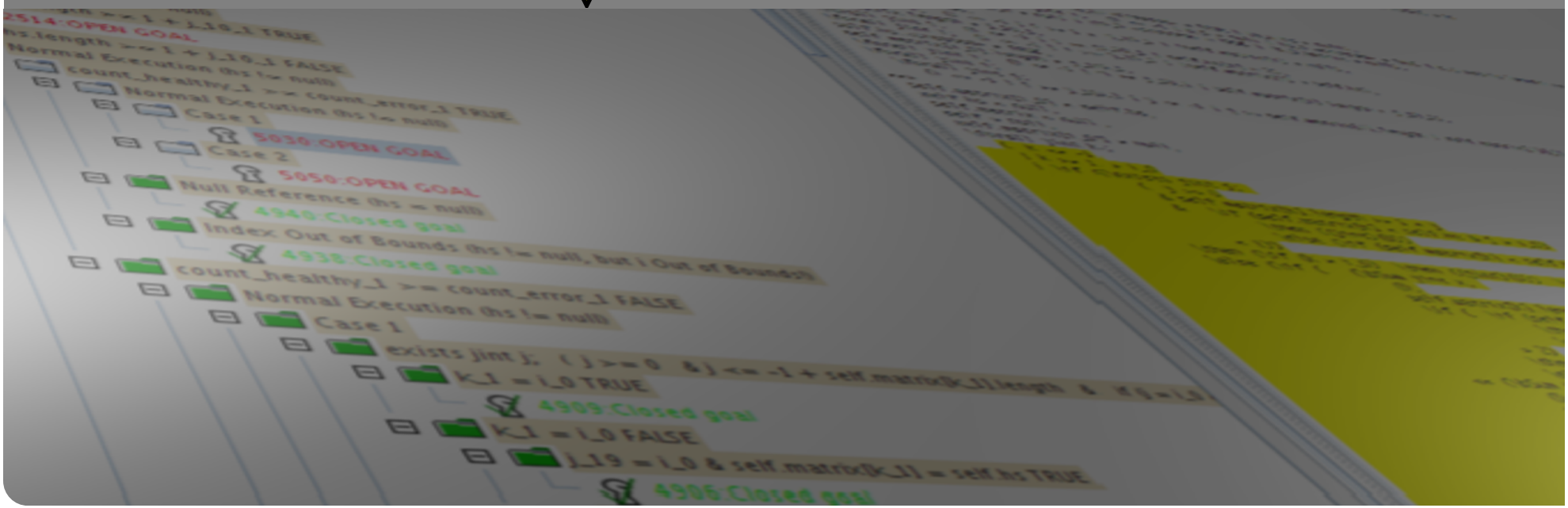
Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2018/2019

Theory Reasoning (Theorie-Schließen) · Folien von M. Ulbrich

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK



www.kit.edu

Satisfiability Modulo Theories – Introduction

Different Questions to Ask

Question so far in this lecture ...

Question: Is formula ϕ valid / satisfiable / unsatisfiable
(in all structures/models)

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

New question ...

Question: Is formula ϕ valid / satisfiable / unsatisfiable
in structures with certain properties
(typically: with fixed interpretation for symbols)

- $\exists x.\ 2 \cdot x^2 - x - 1 = 0 \wedge x < 0$ 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**: $T \not\models \mathit{false}$

Note:
T consistent iff T has a model
T consistent iff $\mathit{false} \notin T$ (because T closed)

Theories: Basic Definitions

- A FOL structure (D, I) is 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 T-satisfiable if it has a T-model.
- $\psi \in Fml_\Sigma$ is T-valid if every T-structure is a T-model of ψ. (Note: $T \models \psi \iff \psi \in T$)
- T is complete if: $\phi \in T$ or $\neg\phi \in T$ for all $\phi \in Fml_\Sigma$
- $\models_T$ is used instead of $T \models$: $S \models_T \phi$ defined as $S \cup T \models \phi$

Defining Theories

Axiomatisation

A theory T may be defined by a **set** $Ax \subset Fml_\Sigma$ **of axioms**.
T is the consequential closure of Ax:

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

(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):

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

Discussion

- Every theory $\mathcal{T}(D, I)$ is complete.

Discussion

- Every theory $\mathcal{T}(D, I)$ is complete.
- If Ax is recursively enumerable,
  then $\mathcal{T}(Ax)$ is recursively enumerable

Discussion

- Every theory $\mathcal{T}(D, I)$ is complete.
- If Ax is recursively enumerable,
  then $\mathcal{T}(Ax)$ is recursively enumerable
- Even if Ax is finite or decidable,
  $\mathcal{T}(Ax)$ is, in general, not decidable.

Discussion

- Every theory $\mathcal{T}(D, I)$ is complete.
- If Ax is recursively enumerable,
  then $\mathcal{T}(Ax)$ is recursively enumerable
- Even if Ax is finite or decidable,
  $\mathcal{T}(Ax)$ is, in general, not decidable.
- There are (D, I) such that $\mathcal{T}(D, I)$ is not rec. enum.
  (and, thus, not axiomatisable with a rec. enum. Ax)

Discussion

- Every theory $\mathcal{T}(D, I)$ is complete.
- If Ax is recursively enumerable,
  then $\mathcal{T}(Ax)$ is recursively enumerable
- Even if Ax is finite or decidable,
  $\mathcal{T}(Ax)$ is, in general, not decidable.
- There are (D, I) such that $\mathcal{T}(D, I)$ is not rec. enum.
  (and, thus, not axiomatisable with a rec. enum. Ax)
- (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.
NOTE: Therefore, free variables in T-SAT problems behave like constants. In difference to that, so far, we treated free variables mostly as being implicitly universally quantified

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 "$\doteq$" replaced by uninterpred "$\approx$".

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

Axioms for Equality

Axioms Eq_Σ:

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

Axioms for Equality

Axioms Eq_Σ:

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

- $\forall x_1, x_1, \ldots, x_n, x'_n.$
  $x_1 \approx x'_1 \wedge \ldots \wedge x_n \approx x'_n \rightarrow f(x_1, ..., x_n) \approx f(x'_1, \ldots, x'_n)$
  for any function f in Σ with arity n. (Congruency)

Axioms for Equality

Axioms Eq_Σ:

- $\forall x.\ x \approx x$ (Reflexivity)
- $\forall x_1, x_1, \ldots, x_n, x'_n.$
  $x_1 \approx x'_1 \wedge \ldots \wedge x_n \approx x'_n \rightarrow f(x_1, ..., x_n) \approx f(x'_1, \ldots, x'_n)$
  for any function f in Σ with arity n. (Congruency)
- $\forall x_1, x_1, \ldots, x_n, x'_n.$
  $x_1 \approx x'_1 \wedge \ldots \wedge x_n \approx x'_n \rightarrow p(x_1, ..., x_n) \leftrightarrow p(x'_1, \ldots, x'_n)$
  for any predicate p in Σ with arity n. (Congruency)
  (This includes predicate $\approx$)

Axioms for Equality

Axioms Eq_Σ:

- $\forall x.\ x \approx x$ (Reflexivity)
- $\forall x_1, x_1, \ldots, x_n, x'_n.$
  $x_1 \approx x'_1 \wedge \ldots \wedge x_n \approx x'_n \rightarrow f(x_1, ..., x_n) \approx f(x'_1, \ldots, x'_n)$
  for any function f in Σ with arity n. (Congruency)
- $\forall x_1, x_1, \ldots, x_n, x'_n.$
  $x_1 \approx x'_1 \wedge \ldots \wedge x_n \approx x'_n \rightarrow p(x_1, ..., x_n) \leftrightarrow p(x'_1, \ldots, x'_n)$
  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)

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

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

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 F within which a certain amount of elementary arithmetic can be carried out is incomplete."

Natural number arithmetic is not axiomatisable with a rec. enum. set of axioms

Peano Arithmetic

Natural number arithmetic is not axiomatisable . . .
Let's **approximate**.

The Peano Axioms *PA*

1. $\forall x(x + 1 \neq 0)$
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. $\forall x(x * 0 \doteq 0)$
6. $\forall x \forall y(x * (y + 1) \doteq (x * y) + x)$

Peano Arithmetic

Natural number arithmetic is not axiomatisable . . .
Let's **approximate**.

The Peano Axioms *PA*

1. $\forall x(x + 1 \neq 0)$
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. $\forall x(x * 0 \doteq 0)$
6. $\forall x \forall y(x * (y + 1) \doteq (x * y) + x)$
7. For any $\phi \in Fml_{\Sigma_{\mathcal{N}}}$
   $(\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x + 1))) \rightarrow \forall x(\phi)$

Peano Arithmetic

Natural number arithmetic is not axiomatisable . . .
Let's **approximate**.

The Peano Axioms *PA*

1. $\forall x(x + 1 \neq 0)$
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. $\forall x(x * 0 \doteq 0)$
6. $\forall x \forall y(x * (y + 1) \doteq (x * y) + x)$
7. For any $\phi \in Fml_{\Sigma_{\mathcal{N}}}$
   $(\phi(0) \land \forall x(\phi(x) \rightarrow \phi(x + 1))) \rightarrow \forall x(\phi)$

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

Peano Arithmetic

- Peano arithmetic approximates natural arithmetic.

Peano Arithmetic

- Peano arithmetic approximates natural arithmetic.
- More $\mathcal{T}(PA)$-models than $\mathcal{T}(\mathcal{N})$-models

Peano Arithmetic

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

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.

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:

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.

Presburger Arithmetic

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

The Presburger Axioms P

1. $\forall x(x + 1 \neq 0)$
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).

Presburger Arithmetic

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

The Presburger Axioms P

1. $\forall x(x + 1 \neq 0)$
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:

$3 \stackrel{def}{=} 1 + 1 + 1$, $\quad 3x \stackrel{def}{=} x + x + x$, $\quad$ 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!

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!

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

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

is T-equivalent to a quantifier-free formula

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

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

Quantifier Elimination

Definition

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

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

is T-equivalent to a quantifier-free formula

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

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

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.

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

Karlsruhe Institute of Technology

Does Presburger Arithmetic admit QE?

Presburger and Quantifier Elimination

Does Presburger Arithmetic admit QE?

Almost ... However

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

Presburger and Quantifier Elimination

Does Presburger Arithmetic admit QE?

Almost ... However

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

Add predicates: $\{k|\cdot : k \in \mathbb{N}_{>0}\}$ "k divides ..."

$\exists x.y = x + x \leftrightarrow 2|y$ is P-valid

Presburger Arithmetic with divisibility admits QE.

$\rightsquigarrow$ Cooper's algorithm

Real arithmetic is decidable

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

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).

Real arithmetic is decidable

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

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).

Real arithmetic is decidable

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

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)

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

Combining Theories

Combining Theories

What if we have two (or more) theories within one formula?

$$f(a) = g(a+1) \ \wedge \ g(a+b) > f(a) \quad \textit{satisfiable}?$$

Decision procedures exist for linear integers, and for uninterpreted functions.

Goal

Find decision procedures for combinations of theories.

Combinations of theories

Let $T_1 \subseteq Fml_{\Sigma_1}$ and $T_2 \subseteq Fml_{\Sigma_2}$ be theories.
The combined theory $T_{1,2} \in Fml_{\Sigma_1 \cup \Sigma_2}$ is defined as:

$$T_{1,2} \stackrel{\text{def}}{=} \mathcal{T}(T_1 \cup T_2)$$

Purification

$$f(a) = g(a+1) \ \wedge \ g(a+b) > f(a) \tag{1}$$

Purification

Extract expressions using fresh constants and equalities.
Make each atomic formula belong to one theory only.

$$f(a) = g(y) \wedge y = a + 1 \wedge$$
$$z = g(u) \wedge u = a + b \wedge w = f(a) \wedge z > w$$

is equisatisfiable to (1).

Note: This resembles the construction of the "short CNF".

Convex Theories

Definition

A Σ theory T is convex if for every conjunctive $\varphi \in Fml_\Sigma$

$$(\varphi \rightarrow \bigvee_{i=1} x_i = y_i) \text{ is } T\text{-valid for some finite } n > 1$$
$$\text{implies that}$$
$$(\varphi \rightarrow x_i = y_i) \text{ is } T\text{-valid for some } i \in \{1, \ldots, n\}$$

where x_i, y_i, for $i \in \{1, \ldots, n\}$, are variables.

Examples:

- Linear arithmetic over $\mathbb{R}$ is convex.
- Linear arithmetic over $\mathbb{N}$ is **not** convex:

$$x_1 = 1 \wedge x_2 = 2 \wedge 1 \leq x_3 \wedge x_3 \leq 2 \rightarrow (x_3 = x_1 \vee x_3 = x_2)$$

Nelson-Oppen Combination Procedure

In order for the Nelson–Oppen procedure to be applicable, the theories T_1, T_2 must comply with the following restrictions:

1. T_1, T_2 are quantifier-free first-order theories with equality.
2. There is a decision procedure for each of the theories
3. The signatures are disjoint, i.e., for all $\Sigma_1 \cap \Sigma_2 = \emptyset$
4. T_1, T_2 are theories are *stably infinite*: Every T-satisfiable formula has an infinite model (e.g., linear arithmetic over $\mathbb{R}$, but not the theory of finite-width bit vectors).

(Generalisation to more than two theories: simple, see literature)

Example

Example 10.7. Consider the formula

$$\begin{array}{c}(f(x_1,0) \geq x_3) \wedge (f(x_2,0) \leq x_3) \wedge \\ (x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge \\ (x_3 - f(x_1,0) \geq 1)\,,\end{array} \tag{10.12}$$

which mixes linear arithmetic and uninterpreted functions. Purification results in

$$\begin{array}{l}(a_1 \geq x_3) \wedge (a_2 \leq x_3) \wedge (x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge (x_3 - a_1 \geq 1) \wedge \\ (a_0 = 0) \wedge \\ (a_1 = f(x_1, a_0)) \wedge \\ (a_2 = f(x_2, a_0))\,.\end{array} \tag{10.13}$$

from: D. Kröning, O.Strichman: *Decision Procedures*, Springer Verlag

Example

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$	$a_1 = f(x_1, a_0)$
$a_2 \leq x_3$	$a_2 = f(x_2, a_0)$
$x_1 \geq x_2$	
$x_2 \geq x_1$	
$x_3 - a_1 \geq 1$	
$a_0 = 0$	
$\star\ x_1 = x_2$	$x_1 = x_2$
$a_1 = a_2$	$\star\ a_1 = a_2$
$\star\ a_1 = x_3$	
$\star$ FALSE	

Nelsson-Oppen Algorithm – convex case

T_1, T_2 convex theories with with the Nelsson-Oppen properties.
Assume convex (conjunctive) problem.

τ bridges between T_1 and T_2 and is a conjunction of equalities over variables

After purification: $\varphi_1 \in Fml_1$, $\varphi_2 \in Fml_2$, $\tau \subseteq Fml_=$

1. If $\varphi_1 \wedge \bigwedge \tau$ is T_1-unsatisfiable, return **UNSAT**
2. If $\varphi_2 \wedge \bigwedge \tau$ is T_2-unsatisfiable, return **UNSAT**
3. "learn" new equalities:
$$\tau := \tau \cup \bigcup\{x = y \mid \varphi_1 \wedge \tau \rightarrow x = y \text{ is } T_1\text{-valid}\} \cup \bigcup\{x = y \mid \varphi_2 \wedge \tau \rightarrow x = y \text{ is } T_2\text{-valid}\}$$
4. If nothing was "learnt", return **SAT**
5. Go to 1

Soundness

This algorithm is a decision procedure for $T_{1/2}$.

To show: $\varphi_1 \wedge \varphi_2$ is satisfiable $\iff$ algorithm returns **SAT** .

Proof sketch on blackboard

see also: D. Kröning, O. Strichman: *Decision Procedures*, Springer Verlag. Section 10.3.3.

Non-convex theories

1. If $\varphi_1 \wedge \tau$ is T_1-unsatisfiable, return **UNSAT**
2. If $\varphi_2 \wedge \tau$ is T_2-unsatisfiable, return **UNSAT**
3. "learn" new equalities:
   $$\tau := \tau \wedge \bigwedge\{x = y \mid \varphi_1 \wedge \tau \rightarrow x = y \text{ is } T_1\text{-valid}\} \wedge \bigwedge\{x = y \mid \varphi_2 \wedge \tau \rightarrow x = y \text{ is } T_2\text{-valid}\}$$
4. If nothing was "learnt", **split**: If there exists i such that
   - $\varphi_i \rightarrow (x_1 = y_1 \vee \ldots \vee x_k = y_k)$ and
   - $\varphi_i \not\rightarrow (x_j = y_j)$

   then apply Nelson–Oppen recursively to adding $x_i = y_i$ to the different τ.
   If any of these subproblems is satisfiable, return "Satisfiable".
   Otherwise, return "Unsatisfiable".