Arithmetic $\mathcal{T}_{\mathsf{RA}} = \langle \Sigma_{\mathsf{RA}}, M_{\mathsf{RA}} \rangle$

$$\Sigma^{S}_{\mathsf{RA}} = \{ \mathsf{Real} \} \qquad \Sigma^{F}_{\mathsf{RA}} = \{ +, -, *, \leq \} \cup \{ q \mid q \text{ is a decimal numeral} \}$$

All $\mathcal{I} \in M_{\mathsf{RA}}$ interpret Real as the set $\mathbb{R}$ of real numbers, and the function symbols in the usual way

Example 2: the theory of Ternary Strings $\mathcal{T}_{\mathsf{TS}} = \langle \Sigma_{\mathsf{TS}}, M_{\mathsf{TS}} \rangle$

$$\Sigma^{S}_{\mathsf{TS}} = \{ \mathsf{String} \} \qquad \Sigma^{F}_{\mathsf{TS}} = \{ \cdot, < \} \cup \{ \mathsf{a}, \mathsf{b}, \mathsf{c} \}$$

All $\mathcal{I} \in M_{\mathsf{TS}}$ interpret String as the set $\{ \mathsf{a}, \mathsf{b}, \mathsf{c} \}^*$ of all strings over the characters $\mathsf{a}, \mathsf{b}, \mathsf{c}$, and $\cdot$ as string concatenation (e.g., $(\mathsf{a} \cdot \mathsf{b})^{\mathcal{I}} = \mathsf{ab}$) and $<$ as alphabetical order

$\mathcal{T}$-interpretations

Let Σ and Ω be two signatures over a set X of variables where $\Omega \supseteq \Sigma$
(i.e., $\Omega^S \supseteq \Sigma^S$ and $\Omega^F \supseteq \Sigma^F$)

Let $\mathcal{I}$ be an Ω-interpretation over X

The *reduct* $\mathcal{I}^\Sigma$ *of* $\mathcal{I}$ *to* Σ is a Σ-interpretation over X obtained from $\mathcal{I}$
by restricting it to interpret only the symbols in Σ and X

Given a theory $\mathcal{T} := \langle \Sigma, M \rangle$,

a $\mathcal{T}$*-interpretation* is any Ω-interpretation $\mathcal{I}$ for some $\Omega \supseteq \Sigma$ such that $\mathcal{I}^\Sigma \in M$

Note: This definition allows us to consider the satisfiability in a theory
$\mathcal{T} := (\Sigma, M)$ of formulas that contain sorts or function symbols not in Σ

These symbols are usually called *uninterpreted* (in $\mathcal{T}$)

$\mathcal{T}$-interpretations

Example: Consider again $\mathcal{T}_{\mathsf{RA}} = \langle \Sigma_{\mathsf{RA}}, M_{\mathsf{RA}} \rangle$ where

$$\Sigma^{S}_{\mathsf{RA}} = \{ \mathsf{Real} \} \qquad \Sigma^{F}_{\mathsf{RA}} = \{ +, -, *, \leq \} \cup \{ q \mid q \text{ is a decimal numeral} \}$$

All $\mathcal{I} \in M_{\mathsf{RA}}$ interpret Real as $\mathbb{R}$ and the function symbols as usual

Which of the following interpretations are $\mathcal{T}_{RA}$-interpretations?

1. $\mathsf{Real}^{\mathcal{I}_1}$ is the rational numbers, symbols in Σ^{F}_{RA} interpreted as usual
2. $\mathsf{Real}^{\mathcal{I}_2} = \mathbb{R}$, symbols in Σ^{F}_{RA} interpreted as usual, and $\mathsf{String}^{\mathcal{I}_2} = \{ 0.5, 1.3 \}$
3. $\mathsf{Real}^{\mathcal{I}_3} = \mathbb{R}$, symbols in Σ^{F}_{RA} interpreted as usual, and $\log^{\mathcal{I}_3}$ is the successor function

$\mathcal{T}$-interpretations

Example: Consider again $\mathcal{T}_{\mathsf{RA}} = \langle \Sigma_{\mathsf{RA}}, M_{\mathsf{RA}} \rangle$ where

$$\Sigma^{S}_{\mathsf{RA}} = \{ \mathsf{Real} \} \qquad \Sigma^{F}_{\mathsf{RA}} = \{ +, -, *, \leq \} \cup \{ q \mid q \text{ is a decimal numeral} \}$$

All $\mathcal{I} \in M_{\mathsf{RA}}$ interpret Real as $\mathbb{R}$ and the function symbols as usual

Which of the following interpretations are $\mathcal{T}_{RA}$-interpretations?

1. $\mathsf{Real}^{\mathcal{I}_1}$ is the rational numbers, symbols in Σ^{F}_{RA} interpreted as usual ✗
2. $\mathsf{Real}^{\mathcal{I}_2} = \mathbb{R}$, symbols in Σ^{F}_{RA} interpreted as usual, and $\mathsf{String}^{\mathcal{I}_2} = \{ 0.5, 1.3 \}$
3. $\mathsf{Real}^{\mathcal{I}_3} = \mathbb{R}$, symbols in Σ^{F}_{RA} interpreted as usual, and $\log^{\mathcal{I}_3}$ is the successor function

$\mathcal{T}$-interpretations

Example: Consider again $\mathcal{T}_{\mathsf{RA}} = \langle \Sigma_{\mathsf{RA}}, M_{\mathsf{RA}} \rangle$ where

$$\Sigma^S_{\mathsf{RA}} = \{ \mathsf{Real} \} \qquad \Sigma^F_{\mathsf{RA}} = \{ +, -, *, \leq \} \cup \{ q \mid q \text{ is a decimal numeral} \}$$

All $\mathcal{I} \in M_{\mathsf{RA}}$ interpret Real as $\mathbb{R}$ and the function symbols as usual

Which of the following interpretations are $\mathcal{T}_{RA}$-interpretations?

1. $\mathsf{Real}^{\mathcal{I}_1}$ is the rational numbers, symbols in Σ^F_{RA} interpreted as usual ✗
2. $\mathsf{Real}^{\mathcal{I}_2} = \mathbb{R}$, symbols in Σ^F_{RA} interpreted as usual, and $\mathsf{String}^{\mathcal{I}_2} = \{ 0.5, 1.3 \}$ ✓
3. $\mathsf{Real}^{\mathcal{I}_3} = \mathbb{R}$, symbols in Σ^F_{RA} interpreted as usual, and $\log^{\mathcal{I}_3}$ is the successor function

$\mathcal{T}$-interpretations

Example: Consider again $\mathcal{T}_{\mathsf{RA}} = \langle \Sigma_{\mathsf{RA}}, M_{\mathsf{RA}} \rangle$ where

$$\Sigma^{S}_{\mathsf{RA}} = \{ \mathsf{Real} \} \qquad \Sigma^{F}_{\mathsf{RA}} = \{ +, -, *, \leq \} \cup \{ q \mid q \text{ is a decimal numeral} \}$$

All $\mathcal{I} \in M_{\mathsf{RA}}$ interpret Real as $\mathbb{R}$ and the function symbols as usual

Which of the following interpretations are $\mathcal{T}_{RA}$-interpretations?

1. $\mathsf{Real}^{\mathcal{I}_1}$ is the rational numbers, symbols in Σ^{F}_{RA} interpreted as usual ✗
2. $\mathsf{Real}^{\mathcal{I}_2} = \mathbb{R}$, symbols in Σ^{F}_{RA} interpreted as usual, and $\mathsf{String}^{\mathcal{I}_2} = \{ 0.5, 1.3 \}$ ✓
3. $\mathsf{Real}^{\mathcal{I}_3} = \mathbb{R}$, symbols in Σ^{F}_{RA} interpreted as usual, and $\log^{\mathcal{I}_3}$ is the successor function ✓

$\mathcal{T}$-satisfiability, $\mathcal{T}$-validity

Let $\mathcal{T} := \langle \Sigma, M \rangle$ be a theory

A formula α is *satisfiable in* $\mathcal{T}$, or $\mathcal{T}$*-satisfiable*,
if it is satisfied by **some** $\mathcal{T}$-interpretation $\mathcal{I}$

A set Γ of formulas $\mathcal{T}$*-entails* a formula α, written $\Gamma \models_{\mathcal{T}} \alpha$,
if every $\mathcal{T}$-interpretation that satisfies all formulas in Γ satisfies α as well

An formula α is *valid in* $\mathcal{T}$, or $\mathcal{T}$*-valid*, written $\models_{\mathcal{T}} \alpha$,
if it is satisfied by **all** $\mathcal{T}$-interpretations

Note: α is valid in $\mathcal{T}$ iff $\{\ \} \models_{\mathcal{T}} \alpha$

$\mathcal{T}$-satisfiability, $\mathcal{T}$-validity

Exercise: Which of the following Σ_{RA}-formulas is satisfiable or valid **in** $\mathcal{T}_{\mathsf{RA}}$?

1. $(x_0 + x_1 \leq 0.5) \wedge (x_0 - x_1 \leq 2)$
2. $\forall x_0.((x_0 + x_1 \leq 1.7) \implies (x_1 \leq 1.7 - x_0))$
3. $\forall x_0.\forall x_1.(x_0 + x_1 \leq 1)$

Note: For every signature Σ, entailment and validity in FOL can be reframed as entailment and validity in the theory $\mathcal{T}_{\mathsf{FOL}} = \langle \Sigma, M_{\mathsf{FOL}} \rangle$ where M_{FOL} is the class of **all** Σ-interpretations

$\mathcal{T}$-satisfiability, $\mathcal{T}$-validity

Exercise: Which of the following Σ_{RA}-formulas is satisfiable or valid **in** $\mathcal{T}_{\mathsf{RA}}$?

1. $(x_0 + x_1 \leq 0.5) \wedge (x_0 - x_1 \leq 2)$ satisfiable, **not valid**
2. $\forall x_0.((x_0 + x_1 \leq 1.7) \implies (x_1 \leq 1.7 - x_0))$
3. $\forall x_0.\forall x_1.(x_0 + x_1 \leq 1)$

$\mathcal{T}$-satisfiability, $\mathcal{T}$-validity

Exercise: Which of the following Σ_{RA}-formulas is satisfiable or valid **in** $\mathcal{T}_{\mathsf{RA}}$?

1. $(x_0 + x_1 \leq 0.5) \wedge (x_0 - x_1 \leq 2)$ — satisfiable, **not valid**
2. $\forall x_0.((x_0 + x_1 \leq 1.7) \implies (x_1 \leq 1.7 - x_0))$ — satisfiable, valid
3. $\forall x_0.\forall x_1.(x_0 + x_1 \leq 1)$

$\mathcal{T}$-satisfiability, $\mathcal{T}$-validity

Exercise: Which of the following Σ_{RA}-formulas is satisfiable or valid **in** $\mathcal{T}_{\mathsf{RA}}$?

1. $(x_0 + x_1 \leq 0.5) \wedge (x_0 - x_1 \leq 2)$ — satisfiable, **not valid**
2. $\forall x_0.((x_0 + x_1 \leq 1.7) \implies (x_1 \leq 1.7 - x_0))$ — satisfiable, valid
3. $\forall x_0.\forall x_1.(x_0 + x_1 \leq 1)$ — **not satisfiable**, **not valid**

Note: For every signature Σ, entailment and validity in FOL can be reframed as entailment and validity in the theory $\mathcal{T}_{\mathsf{FOL}} = \langle \Sigma, M_{\mathsf{FOL}} \rangle$ where M_{FOL} is the class of **all** Σ-interpretations

Alternative definition of theory

A theory $\mathcal{T}$ is defined by a signature Σ and a set $\mathcal{A}$ of Σ-**sentences**, or *axioms*

In particular, an Ω-formula α is *valid* in this kind of theory if every Ω-interpretation $\mathcal{I}$ that satisfies $\mathcal{A}$ also satisfies α

We refer to such theories as *(first-order) axiomatic theories* These notions of

theory and validity are a **special case** of those in the previous slides

Given a theory $\mathcal{T}$ defined by Σ and $\mathcal{A}$, we define a theory $\mathcal{T}' := \langle \mathcal{T}, M \rangle$ where M is the class of all Σ-interpretations that satisfy $\mathcal{A}$

It is not hard to show that a formula α is valid in $\mathcal{T}$ **iff** it is valid in $\mathcal{T}'$

In fact, they are strictly less general since **not all theories are first-order axiomatizable**

Alternative definition of theory

Example

Consider the theory $\mathcal{T}_{\mathsf{Nat}}$ of the natural numbers, with signature Σ where $\Sigma^S = \{\,\mathsf{Nat}\,\}$,
$\Sigma^F = \{\,0, \mathsf{S}, +, <\,\}$, and $M = \{\,\mathcal{I}\,\}$ where $\mathsf{Nat}^{\mathcal{I}} = \mathbb{N}$ and Σ^F is interpreted as usual

Alternative definition of theory

Example

Consider the theory $\mathcal{T}_{\mathsf{Nat}}$ of the natural numbers, with signature Σ where
$\Sigma^S = \{\, \mathsf{Nat} \,\}$,
$\Sigma^F = \{\, 0, \mathsf{S}, +, < \,\}$, and $M = \{\, \mathcal{I} \,\}$ where $\mathsf{Nat}^{\mathcal{I}} = \mathbb{N}$ and Σ^F is interpreted as usual

Any set of axioms for this theory is satisfied by *non-standard models*, e.g., interpretations $\mathcal{I}$ where
$\mathsf{Nat}^{\mathcal{I}}$ includes other chains of elements besides the natural numbers

Alternative definition of theory

Example

Consider the theory $\mathcal{T}_{\mathsf{Nat}}$ of the natural numbers, with signature Σ where
$\Sigma^S = \{\, \mathsf{Nat} \,\}$,
$\Sigma^F = \{\, 0, \mathsf{S}, +, < \,\}$, and $M = \{\, \mathcal{I} \,\}$ where $\mathsf{Nat}^{\mathcal{I}} = \mathbb{N}$ and Σ^F is interpreted as usual

Any set of axioms for this theory is satisfied by *non-standard models*, e.g., interpretations $\mathcal{I}$ where
$\mathsf{Nat}^{\mathcal{I}}$ includes other chains of elements besides the natural numbers

These models **falsify** formulas that are **valid** in $\mathcal{T}_{\mathsf{Nat}}$ (e.g., $\neg\exists x.\, x < 0$ or $\forall x.\, (x \doteq 0 \vee \exists y.\, x \doteq \mathsf{S}(y))$)

Completeness of theories

A Σ-theory $\mathcal{T}$ is *complete* if for every Σ-**sentence** α, either α or $\neg\alpha$ is valid in $\mathcal{T}$

Note: In a complete Σ-theory, every Σ-sentence is either **valid** or **unsatisfiable**

Completeness of theories

Example 1:

Any theory $\mathcal{T} = \langle \Sigma, M \rangle$ where all the interpretations in M only differ in how they interpret the variables (e.g., $\mathcal{T}_{\mathrm{RA}}$) is **complete**

Example 2:

The axiomatic (mono-sorted) theory of *monoids* with $\Sigma^F = \{ \cdot, \epsilon \}$ and axioms

$$\forall x. \forall y. \forall z. (x \cdot y) \cdot z \doteq x \cdot (y \cdot z) \qquad \forall x. x \cdot \epsilon \doteq x \qquad \forall x. \epsilon \cdot x \doteq x$$

is **incomplete**. For instance, the sentence $\forall x. \forall y. x \cdot y \doteq y \cdot x$ is true in some monoids (e.g., the integers with addition) but **false** in others (e.g., the strings with concatenation)

Completeness of theories

Example 3: The axiomatic (mono-sorted) theory of *dense linear orders without endpoints* with $\Sigma^F = \{ \prec \}$ and axioms

$$\forall x. \forall y. (x \prec y \implies \exists z. (x \prec z \wedge z \prec y)) \qquad \text{(dense)}$$

$$\forall x. \forall y. (x \prec y \vee x \doteq y \vee y \prec x) \qquad \text{(linear)}$$

$$\forall x. \neg(x \prec x) \qquad \forall x. \forall y. \forall z. (x \prec y \wedge y \prec z \implies x \prec z) \qquad \text{(orders)}$$

$$\forall x. \exists y. y \prec x \qquad \forall x. \exists y. x \prec y \qquad \text{(without endpoints)}$$

is **complete**

Decidability

Recall: We say that a set A is *decidable* if there exists a **terminating** procedure
that, for every input element a, returns **yes** if $a \in A$ and **no** otherwise

A theory $\mathcal{T} := \langle \Sigma, M \rangle$ is *decidable* if the set of all Σ-formulas **valid in** $\mathcal{T}$ is decidable

A *fragment* of $\mathcal{T}$ is a **syntactically-restricted subset** of the Σ-formulas valid in $\mathcal{T}$

Decidability

Recall: We say that a set A is *decidable* if there exists a **terminating** procedure
that, for every input element a, returns **yes** if $a \in A$ and **no** otherwise

A theory $\mathcal{T} := \langle \Sigma, M \rangle$ is *decidable* if the set of all Σ-formulas **valid in** $\mathcal{T}$ is decidable

A *fragment* of $\mathcal{T}$ is a **syntactically-restricted subset** of the Σ-formulas valid in $\mathcal{T}$

Example 1: The *quantifier-free* fragment of $\mathcal{T}$ is the set of all quantifier-free formulas valid in $\mathcal{T}$

Example 2: The *linear* fragment of $\mathcal{T}_{\text{RA}}$ is the set of all Σ_{RA}- valid in $\mathcal{T}$ that do not contain multiplication $(*)$

Axiomatizability

A theory $\mathcal{T} = \langle \Sigma, M \rangle$ is *recursively axiomatizable* if M is the class of all interpretations satisfying a **decidable set** of (first-order) axioms $\mathcal{A}$

Lemma 1:
Every recursively axiomatizable theory $\mathcal{T}$ admits a procedure $E_{\mathcal{T}}$ that **enumerates** all formulas valid in $\mathcal{T}$

Theorem 1:
For every **complete** and **recursively axiomatizable** theory $\mathcal{T}$, validity in $\mathcal{T}$ is decidable

Proof:
Given a formula α, we use $E_{\mathcal{T}}$ to enumerate all valid formulas. Since $\mathcal{T}$ is complete, either α or $\neg\alpha$ will eventually be produced by $E_{\mathcal{T}}$.

Common theories in Satisfiability Modulo Theories

As a branch of Automated Reasoning, SMT has traditionally **focused** on theories with **decidable quantifier-free fragment**

SMT is it concerned with the **(un)satisfiability** of formulas in a theory $\mathcal{T}$, but recall that a formula α is $\mathcal{T}$-valid iff $\neg\alpha$ is $\mathcal{T}$-unsatisfiable

In the rest of the course, we will study

- a few of those theories and their decision procedures
- proof systems to reason modulo theories automatically

From quantifier-free formulas to conjunctions of literals

As in PL, thanks to DNF transformations,

the satisfiability of quantifier-free formulas in a theory $\mathcal{T}$ is decidable **iff** the satisfiability in $\mathcal{T}$ of **conjunctions of literals** is decidable

In fact, we will study a general **extension** of CDCL to **SMT** that uses decision procedures for conjunctions of literals

So, we will mostly **focus** on **conjunctions of literals**

Theory of Uninterpreted Functions: $\mathcal{T}_{\text{EUF}}$

Given a signature Σ, the most general theory consists of the class of **all** Σ-interpretations

This is really **a family** of theories parameterized by the signature Σ

It is known as the theory of *Equality with Uninterpreted Functions (*EUF*)*, or the *empty theory* since it is axiomatized by the empty set of formulas

Validity, and so satisfiability, in $\mathcal{T}_{\text{EUF}}$ is only **semi-decidable** (as it is just validity in FOL)

However, the satisfiability of conjunctions of $\mathcal{T}_{\text{EUF}}$-literals is **decidable**, in polynomial time, with a **congruence closure** algorithm

Theory of Uninterpreted Functions: $\mathcal{T}_{\mathsf{EUF}}$

Example: $a \doteq b \ \wedge \ f(a) \doteq b \ \wedge \ \neg(g(a) \doteq g(f(a)))$

Is this formula satisfiable in $\mathcal{T}_{\mathsf{EUF}}$?

Theory of Real Arithmetic: $\mathcal{T}_{RA}$

$\Sigma^S = \{ \text{Real} \}$

$\Sigma^F = \{ +, -, *, \leq \} \cup \{ q \mid q \text{ is a decimal numeral} \}$

M is the class of interpretations that interpret Real as the set of real numbers, and the function symbols in the usual way

Satisfiability in the full $\mathcal{T}_{RA}$ is **decidable** (but in worst-case doubly-exponential time)

Restricted fragments can be decided more efficiently

Theory of Real Arithmetic: $\mathcal{T}_{RA}$

Example: quantifier-free **linear real arithmetic** (QF_LRA): $*$ can only appear if at least one pf its two arguments is a decimal numeral

The satisfiability of conjunctions of literals in QF_LRA is decidable in polynomial time

Theory of Integer Arithmetic: $\mathcal{T}_{\mathsf{IA}}$

$\Sigma^S = \{\,\mathsf{Int}\,\}$

$\Sigma^F = \{\,+, -, *, \leq\,\} \cup \{\,n \mid \text{ n is a numeral}\,\}$

M is the class of interpretations that interpret Int as the set of integers numbers, and the function symbols in the usual way

Satisfiability in $\mathcal{T}_{\mathsf{IA}}$ is **not even semi**-decidable!

Satisfiability of quantifier-free Σ-formulas in $\mathcal{T}_{\mathsf{IA}}$ is **undecidable** as well

Linear integer arithmetic (LIA) (aka., *Presburger arithmetic*) is decidable, but not efficiently (worst case triply-exponential)

Theory of Arrays with Extensionality: $\mathcal{T}_{\mathrm{A}}$

$\Sigma^S = \{ A, I, E \}$ (for **arrays**, **indices**, **elements**)

$\Sigma^F = \{ \mathrm{read}, \mathrm{write} \}$, where $\mathrm{rank}(\mathrm{read}) = \langle A, I, E \rangle$ and $\mathrm{rank}(\mathrm{write}) = \langle A, I, E, A \rangle$

Useful for modeling RAM or array data structures

Let a, a' be variables of sort A, and i and v variables of sort I and E, respectively

- $\mathrm{read}(a, i)$ denotes the value stored in array a at position i
- $\mathrm{write}(a, i, v)$ denotes the array that stores value v at position i and is otherwise identical to a

Theory of Arrays with Extensionality: $\mathcal{T}_{\mathsf{A}}$

Example 1: $\mathsf{read}(\mathsf{write}(a, i, v), i) \doteq_E v$

Intuitively, is the above formula valid/satisfiable/unsatisfiable in $\mathcal{T}_{\mathsf{A}}$?

Example 2: $\forall i.\, \mathsf{read}(a, i) \doteq_E \mathsf{read}(a', i) \implies a \doteq_A a'$

Intuitively, is the above formula valid/satisfiable/unsatisfiable in $\mathcal{T}_{\mathsf{A}}$?

Theory of Arrays with Extensionality: $\mathcal{T}_{\mathrm{A}}$

$\mathcal{T}_{\mathrm{A}}$ is finitely axiomatizable

M is the class of interpretations that satisfy the following axioms:

1. $\forall a.\, \forall i.\, \forall v.\, \mathsf{read}(\mathsf{write}(a, i, v), i) \doteq v$
2. $\forall a.\, \forall i.\, \forall i'.\, \forall v.\, (\neg(i \doteq i') \implies \mathsf{read}(\mathsf{write}(a, i, v), i') \doteq \mathit{read}(a, i'))$
3. $\forall a.\, \forall a'.\, (\forall i.\mathsf{read}(a, i) \doteq \mathsf{read}(a', i) \implies a \doteq a')$

Note: Axiom 3 can be omitted to obtain a theory of arrays **without extensionality**

Satisfiability in $\mathcal{T}_{\mathrm{A}}$ is **undecidable**

But there are several decidable fragments, as we will see