

CS6133 Fall 2011 Software Specification and Verification

Lecture 2 Propositional Logic and Proof Procedure

Propositional Logic as Formal Language

- ◆ A logic consists of
 - Syntax: define well-formed formula
 - Semantics: define meaning of formula
 - interpretation of logical connectives
 - satisfaction relation
 - semantic entailment
 - Proof procedure (also called proof theory)
 - Soundness
 - Completeness

CS6133

2

Propositional Logic Syntax

- ◆ The syntax elements
 - Two constant symbols: true and false
 - Propositions: A, B
 - Logic connectives
 - \neg
 - \wedge
 - \vee
 - \Rightarrow
 - Brackets

CS6133

3

Propositional Logic Syntax

- ◆ A well-formed formula (WFF) of propositional logic is constructed as below
 - Every proposition p is a WFF
 - If P is a WFF, then so is (P)
 - If P is a WFF, then so is $\neg P$
 - If P and Q are WFFs, then so is $P \wedge Q$
 - If P and Q are WFFs, then so is $P \vee Q$
 - If P and Q are WFFs, then so is $P \rightarrow Q$

CS6133

4

Propositional Logic Semantics

- ◆ Semantics mean "meaning" and relate two worlds: provide an interpretation (mapping) of expressions in one world in terms of values in another world
- ◆ Semantics are often a function from expressions in one world to expressions in another world
- ◆ The range of the semantic function for propositional logic is the set of truth values
 $Tr = \{TRUE, FALSE\}$

CS6133

5

Truth Table

- ◆ Truth assignment
A truth assignment is a mapping of the variables within a formula into the value TRUE or FALSE
- ◆ Truth tables are used to describe the functions of logic connectives on the truth values
- ◆ Truth tables determine the truth value of logic formulas

CS6133

6

Propositional Logic Semantics

- ◆ Satisfiable
A formula is satisfiable if there exists some truth assignment under which the formula has truth value TRUE
- ◆ Valid
A formula is valid or a tautology, if it has truth value TRUE under all possible truth assignments

CS6133

7

Satisfaction and Entailment

- ◆ Satisfaction relation
A model M satisfies the formula P is called a satisfaction relation
 $M \models P$
- ◆ Entailment relation
From the premises P_1, P_2, P_3, \dots , we may conclude Q , where P_1, P_2, P_3, \dots and Q are all well-formed propositional logic formulas
 $P_1, P_2, P_3 \models Q$

CS6133

8

Decidability

- ◆ A logic is decidable if there is an algorithm to determine if any formula of the logic is a tautology (is a theorem, is valid)
- ◆ Propositional logic is decidable because we can always construct the truth table for the propositional formula

Propositional Logic Proof Procedure

- ◆ A proof procedure is a set of rules we use to transform premises and conclusions into new premises and conclusions
- ◆ A goal is a formula that we want to prove is a tautology
- ◆ A proof is a sequence of proof rules that when chained together relate the premise of the goal to the conclusion of the goal

Truth Table vs. Proof Procedure

- ◆ Determine if a formula is a tautology by using truth tables: determine the value of the formula for every possible combination of values for its proposition letters
- ◆ Constructing truth table would be very tedious since the size of the truth table grows exponentially: it is NP-complete
- ◆ Proof procedures for propositional logic are alternate means to determine tautologies

Example Proof Procedures

- ◆ Hilbert Systems: axiom systems
- ◆ Natural Deduction
- ◆ Binary Decision Diagrams
- ◆ Sequent Calculus

Hilbert System

- ◆ A Hilbert system consists of
 - Axioms: a set of valid formulas
 - Inference rules
- ◆ Inference Rules
 - Determine tautology or unsatisfiability
 - Manipulate formulas as formal strings of symbols
 - But do not make use of the meanings of formulas

CS6133

13

Proof in Hilbert System

- ◆ Proof is a finite sequence X_1, X_2, \dots, X_n of formulas such that each term is either an axiom or follows from earlier terms by one of the rules of inference
- ◆ Write proofs as a list of formulas, each on its own line, and refer to the line of a proof in the justification for steps

CS6133

14

Hilbert System

- ◆ Hilbert system is sound
 - If start with axioms (which are valid)
 - Then each subsequent formula derived with inference rules is also valid
- ◆ Hilbert system is complete
 - If start with axioms (which are valid)
 - Then it can derive all formulas which are valid
- ◆ Hilbert system is consistent
 - If start with axioms (which are valid)
 - Then it is impossible to prove both P and $\neg P$

CS6133

15

An Axiomatic System for Propositional Logic

- ◆ Three axioms
 - $A \Rightarrow (B \Rightarrow A)$
 - $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
 - $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$
- ◆ One rule of inference
 - From A and $A \Rightarrow B$, B can be derived, where A and B are any well-formed formulas

CS6133

16

Exercise

- ◆ Show $(X \Rightarrow Y) \Rightarrow (X \Rightarrow X)$

CS6133

17

Natural Deduction

- ◆ A collection of proof rules, each of which allows us to infer formulas from other formulas, eventually to get from a set of premises to a conclusion
- ◆ A form of forward proof
 - Starting from the premises
 - Use the inference rules to deduce new formulas that logically follow from the premises
 - Continue this process until we have deduced the conclusion

CS6133

18

Natural Deduction Rules

- ◆ Rules for conjunction
- ◆ Rules for double negation
- ◆ Rules for eliminating implication: modus ponens
- ◆ Rule implies introduction
- ◆ Rules for disjunction

CS6133

19

Natural Deduction Rules

- ◆ Rules for conjunction

$$\frac{p \quad q}{p \wedge q} \wedge i$$

$$\frac{p \wedge q}{p} \wedge e1$$

$$\frac{p \wedge q}{q} \wedge e2$$

CS6133

20

Natural Deduction Rules

◆ Rules for double negation

$$\frac{\neg\neg p}{p} \neg\neg e$$

$$\frac{p}{\neg\neg p} \neg\neg i$$

CS6133

21

Natural Deduction Rules

◆ Rules for eliminating implication

$$\frac{p \quad p \Rightarrow q}{q} \Rightarrow e$$

$$\frac{p \Rightarrow q \quad \neg q}{\neg p} \Rightarrow e$$

CS6133

22

Natural Deduction Rules

◆ Rule implies introduction

$$\frac{\begin{array}{l} p \\ \vdots \\ q \end{array}}{p \Rightarrow q} \Rightarrow i$$

CS6133

23

Natural Deduction Rules

◆ Rules for disjunction

$$\frac{p}{p \vee q} \vee i1$$

$$\frac{q}{p \vee q} \vee i2$$

CS6133

24