CS477 Formal Software Development Methods

Elsa L Gunter
2112 SC, UIUC
egunter@illinois.edu
http://courses.engr.illinois.edu/cs477

Slides based in part on previous lectures by Mahesh Vishwanathan, and by Gul Agha

January 24, 2013

Course Overview

- Review of basic math underlying most formal methods
- Intro to interactive theorem proving
  - Intro to Isabelle/HOL
- Floyd-Hoare Logic (aka Axiomatic Semantics)
  - Verification Conditions
  - Verification Condition Generators (VCGs)
- Rewrite Logic
  - Intro to Maude
- Operation Semantics
  - Structured Oper. Sem., Transition Sem., Contexts Reduction Sem.
- Models of Concurrency
  - Finite State Automata, Buchi Automata, Concurrent Game Structures, Petri Nets

Course Overview

- Temporal Logics
  - LTL
  - CTL
- Model Checkers
  - Spin
  - NuSMV
  - SAL
- Process Algebras, Pi Calculus, CSP, Actors
  - Intro to FDR
  - Intro to Rebeca
- Type Systems
  - Type Soundness
  - Dependent Types, Liquid Types, DML
  - Communication Types (aka Session Types)
  - Runtime Type Checking, Runtime Verification

Course Objectives

- How to do proofs in Hoare Logic, and what role a loop invaraint plays
- How to use finite automata to model computer systems
- How to express properties of concurrent systems in a temporal logic
- How to use a model checker to verify / falsify a temporal safety property of a concurrent system
- The connection between types and propgram properties
- What type soundness does and does not guarantee about a well-typed program

Propositional Logic

The Language of Propositional Logic

- Begins with constants $\{\mathbf{T}, \mathbf{F}\}$
- Assumes countable set AP of propositional variables, a.k.a. propositional atoms, a.k.a. atomic propositions
- Assumes logical connectives: $\wedge$ (and); $\vee$ (or); $\neg$ (not); $\Rightarrow$ (implies); $\Leftrightarrow$ = (if and only if)
- The set of propositional formulae $PROP$ is the inductive closure of these as follows:
  - $\{\mathbf{T}, \mathbf{F}\} \subseteq PROP$
  - $AP \subseteq PROP$
  - if $A \in PROP$ then $(A) \in PROP$ and $\neg A \in A$
  - if $A \in PROP$ and $B \in PROP$ then $(A \wedge B) \in PROP$, $(A \vee B) \in PROP$, $(A \Rightarrow B) \in PROP$, $(A \Leftrightarrow B) \in PROP$.
  - Nothing else is in $PROP$
- Informal definition; formal definition requires math foundations, set theory, fixed point theorem ...

Semantics of Propositional Logic: Model Theory

Model for Propositional Logic has three parts

- Mathematical set of values used as meaning of propositions
- Interpretation function giving meaning to props built from logical connectives, via structural recursion

Standard Model of Propositional Logic

- $\mathcal{B} = \{\mathrm{true}, \mathrm{false}\}$ boolean values
- $v : AP \to \mathcal{B}$ a valuation
- Interpretation function ...

Semantics of Propositional Logic: Model Theory

Standard Model of Propositional Logic (cont)

- Standard interpretation $\mathcal{I}_v$ defined by structural induction on formulae:
  - $\mathcal{I}_v(\mathbf{T}) = \mathrm{true}$ and $\mathcal{I}_v(\mathbf{F}) = \mathrm{false}$
  - If $a \in AP$ then $\mathcal{I}_v(a) = v(a)$
  - For $p \in PROP$, if $\mathcal{I}_v(p) = \mathrm{true}$ then $\mathcal{I}_v(\neg p) = \mathrm{false}$, and if $\mathcal{I}_v(p) = \mathrm{false}$ then $\mathcal{I}_v(\neg p) = \mathrm{true}$
  - For $p, \ q \in PROP$
    - If $\mathcal{I}_v(p) = \mathrm{true}$ and $\mathcal{I}_v(q) = \mathrm{true}$, then $\mathcal{I}_v(p \wedge q) = \mathrm{true}$, else $\mathcal{I}_v(p \wedge q) = \mathrm{false}$
    - If $\mathcal{I}_v(p) = \mathrm{true}$ or $\mathcal{I}_v(q) = \mathrm{true}$, then $\mathcal{I}_v(p \vee q) = \mathrm{true}$, else $\mathcal{I}_v(p \vee q) = \mathrm{false}$
    - If $\mathcal{I}_v(q) = \mathrm{true}$ or $\mathcal{I}_v(p) = \mathrm{false}$, then $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$, else $\mathcal{I}_v(p \Rightarrow q) = \mathrm{false}$
    - If $\mathcal{I}_v(p) = \mathcal{I}_v(q)$ then $\mathcal{I}_v(p \Leftrightarrow q) = \mathrm{true}$, else $\mathcal{I}_v(p \Leftrightarrow q) = \mathrm{false}$

Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true					
true	false					
false	true					
false	false					

Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false				
true	false	false				
false	true	true				
false	false	true				

Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true			
true	false	false	false			
false	true	true	false			
false	false	true	false			

Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true	true		
true	false	false	false	true		
false	true	true	false	true		
false	false	true	false	false		

Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true	true	true	
true	false	false	false	true	false	
false	true	true	false	true	true	
false	false	true	false	false	true	

Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true	true	true	true
true	false	false	false	true	false	false
false	true	true	false	true	true	false
false	false	true	false	false	true	true

Modeling Propositional Formulae

- $(\mathcal{B}, \mathcal{I})$ is the standard model of proposition logic
- Given valuation v and proposition $p \in PROP$, write $v \models p$ iff $\mathcal{I}_v(p) = \mathrm{true}$
  - More fully written as $\mathcal{B}, \mathcal{I}, v \models p$
  - Say v satisfies p, or v models p
  - Write $v \not\models p$ if $\mathcal{I}_v(p) = \mathrm{false}$
- p is satisfiable if there exists valuation v such that $v \models p$
- p is valid, a.k.a. a tautology if for every valuation v we have $v \models p$
- p is logically equivalent to q, $p \equiv q$ if for every valuation, v, we have $v \models p$ iff $v \models q$
  - Claim: Logical equivalence is an equivalence relation

Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true			
true	false			
false	true			
false	false			

Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true	true		
true	false	false		
false	true	true		
false	false	true		

Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true	true	true	
true	false	false	true	
false	true	true	true	
false	false	true	false	

Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true	true	true	true
true	false	false	true	true
false	true	true	true	true
false	false	true	false	true

Example Tautology – Your Turn

Example: Logical Equivalence

$$A \Rightarrow B \equiv ((\neg A) \vee B)$$

A	B	$A \Rightarrow B$	$\neg A$	$(\neg A) \vee B$
true	true	true	false	true
true	false	false	false	false
false	true	true	true	true
false	false	true	true	true

More Useful Logical Equivalences

$$
\begin{array}{rclrclrcl}
\neg\neg A & \equiv & A & \neg\mathbf{T} & \equiv & \mathbf{F} & \neg\mathbf{F} & \equiv & \mathbf{T} \\
(A \vee A) & \equiv & A & (A \vee B) \vee C & \equiv & A \vee (B \vee C) & & & \\
(A \wedge A) & \equiv & A & (A \wedge B) \wedge C & \equiv & A \wedge (B \wedge C) & & & \\
A \vee B & \equiv & B \vee A & \neg(A \vee B) & \equiv & (\neg A) \wedge (\neg B) & & & \\
A \wedge B & \equiv & B \wedge A & \neg(A \wedge B) & \equiv & (\neg A) \vee (\neg B) & & & \\
(A \wedge \neg A) & \equiv & \mathbf{F} & A \vee (B \wedge C) & \equiv & (A \vee B) \wedge (A \vee C) & & & \\
(A \vee \neg A) & \equiv & \mathbf{T} & (A \wedge B) \vee C & \equiv & (A \vee C) \wedge (B \vee C) & & & \\
(\mathbf{T} \wedge A) & \equiv & A & A \wedge (B \vee C) & \equiv & (A \wedge B) \vee (A \wedge C) & & & \\
(\mathbf{T} \vee A) & \equiv & \mathbf{T} & (A \wedge B) \vee C & \equiv & (A \wedge C) \vee (B \wedge C) & & & \\
(\mathbf{F} \wedge A) & \equiv & \mathbf{F} & (\mathbf{F} \vee A) & \equiv & A & & &
\end{array}
$$

Logical Equivalence a Structural Congruence

Theorem

Logical equivalence is a structural congruence. That is, if $p \equiv p'$ *and* $q \equiv q'$ *then*

1. $\neg p \equiv \neg p'$
2. $p \wedge q \equiv p' \wedge q'$
3. $p \vee q \equiv p' \vee q'$
4. $p \Rightarrow q \equiv p' \Rightarrow q'$
5. $p \Leftrightarrow q \equiv p' \Leftrightarrow q'$

Logical Equivalence a Structural Congruence

Proof.

- Assume $p \equiv p'$ and $q \equiv q'$
- **Hyp**: Then for all valuations v, $v \models p$ iff $v \models p'$ and $v \models q$ iff $v \models q'$, i.e. $\mathcal{I}_v(p) = \mathrm{true}$ iff $\mathcal{I}_v(p') = \mathrm{true}$ and $\mathcal{I}_v(q) = \mathrm{true}$ iff $\mathcal{I}_v(q') = \mathrm{true}$
- Case 4: Show $p \Rightarrow q \equiv p' \Rightarrow q'$
  - Other cases done same way
- Need to show for all v, $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$ iff $\mathcal{I}_v(p' \Rightarrow q') = \mathrm{true}$
- Fix v
- Need to show if $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$ then $\mathcal{I}_v(p' \Rightarrow q') = \mathrm{true}$, and if $\mathcal{I}_v(p' \Rightarrow q') = \mathrm{true}$ then $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$

$\square$

Logical Equivalence a Structural Congruence

Proof.

- $(\Longrightarrow)$
  - Assume $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$
  - By closure property of inductive definition of $\mathcal{I}$, either $\mathcal{I}_v(q) = \mathrm{true}$ or $\mathcal{I}_v(p) = \mathrm{false}$.
  - Therefore, by **Hyp**, either $\mathcal{I}_v(q') = \mathrm{true}$ or $\mathcal{I}_v(p') = \mathrm{false}$
    - since $\mathcal{B}$ has only two elements, and $\mathcal{I}_v$ total (proof?)
  - By $\mathcal{I}$ def, have $\mathcal{I}_v(p' \Rightarrow q')$
- $(\Longleftarrow)$ $\square$

Non-standard Model of Propositional Logic

Other models possible
Example:

- $\mathcal{C} = \{\text{true}, \text{false}\bot\}$
- Valuations assign values in cC to propositional atoms
- If $\mathcal{J}_w(p) = \bot$ then $\mathcal{J}_w(\neg p) = \bot$, otherwise same as for $\mathcal{I}$
- $\mathcal{J}_w(p) = bot$ or $\mathcal{J}_w(q) = \bot$ then $\mathcal{J}_w(\neg p) = \bot$, $\mathcal{J}_w(p \wedge q) = \bot$, $\mathcal{J}_w(p \vee q) = \bot$, $\mathcal{J}_w(p \Rightarrow q) = \bot$, and $\mathcal{J}_w(p \Leftrightarrow q) = \bot$; otherwise same as for $\mathcal{I}$
- Note: $A \vee \neg A \not\equiv \mathbf{T}$