

# 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

April 3, 2013

# Formal LTL Semantics

- $\sigma \models \circ\varphi$  iff  $\sigma^1 \models \varphi$
- $\sigma \models \varphi\mathcal{U}\psi$  iff for some  $k$ ,  $\sigma^k \models \psi$  and for all  $i < k$ ,  $\sigma^i \models \varphi$
- $\sigma \models \varphi\mathcal{V}\psi$  iff for some  $k$ ,  $\sigma^k \models \varphi$  and for all  $i \leq k$ ,  $\sigma^i \models \psi$ ,  
or for all  $i$ ,  $\sigma^i \models \psi$ .
- $\sigma \models \Box\varphi$  if for all  $i$ ,  $\sigma^i \models \varphi$
- $\sigma \models \Diamond\varphi$  if for some  $i$ ,  $\sigma^i \models \varphi$

# Some More Equivalences

- $\Box\varphi \Leftrightarrow \varphi \wedge \circ\Box\varphi$
- $\Diamond\varphi \Leftrightarrow \varphi \vee \circ\Diamond\varphi$
- $\varphi\mathcal{U}\psi \Leftrightarrow \phi \vee (\psi \wedge \circ(\varphi\mathcal{U}\psi))$
- $\varphi\mathcal{V}\psi \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \circ(\varphi\mathcal{V}\psi))$
- $\Box$ ,  $\Diamond$ ,  $\mathcal{U}$ ,  $\mathcal{V}$  may all be understood recursively, by what they state about right now, and what they state about the future
- Caution:  $\Box$  vs  $\Diamond$ ,  $\mathcal{U}$  vs  $\mathcal{V}$  differ in there limit behavior

# Traffic Light Example

## Basic Behavior:

- $\Box((NSC = Red) \vee (NSC = Green) \vee (NSC = Yellow))$
- $\Box((NSC = Red) \Rightarrow ((NSC \neq Green) \wedge (NSC \neq Yellow)))$
- Similarly for *Green* and *Red*
- $\Box(((NCS = Red) \wedge \circ(NCS \neq Red)) \Rightarrow \circ(NCS = Green))$
- Same as  $\Box((NCS = Red) \Rightarrow ((NCS = Red) \cup (NCS = Green)))$
- $\Box(((NCS = Green) \wedge \circ(NCS \neq Green)) \Rightarrow \circ(NCS = Yellow))$
- $\Box(((NCS = Yellow) \wedge \circ(NCS \neq Yellow)) \Rightarrow \circ(NCS = Red))$
- Same for *EWC*

# Traffic Light Example

## Basic Safety

- $\Box((NSC = Red) \vee (EWC = Red))$
- $\Box( ((NSC = Red) \wedge (EWC = Red)) \vee ((NSC \neq Green) \Rightarrow (\circ(NSC = Green))))$

## Basic Liveness

- $(\Diamond(NSC = Red)) \wedge (\Diamond(NSC = Green)) \wedge (\Diamond(NSC = Yellow))$
- $(\Diamond(EWC = Red)) \wedge (\Diamond(EWC = Green)) \wedge (\Diamond(EWC = Yellow))$

# Proof System for LTL

- First Step: View  $\varphi \mathcal{V} \psi$  as macro:  $\varphi \mathcal{V} \psi = \neg((\neg\varphi)\mathcal{U}(\neg\psi))$
- Second Step: Extend all rules of Prop Logic to LTL
- Third Step: Add one more rule:  $\frac{\varphi}{\Box\varphi}$  Gen
- Fourth Step: Add a collection of axioms (a sufficient set of 8 exists)
  - A1:  $\Box\varphi \Leftrightarrow \neg(\Diamond(\neg\varphi))$
  - A2:  $\Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi)$
  - A3:  $\Box\varphi \Rightarrow (\varphi \wedge \circ\Box\varphi)$
  - A4:  $\circ\neg\varphi \Leftrightarrow \neg\circ\varphi$
  - A5:  $\circ(\varphi \Rightarrow \psi) \Rightarrow (\circ\varphi \Rightarrow \circ\psi)$
  - A6:  $\Box(\varphi \Rightarrow \circ\varphi) \Rightarrow (\varphi \Rightarrow \Box\varphi)$
  - A7:  $\varphi\mathcal{U}\psi \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \circ(\varphi\mathcal{V}\psi))$
  - A8:  $\varphi\mathcal{U}\psi \Rightarrow \Diamond\psi$
- Result: a **sound** and **relatively complete** proof system
- Can implement in Isabelle in much the same way as we did Hoare Logic

# Important Meta-Definitions

- $A$  is **sound** with respect to  $B$  if things that are “true” according to  $A$  are things that are “true” according to  $B$ .
- $A$  is **complete** with respect to  $B$  if things that are “true” according to  $B$  are things that are “true” according to  $A$ .
- $A$  is **sound** if things that are “true” according to  $A$  are true.
- $A$  is **complete** everything that is true (that is in the scope of  $A$ ) is “true” according to  $A$ .
- $A$  is **relatively complete** with respect to  $B$  if  $A$  is complete when  $B$  is.  
Think:  $A$  proof system;  $B$  mathematical model

Exercise:  $\varphi \wedge \psi \Rightarrow \Box\varphi \wedge \Box\psi$



# What is Model Checking?

Most generally **Model Checking** is

- an **automated** technique, that given
- a **finite-state model**  $M$  of a system
- and a **logical** property  $\varphi$ ,
- **checks** whether the property holds of model:  $M \models \varphi$ ?

# Model Checking

- Model checkers usually give example of failure if  $M \not\models \varphi$ .
- This makes them useful for **debugging**.
- **Problem:** Can only handle finite models: unbounded or continuous data sets can't be directly handled
- **Problem:** Number of **states** grows exponentially in the size of the system.
- **Answer:** Use **abstract** model of system
- **Problem:** Relationship of results on abstract model to real system?

# LTL Model Checking

- **Model Checking Problem:** Given model  $\mathcal{M}$  and logical property  $\varphi$  of  $\mathcal{M}$ , does  $\mathcal{M} \models \varphi$ ?
- Given transition system with states  $Q$ , transition relation  $\delta$  and initial state  $I$ , say  $(Q, \delta, I) \models \varphi$  for LTL formula  $\varphi$  if every run of  $(Q, \delta, I)$ ,  $\sigma$  satisfies  $\sigma \models \varphi$ .

## Theorem

*The Model Checking Problem for finite transition systems and LTL formulae is decidable.*

- Treat states  $q \in Q$  as letters in an alphabet.
- Language of  $(Q, \delta, I)$ ,  $\mathcal{L}(Q, \delta, I)$  (or  $\mathcal{L}(Q)$  for short) is set of runs in  $Q$
- Language of  $\varphi$ ,  $\mathcal{L}\varphi = \{\sigma \mid \sigma \models \varphi\}$
- Question:  $\mathcal{L}(Q) \subseteq \mathcal{L}\varphi$ ?
- Same as:  $\mathcal{L}(Q) \cap \mathcal{L}(\neg\varphi) = \emptyset$ ?