

# Formale Systeme II: Theorie

## Theories

SS 2018

Prof. Dr. Bernhard Beckert · Dr. Mattias Ulbrich

# Theories and Satisfiability – Introduction

## Deciding logics

**Question:** Is formula  $\phi$  valid, i.e.,  $\phi$  satisfied in all possible structures.

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

## Deciding theories

**Question:** Is formula  $\phi$  satisfied structures with fixed interpretation for symbols.

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

Given a FOL signature  $\Sigma$

$Fml_{\Sigma}$  ... set of closed FOL-formulas over  $\Sigma$ .

## 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  $\phi \in T$

- 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  $\psi$ .  
 $\iff T \models \psi \iff \psi \in T$
- $T$  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  $S \cup T \models \phi$

## 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:

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

- 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)

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  $FV(\phi_2) = \{x\}$

$Fml_{\Sigma}^o \supset Fml_{\Sigma}$  ... set of **open** formulas

## Existential closure $\exists[\cdot]$

For  $\phi \in Fml_{\Sigma}^o$  with  $FV = \{x_1, \dots, x_n\}$  define:

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

$\phi \in Fml_{\Sigma}^o$  is called **T-satisfiable** if  $\exists[\phi]$  is T-satisfiable.



## Theorem

Equality can be axiomatised in first order logic.

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

$\phi^{\approx}$  is formula  $\phi$  with interpreted “=” replaced by uninterpreted “ $\approx$ ”.

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

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

## Axioms $Eq_{\Sigma}$ :

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

Symmetry and transitivity of  $\approx$  are consequences of  $Eq_{\Sigma}$

$\rightsquigarrow$  Exercise

## 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

A decision procedure  $DP_T$  for a theory  $T$  is a deterministic algorithm that always terminates.

It takes a formula  $\phi$  as input and returns SAT if  $\phi$  is  $T$ -satisfiable, UNSAT otherwise.

### N.B.:

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

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

## Standard model of natural numbers

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

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

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

$\mathcal{T}(\mathcal{N})$  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 (w/ a r.e. set of axioms)

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  $\phi \in Fml_{\Sigma_{\mathcal{N}}}$   
 $(\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x + 1))) \rightarrow \forall x(\phi)$

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



- Peano arithmetic approximates natural arithmetic.
  - More  $\mathcal{T}(PA)$ -models than  $\mathcal{T}(\mathcal{N})$ -models
  - $\mathcal{T}(PA)$  is not complete.
- ⇒ 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,  $266 = 2^{2^3} + 2^{2^1+1} + 2^1$ .) Repeat with exponents of exponents and so on until the representation stabilizes. For example, 266 stabilizes at the representation  $2^{2^{2^1+1}} + 2^{2^1+1} + 2^1$ .

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,  $G_2(266) = 3^{3^{3^1+1}} + 3^{3^1+1} + 2$ .)

Now define the Goodstein sequence for  $m$  starting at 2 by

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

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)

Theory	QF-SAT	SAT
Equality	YES	YES
Uninterpreted functions	YES	co-SEMI
Integer arithmetic	NO <sup>1</sup>	NO
Linear arithmetic		
Real arithmetic		
Bitvectors	YES	YES
Floating points	YES	YES

<sup>1</sup> Yuri Matiyasevich. Enumerable sets are diophantine. Journal of Sovietic Mathematics, 1970.

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:

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

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!

## Definition

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

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

is  $T$ -equivalent to a quantifier-free formula

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

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

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

## Lemma

If  $T$  admits QE for any formula

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

with  $\phi_i$  literals, then  $T$  admits QE for any formula in  $Fml^\circ$ .

Literal: atomic formula or a negation of one.

**Proof:** (Easy) exercise.



Does Presburger Arithmetic admits 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 ... Blackboard

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

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

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  $\psi$  such that  $(\exists x. \varphi(x, y)) \leftrightarrow \psi(y)$ .

Computer algebra systems do this: REDLOG, Mathematica, (Z3)

## Real arithmetic has a **finite** axiomatisation $R$

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

$$\forall x, y, z. (x + y) + z = x + (y + z) \quad \forall x, y, z. (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$\forall x, y. x + y = y + x \quad \forall x, y. x \cdot y = y \cdot x$$

$$\forall x. x + 0 = x \wedge 0 + x = x \quad \forall x. x \cdot 1 = x \wedge 1 \cdot x = x$$

$$\forall x. x + (-x) = 0 \wedge (-x) + x = 0$$

- **Distributive Laws**

$$\forall x, y, z. (x + y) \cdot z = x \cdot z + y \cdot z \quad \wedge \quad z \cdot (x + y) = z \cdot x + z \cdot y$$

- **Ordering**

$$\forall x, y, z. x \leq y \rightarrow x + z \leq y + z$$

$$\forall x, y. 0 \leq x \wedge 0 \leq y \rightarrow 0 \leq xy$$

$\mathcal{T}(\mathbb{R}) = \mathcal{T}(R)$  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 set

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

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

## Observation:

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

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

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

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

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

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

## Tarski-Seidenberg Theorem (*Projektionssatz*)

Let  $S \subseteq \mathbb{R}^n$  be semialgebraic.

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



## 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  $a, b, c$ .

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

$$\iff$$

$$(a \neq 0 \wedge b^2 - 4ac \geq 0)$$

$$\vee (a = 0 \wedge (b = 0 \rightarrow c = 0))$$

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

① Sufficient to look at  $\exists x. \bigwedge_i \phi_i(\bar{y}, x)$  for atomic  $\phi_i$ . → Exercise

② Sufficient to consider  $\phi_i$  of shape  $p(\bar{y}, x) \begin{cases} < \\ > \\ = \end{cases} 0$   
for  $p \in \mathbb{R}[\bar{y}][x]$  → Why?

③ Every polynomial  $p \in R[x]$  has finitely many connected regions with same sign. → Board  
Choose a set  $Rep$  of representatives.

$$\textcircled{4} \quad \exists x. \bigwedge_i \phi_i(x, \bar{y}) \leftrightarrow \bigvee_{r \in Rep} \bigwedge_i \phi_i(r, \bar{y})$$

## Decision Technique

Cylindrical Algebraic Decomposition (CAD)

# Quantifier Elimination – Linear Example

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

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

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

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

**For the example:**

$$\begin{aligned} \psi &\leftrightarrow \bigvee_{r \in \text{Rep}} r > 2 \wedge r < 3 \wedge x > z \\ &\leftrightarrow 2.5 > z \vee (z > 2 \wedge z < 4 \wedge 2 > z) \vee (z > 1 \wedge z < 3 \wedge 3 > z) \\ &\leftrightarrow z < 3 \end{aligned}$$

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

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

Consider  $\Sigma_{div} = \Sigma \cup \{\cdot^{-1}\}$ .

Let quantifier-free  $\varphi \in Fml_{\Sigma_{div}}^{qf}$  contain a division by  $t$ :

$$\varphi[t^{-1}] \leftrightarrow ((\exists y. y = t^{-1} \wedge \varphi[y]) \vee (t = 0 \wedge \varphi[n])) \quad (1)$$

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

Let  $\psi \in Fml_{\Sigma_{div}}$  contain divisions.

Obtain  $\psi' \in Fml_{\Sigma}$  by applying (1) to literals in  $\psi$ .

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

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

# 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:

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

$$f(a) = g(a + 1) \wedge g(a + b) > f(a) \quad (1)$$

## 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”.



## Definition

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

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

$(\varphi \rightarrow x_i = y_i)$  is  $T$ -valid for some  $i \in \{1, \dots, n\}$

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

## Examples:

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

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

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 10.7.** Consider the formula

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

which mixes linear arithmetic and uninterpreted functions. Purification results in

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

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

# Example

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

# Nelsson-Oppen Algorithm – convex case

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

$\tau$  bridges between  $T_1$  and  $T_2$  and is a conjunction of equalities over variables

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

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

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.

- 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
  - $\varphi_i \rightarrow (x_1 = y_1 \vee \dots \vee x_k = y_k)$  and
  - $\varphi_i \not\rightarrow (x_j = y_j)$

then apply Nelson–Oppen recursively to adding  $x_i = y_i$  to the different  $\tau$ .

If any of these subproblems is satisfiable, return “Satisfiable”.  
Otherwise, return “Unsatisfiable”.