

# Advanced Software Security

## 9. Propositional Logic

Kihong Heo



# Logic

- What is logic? A tool for reasoning about truths
- Why logic for computer scientists? Reasoning about computation
- For example,
  - “Does this program accept an array of integers and produce a sorted array?”
  - “Does this program access an unallocated memory?”
  - “Does this function always halt?”
- This course: propositional logic (PL) and first-order logic (FOL)

# Syntax

- Atom: basic elements
  - Truth symbols:  $\top$  (“true”) and  $\perp$  (“false”)
  - Propositional variables:  $P, Q, R, \dots$
- Literal: an atom  $\alpha$  or its negation  $\neg\alpha$
- Formula: a literal or the application of a logical connective to formulae

$$\begin{array}{l} F \rightarrow \perp \\ \quad | \quad \top \\ \quad | \quad P, Q, R, \dots \\ \quad | \quad \neg F \\ \quad | \quad F_1 \wedge F_2 \\ \quad | \quad F_1 \vee F_2 \\ \quad | \quad F_1 \rightarrow F_2 \\ \quad | \quad F_1 \leftrightarrow F_2 \end{array}$$

# Semantics

- Give meaning to formulae
  - In propositional logic, the truth values
- The semantics of a formula is defined with an interpretation  $I$ 
  - An interpretation assigns to every propositional variable exactly one truth value
- For example,  $F : P \wedge Q \rightarrow P \vee \neg Q$  and  $I : \{P \mapsto \top, Q \mapsto \perp\}$

# Inductive Definition of PL

- Notation:

- $I \models F$  if  $F$  evaluates to true under  $I$
- $I \not\models F$  if  $F$  evaluates to false under  $I$

$I \models \top$	
$I \not\models \perp$	
$I \models P$	iff $I[P] = \text{true}$
$I \not\models P$	iff $I[P] = \text{false}$
$I \models \neg F$	iff $I \not\models F$
$I \models F_1 \wedge F_2$	iff $I \models F_1$ and $I \models F_2$
$I \models F_1 \vee F_2$	iff $I \models F_1$ or $I \models F_2$
$I \models F_1 \rightarrow F_2$	iff, if $I \models F_1$ then $I \models F_2$
$I \models F_1 \leftrightarrow F_2$	iff, if $I \models F_1$ and $I \models F_2$ , or if $I \not\models F_1$ and $I \not\models F_2$

# Example

- $F : P \wedge Q \implies P \vee \neg Q$  and  $I : \{P \mapsto \top, Q \mapsto \perp\}$

# Satisfiability and Validity

- Two important tasks in logic (why? when?)
- A formula  $F$  is satisfiable iff there exists an interpretation  $I$  such that  $I \models F$
- A formula  $F$  is valid iff for all interpretations  $I$ ,  $I \models F$
- Satisfiability and validity are dual:  $F$  is valid iff  $\neg F$  is unsatisfiable
- We are free to focus on either one; the other will follow

# Determining Validity and Satisfiability (1)

- Truth table method
  - For example,  $F : P \wedge Q \rightarrow P \vee \neg Q$
- Impractical:  $2^n$  interpretations
- Impossible: for any other logic where the domain is not finite (e.g., first-order logic)

P	Q	$P \wedge Q$	$\neg Q$	$P \vee \neg Q$	F
0	0	0	1	1	1
0	1	0	0	0	1
1	0	0	1	1	1
1	1	1	0	1	1



# Determining Validity and Satisfiability (2)

- Semantic argument method (proof by contradiction)
  - Assume  $F$  is invalid:  $I \not\models F$
  - Apply proof rules to derive
  - Derive a contradiction in every branch of the proof
  - Then,  $F$  is valid

# Proof Rules (1)

- According to semantics of negation,

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

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

- According to semantics of conjunction,

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

$$\frac{I \not\models F \wedge G}{I \not\models F \mid I \not\models G}$$

# Proof Rules (2)

- According to semantics of disjunction,

$$\frac{I \models F \vee G}{I \models F \mid I \models G}$$

$$\frac{I \not\models F \vee G}{I \not\models F, I \not\models G}$$

- According to semantics of implication,

$$\frac{I \models F \rightarrow G}{I \not\models F \mid I \models G}$$

$$\frac{I \not\models F \rightarrow G}{I \models F, I \not\models G}$$

# Proof Rules (3)

- According to semantics of iff,

$$\frac{I \models F \leftrightarrow G}{I \models F \wedge G \mid I \models \neg F \wedge \neg G}$$

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

- Contradiction

$$\frac{I \models F, I \not\models F}{I \models \perp}$$

# Example

- Prove  $F : P \wedge Q \rightarrow P \vee \neg Q$  is valid

# Summary

- Propositional logic: the simplest form of logic
- Interpretation: decide the meaning of a formula (either true or false)
- Satisfiability: is there any interpretation that makes the formula be true?
- Validity: does the formula evaluate to be true for all interpretations?
- Duality of satisfiability and validity
  - E.g., “no input can trigger this bug” = “all inputs work well”