

## Lecture 4

# First-Order Theories

Zvonimir Rakamarić  
University of Utah

slides acknowledgements: Zohar Manna

## Administrivia

- ▶ Conference traveling: Sep 10-14
- ▶ There will be classes
  - ▶ Diego (postdoc and SMT expert) will cover for me
    - ▶ Theory combination and SMT (satisfiability modulo theory) solvers
- ▶ Project proposal (1 page) due on Sep 26:  
*“Absolutely make sure you discuss your project idea with me at least a week before the proposal due date.”*
- ▶ Houston, we have a problem...

## Some Project Ideas

- ▶ Extend SMACK (Static Modular Assertion Checker) with something
  - ▶ Publicly available, uses LLVM, checks C programs,...
- ▶ Resilience
  - ▶ Catching (transient) hardware errors in software
- ▶ NASA project
  - ▶ Improving coverage of testing using automata-learning techniques and concolic execution
- ▶ And many more...

3

## Last Time

- ▶ First-order logic
  - ▶ Syntax and semantics
  - ▶ Quantifiers
  - ▶ Undecidable
- ▶ Proving validity with semantic argument method

4

## First-Order Theories

- ▶ Software manipulates structures
  - ▶ Numbers, arrays, lists, bitvectors,...
- ▶ Software (and hardware) verification
  - ▶ Reasoning about such structures
- ▶ First-order theories
  - ▶ Formalize structures to enable reasoning about them
  - ▶ Validity is often decidable

5

## Definition

- ▶ **First-order theory**  $T$  defined by:
  - ▶ **Signature**  $\Sigma_T$  – set of constant, function, and predicate symbols
    - ▶ Have no meaning
  - ▶ **Axioms**  $A_T$  – set of closed (no free variables)  $\Sigma_T$ -formulae
    - ▶ Provide meaning for symbols of  $\Sigma_T$

6

## $\Sigma_T$ -formula

- ▶  $\Sigma_T$ -formula is a formula constructed of:
  - ▶ Constants, functions, and predicate symbols from  $\Sigma_T$
  - ▶ Variables, logical connectives, and quantifiers

7

## $T$ -interpretation

- ▶ Interpretation  $I$  is  $T$ -interpretation if it satisfies all axioms  $A_T$  of  $T$ :

$$I \models A \text{ for every } A \in A_T$$

8

## Satisfiability and Validity

- ▶  $\Sigma_T$ -formula  $F$  is **satisfiable in theory  $T$**  ( $T$ -satisfiable) if there is a  $T$ -interpretation  $I$  that satisfies  $F$
- ▶  $\Sigma_T$ -formula  $F$  is **valid in theory  $T$**  ( $T$ -valid,  $T \models F$ ) if every  $T$ -interpretation  $I$  satisfies  $F$ 
  - ▶ Theory  $T$  consists of all closed  $T$ -valid formulae
- ▶ Two  $\Sigma_T$ -formulae  $F_1$  and  $F_2$  are **equivalent in  $T$**  ( $T$ -equivalent) if  $T \models F_1 \leftrightarrow F_2$

9

## Fragment of a Theory

- ▶ **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 formulae without quantifiers that are valid in  $T$
- ▶ Often decidable fragments for undecidable theories

10

## Decidability

- ▶ Theory  $T$  is **decidable** if  $T$ -validity is decidable for every  $\Sigma_T$ -formula  $F$ 
  - ▶ There is an algorithm that always terminates with “yes” if  $F$  is  $T$ -valid, and “no” if  $F$  is  $T$ -invalid
- ▶ Fragment of  $T$  is **decidable** if  $T$ -validity is decidable for every  $\Sigma_T$ -formula  $F$  in the fragment

11

## Theory of Equality $T_E$

Signature

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

consists of:

- ▶ a binary predicate “=” interpreted using provided axioms
- ▶ constant, function, and predicate symbols

12

## 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 int.  $n$  and  $n$ -ary function symbol  $f$ ,  
 $\forall x_1, \dots, x_n, y_1, \dots, y_n. \left( \bigwedge_{i=1}^n x_i = y_i \right) \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$   
 (function congruence)
5. for each positive int.  $n$  and  $n$ -ary predicate symbol  $p$ ,  
 $\forall x_1, \dots, x_n, y_1, \dots, y_n. \left( \bigwedge_{i=1}^n x_i = y_i \right) \rightarrow (p(x_1, \dots, x_n) \leftrightarrow p(y_1, \dots, y_n))$   
 (predicate congruence)

13

## Decidability of $T_E$

- ▶ Bad news
  - ▶  $T_E$  is undecidable
- ▶ Good news
  - ▶ Quantifier-free fragment of  $T_E$  is decidable
  - ▶ Very efficient algorithms

14

## Arithmetic: Natural Numbers and Integers

Natural numbers  $\mathbb{N} = \{0, 1, 2, \dots\}$

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

Three theories:

- ▶ **Peano arithmetic**  $T_{PA}$ 
  - ▶ Natural numbers with addition (+), multiplication (\*), equality (=)
- ▶ **Presburger arithmetic**  $T_{\mathbb{N}}$ 
  - ▶ Natural numbers with addition (+), equality (=)
- ▶ **Theory of integers**  $T_{\mathbb{Z}}$ 
  - ▶ Integers with addition (+), subtraction (-), comparison (>), equality (=), multiplication by constants

15

## Peano Arithmetic $T_{PA}$

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

- ▶  $T_{PA}$ -satisfiability and  $T_{PA}$ -validity are undecidable
  - ▶ Restrict the theory more

16

## Presburger Arithmetic $T_{\mathbb{N}}$

$\Sigma_{\mathbb{N}} : \{0, 1, +, =\}$       no multiplication!

Axioms:

1. equality axioms for =
2.  $\forall x. \neg(x+1=0)$       (zero)
3.  $\forall x, y. x+1=y+1 \rightarrow x=y$       (successor)
4.  $F[0] \wedge (\forall x. F[x] \rightarrow F[x+1]) \rightarrow \forall x. F[x]$  (induction)
5.  $\forall x. x+0=x$       (plus zero)
6.  $\forall x, y. x+(y+1)=(x+y)+1$       (plus successor)

17

## Decidability of $T_{\mathbb{N}}$

- ▶  $T_{\mathbb{N}}$ -satisfiability and  $T_{\mathbb{N}}$ -validity are decidable

18

## Theory of Integers $T_{\mathbb{Z}}$

$\Sigma_{\mathbb{Z}} : \{\dots, -2, -1, 0, 1, 2, \dots, -3^*, -2^*, 2^*, 3^*, \dots, +, -, =, >\}$

where

- ▶  $\dots, -2, -1, 0, 1, 2, \dots$  are constants
- ▶  $\dots, -3^*, -2^*, 2^*, 3^*, \dots$  are unary functions  
(intended meaning:  $2^*x$  is  $x+x$ ,  $-3^*x$  is  $-x-x-x$ )
- ▶  $+, -, >, =$  have the usual meaning
- ▶  $T_{\mathbb{N}}$  and  $T_{\mathbb{Z}}$  have the same expressiveness
  - ▶ Every  $\Sigma_{\mathbb{Z}}$ -formula can be reduced to  $\Sigma_{\mathbb{N}}$ -formula
  - ▶ Every  $\Sigma_{\mathbb{N}}$ -formula can be reduced to  $\Sigma_{\mathbb{Z}}$ -formula

19

## Example of $T_{\mathbb{Z}}$ to $T_{\mathbb{N}}$ Reduction

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

$$F_0 : \forall w, x. \exists y, z. x + 2^*y - z - 13 > -3^*w + 5$$

Introduce two variables  $v_p$  and  $v_n$  (range over natural numbers) for each variable  $v$  (range over integers) in  $F_0$ :

$$F_1 : \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \\ (x_p - x_n) + 2^*(y_p - y_n) - (z_p - z_n) - 13 > -3^*(w_p - w_n) + 5$$

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

$$F_2 : \forall w_p, w_n, x_p, x_n. \exists y_p, y_n, z_p, z_n. \\ x_p + 2^*y_p + z_n + 3^*w_p > x_n + 2^*y_n + z_p + 13 + 3^*w_n + 5$$

20

## Example of $T_{\mathbb{Z}}$ to $T_{\mathbb{N}}$ Reduction cont.

Eliminate \* and >:

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

►  $F_3$  is a  $\Sigma_{\mathbb{N}}$ -formula equisatisfiable to  $F_0$

21

## Example of $T_{\mathbb{N}}$ to $T_{\mathbb{Z}}$ Reduction

Consider  $\Sigma_{\mathbb{N}}$ -formula

$$F: \forall x. \exists y. x=y+1$$

$F$  is equisatisfiable to  $\Sigma_{\mathbb{Z}}$ -formula

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

22

## Decidability of $T_{\mathbb{Z}}$

- ▶  $T_{\mathbb{Z}}$ -satisfiability and  $T_{\mathbb{Z}}$ -validity are decidable

23

## Next Time

- ▶ More on first-order theories
  - ▶ Arithmetic with rationals and reals
  - ▶ Arrays
  - ▶ Recursive data structures
- ▶ Complexities for theories

24