Lecture 3
First-Order Logic

Zvonimir Rakamarić
University of Utah

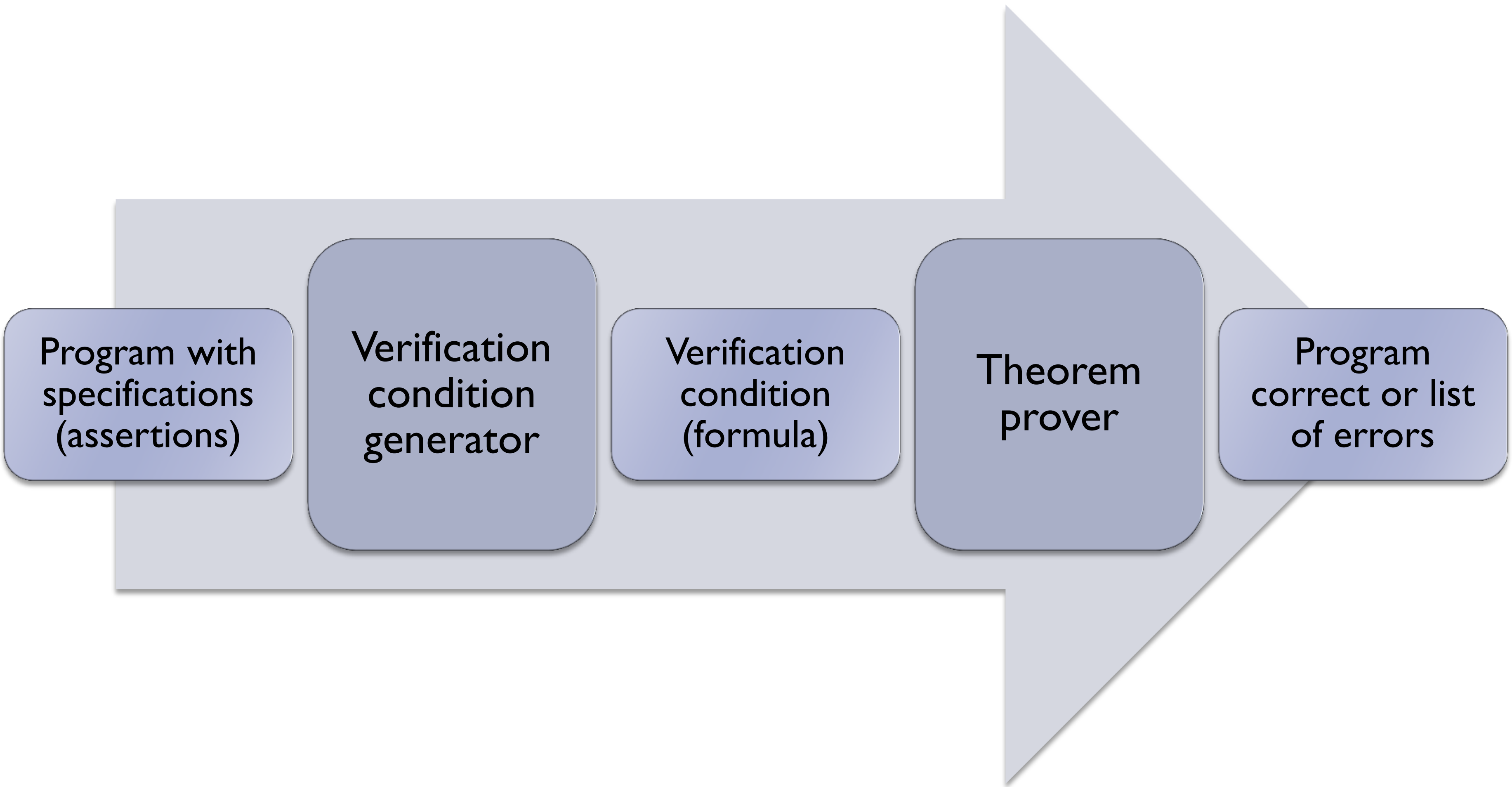
Last Time

- Propositional logic
- DPLL algorithm
  - Used in modern SAT solvers

This Time

- Encoding a problem into SAT
  - Homework assignment 1
- First-order logic
- Reading: Chapter 2

Basic Verifier Architecture



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

    $\forall x, y, z.\ \mathit{triangle}(x, y, z) \rightarrow \mathit{len}(x) < \mathit{len}(y) + \mathit{len}(z)$
  - All elements of array A are 0

    $\forall i.\ 0 \leq i \wedge i < \mathit{size}(A) \rightarrow A[\, i \,] = 0$

Syntax

variables	x, y, z, …
constants	a, b, c, …
functions	f, g, h, …
terms	variables, constants, or n-ary function applied to n terms as arguments
predicates	p, q, r, …
atom	$\top$, $\bot$, 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

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

Semantics

- An interpretation $I : (D_I, \alpha_I)$ is a pair
  - Domain D_I
    - Non-empty set of values or objects
  - Assignment α_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 $p_I : D_I^n \rightarrow \{\text{true, false}\}$
  - Boolean connectives evaluated as in propositional logic

Example

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

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

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

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

$F_I : x + y > z \rightarrow \mathrm{y} > z - x$

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

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

Compute the truth value of F under I

1. $I \vDash x + y > z$ since $13 + 42 > 1$
2. $I \vDash y > z - x$ since $42 > 1 - 13$
3. $I \vDash F$ 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

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

  $$J_2 : J_1 \triangleleft \{y \mapsto v/2\} \text{ be y-variant of } J_1$$

  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, $I \models F$

$$F \text{ is valid iff } \neg F \text{ is unsatisfiable}$$

- 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 $\wedge$

$$\frac{I \models F \wedge G}{\begin{array}{l} I \models F \\ I \models G \end{array}} \qquad \frac{I \not\models F \wedge G}{I \not\models F \quad \mid \quad I \not\models G}$$

Proof Rules for Propositional Part I

$$\frac{I \models \neg F}{I \not\models F} \qquad \frac{I \not\models \neg F}{I \models F}$$

$$\frac{I \models F \wedge G}{\begin{array}{l} I \models F \\ I \models G \end{array}} \qquad \frac{I \not\models F \wedge G}{I \not\models F \quad \mid \quad I \not\models G}$$

$$\frac{I \models F \vee G}{I \models F \quad \mid \quad I \models G} \qquad \frac{I \not\models F \vee G}{\begin{array}{l} I \not\models F \\ I \not\models G \end{array}}$$

Proof Rules for Propositional Part II

$$\frac{I \models F \rightarrow G}{I \not\models F \quad | \quad I \models G}$$

$$\frac{I \not\models F \rightarrow G}{\begin{array}{l} I \models F \\ I \not\models G \end{array}}$$

$$\frac{I \models F \leftrightarrow G}{I \models F \wedge G \quad | \quad I \not\models F \vee G}$$

$$\frac{I \not\models F \leftrightarrow G}{I \models F \wedge \neg G \quad | \quad I \models \neg F \wedge G}$$

$$\frac{\begin{array}{l} I \models F \\ I \not\models F \end{array}}{I \models \bot}$$

Proof Rules for Quantifiers

$$\frac{I \models \forall x.\ F}{I \lhd \{x \mapsto \mathsf{v}\} \models F} \quad \text{for any } \mathsf{v} \in D_I$$

$$\frac{I \not\models \forall x.\ F}{I \lhd \{x \mapsto \mathsf{v}\} \not\models F} \quad \text{for a } \textit{fresh } \mathsf{v} \in D_I$$

$$\frac{I \models \exists x.\ F}{I \lhd \{x \mapsto \mathsf{v}\} \models F} \quad \text{for a } \textit{fresh } \mathsf{v} \in D_I$$

$$\frac{I \not\models \exists x.\ F}{I \lhd \{x \mapsto \mathsf{v}\} \not\models F} \quad \text{for any } \mathsf{v} \in D_I$$

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

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

Example 1

$F : (p \wedge q) \rightarrow (p \vee \neg q)$

Example 2

$$F : (p \to q) \land (q \to r) \to (p \to r)$$

Example 3

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

Example 4

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

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