

CS 6110 – Formal Methods in System Design | Spring 2015  
Jan-21

## Lecture 3 First-Order Logic

Zvonimir Rakamarić  
University of Utah

### Last Time

- ▶ Propositional logic
  - ▶ Syntax and semantics
- ▶ Normal forms
  - ▶ NNF, DNF, CNF
- ▶ Tseitin transformation
- ▶ DPLL algorithm
  - ▶ Used in SAT solvers

## First-Order Logic (FOL)

- ▶ Extends propositional logic with predicates, functions, and quantifiers
  - ▶ More expressive than PL
  - ▶ Suitable for reasoning about computation
- ▶ Examples
  - ▶ The length of one side of a triangle is less than the sum of the lengths of the other two sides
 
$$\forall x, y, z. \text{triangle}(x, y, z) \rightarrow \text{len}(x) < \text{len}(y) + \text{len}(z)$$
  - ▶ All elements of array  $A$  are 0
 
$$\forall i. 0 \leq i \wedge i < \text{size}(A) \rightarrow A[i] = 0$$

## Syntax

*variables*  $x, y, z, \dots$

*constants*  $a, b, c, \dots$

*functions*  $f, g, h, \dots$

*terms* variables, constants, or n-ary function applied to n terms as arguments

*predicates*  $p, q, r, \dots$

*atom*  $\top, \perp$ , or n-ary predicate applied to n terms

*literal* atom or its negation

## Syntax cont.

*formula* literal, application of a logical connective  $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$  to formulae, or application of a *quantifier* to a formula

### ▶ Quantifiers

- ▶ Existential:  $\exists x. F[x]$   
“there exists an  $x$  such that  $F[x]$ ”
- ▶ Universal:  $\forall x. F[x]$   
“for all  $x$ ,  $F[x]$ ”

## Example

$$\forall x. p(f(x), x) \rightarrow (\exists y. p(f(g(x, y)), g(x, y))) \wedge q(x, f(x))$$

## Semantics

- ▶ An interpretation  $I : (D_I, \alpha_I)$  is a pair
  - ▶ Domain  $D_I$ 
    - ▶ Non-empty set of values or objects
  - ▶ Assignment  $\alpha_I$  maps
    - ▶ each variable  $x$  into value  $x_I \in D_I$
    - ▶ each  $n$ -ary function  $f$  into  $f_I : D_I^n \rightarrow D_I$
    - ▶ each  $n$ -ary predicate  $p$  into  $p_I : D_I^n \rightarrow \{\text{true}, \text{false}\}$
  - ▶ Boolean connectives evaluated as in propositional logic

## Example

$$F : p(f(x,y),z) \rightarrow p(y,g(z,x))$$

Interpretation  $I : (D_I, \alpha_I)$  with

$$D_I = \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \quad (\text{integers})$$

$$\alpha_I : \{ f \mapsto +, g \mapsto -, p \mapsto > \}$$

$$F_I : x + y > z \rightarrow y > z - x$$

$$\alpha_I : \{ x \mapsto 13, y \mapsto 42, z \mapsto 1 \}$$

$$F_I : 13 + 42 > 1 \rightarrow 42 > 1 - 13$$

Compute the truth value of  $F$  under  $I$

1.  $I \models x + y > z$       since  $13 + 42 > 1$
2.  $I \models y > z - x$       since  $42 > 1 - 13$
3.  $I \models F$               follows from 1, 2, and  $\rightarrow$

$F$  is true under  $I$

## Semantics of Quantifiers

- ▶  $x$ -variant of interpretation  $I : (D_I, \alpha_I)$  is an interpretation  $J : (D_J, \alpha_J)$  such that
  - ▶  $D_I = D_J$
  - ▶  $\alpha_I[y] = \alpha_J[y]$  for all symbols  $y$ , except possibly  $x$ $I$  and  $J$  agree on everything except maybe the value of  $x$
  
- ▶ Denote  $J : I \triangleleft \{x \mapsto v\}$  the  $x$ -variant of  $I$  in which  $\alpha_J[x] = v$  for some  $v \in D_I$ . Then
  - ▶  $I \models \forall x.F$  iff for all  $v \in D_I$ ,  $I \triangleleft \{x \mapsto v\} \models F$
  - ▶  $I \models \exists x.F$  iff there exists  $v \in D_I$  such that  $I \triangleleft \{x \mapsto v\} \models F$

## Example

- ▶ For  $D_I = \mathbb{Q}$  (set of rational numbers), consider
 
$$F : \forall x. \exists y. 2 * y = x$$
- ▶ Compute the value of  $F_I$ :
 

Let

$$J_1 : I \triangleleft \{x \mapsto v\} \text{ be } x\text{-variant of } I$$

$$J_2 : J_1 \triangleleft \{y \mapsto v/2\} \text{ be } y\text{-variant of } J_1$$
 for  $v \in \mathbb{Q}$ .
 

Then

  1.  $J_2 \models 2 * y = x$       since  $2 * v/2 = v$
  2.  $J_1 \models \exists y. 2 * y = x$
  3.  $I \models \forall x. \exists y. 2 * y = x$  since  $v \in \mathbb{Q}$  is arbitrary

## Satisfiability and Validity

- ▶  $F$  is **satisfiable** iff there exists  $I$  such that  $I \models F$
  - ▶  $F$  is **valid** iff for all  $I$ ,  $I \models F$
- $F$  is valid iff  $\neg F$  is unsatisfiable
- ▶ **FOL is undecidable**
    - ▶ There does not exist an algorithm for deciding if a FOL formula  $F$  is valid/unsat
      - ▶ I.e., that always halts and returns “yes” if  $F$  is valid/unsat or “no” if  $F$  is invalid/sat.
  - ▶ **FOL is semi-decidable**
    - ▶ There is a procedure that always halts and returns “yes” if  $F$  is valid, but may not halt if  $F$  is invalid.

## Semantic Argument Method

- ▶ For proving validity of  $F$  in FOL
- ▶ Assume  $F$  is not valid and  $I$  is a falsifying interpretation:  $I \not\models F$
- ▶ Exhaustively apply proof rules
  - ▶ If no contradiction reached and no more rules are applicable
    - ▶  $F$  is invalid
  - ▶ If in every branch of proof a contradiction reached
    - ▶  $F$  is valid

## Proof Rule

- ▶ Consists of:
  - ▶ Premises (one or more)
  - ▶ Deductions (one or more)
- ▶ Application
  - ▶ Match premises to existing facts and form deductions
  - ▶ Branch (fork) when needed
- ▶ Example – proof rules for  $\wedge$

$$\frac{I \models F \wedge G}{I \models F}$$

$$\frac{I \models F \wedge G}{I \models G}$$

$$\frac{I \models F \wedge G}{I \models F \quad I \models G}$$

## Proof Rules for Propositional Part

$$\frac{I \models :F}{I \models F}$$

$$\frac{I \models :F}{I \models F}$$

$$\frac{I \models F \wedge G}{I \models F}$$

$$\frac{I \models F \wedge G}{I \models G}$$

$$\frac{I \models F \wedge G}{I \models F \quad I \models G}$$

$$\frac{I \models F \_ G}{I \models F \quad I \models G}$$

$$\frac{I \models F \_ G}{I \models F}$$

$$\frac{I \models F \_ G}{I \models G}$$

$$\frac{I \models F ! G}{I \models F \quad I \models G}$$

$$\frac{I \models F ! G}{I \models F}$$

$$\frac{I \models F ! G}{I \models G}$$

$$\frac{I \models F \$ G}{I \models F \wedge G \quad I \models F \_ G}$$

$$\frac{I \models F \$ G}{I \models F \wedge : G \quad I \models : F \wedge G}$$

$$\frac{I \models F}{I \models F}$$

$$\frac{I \models F}{I \models ?}$$

## Proof Rules for Quantifiers

$$\frac{I \models \exists x:F}{I / f x \nabla v g \models F} \text{ for any } v \in D_I$$

$$\frac{I \models \exists x:F}{I / f x \nabla v g \models F} \text{ for a fresh } v \in D_I$$

any – usually use  $v$  introduced earlier in the proof

$$\frac{I \models \exists x:F}{I / f x \nabla v g \models F} \text{ for a fresh } v \in D_I$$

fresh – use  $v$  that has not been previously used in the proof

$$\frac{I \models \exists x:F}{I / f x \nabla v g \models F} \text{ for any } v \in D_I$$

### Example 1

$$F : p(a) \rightarrow \exists x. p(x)$$



## Example 2

$$F : (\forall x. p(x)) \leftrightarrow (\neg \exists x. \neg p(x))$$

## Next Lecture

- ▶ Issues with FOL
  - ▶ Validity in FOL is undecidable
  - ▶ Too general
- ▶ First-order logic theories
  - ▶ Often decidable fragments of FOL suitable for reasoning about particular domain
    - ▶ Equality
    - ▶ Arithmetic
    - ▶ Arrays