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

April 11, 2014
Example: Traffic Light

\[ V = \{ \text{Turn, NSC, EWC} \}, \quad F = \{ \text{NS, EW, Red, Yellow, Green} \} \text{ (all arity 0),} \]
\[ R = \{ = \} \]

\[ \text{NSG} \quad \text{Turn} = \text{NS} \land \text{NSC} = \text{Red} \rightarrow \text{NSC} := \text{Green} \]
\[ \text{NSY} \quad \text{NSC} = \text{Green} \rightarrow \text{NSC} := \text{Yellow} \]
\[ \text{NSR} \quad \text{NSC} = \text{Yellow} \rightarrow (\text{Turn, NSC}) := (\text{EW, Red}) \]
\[ \text{EWG} \quad \text{Turn} = \text{EW} \land \text{EWC} = \text{Red} \rightarrow \text{EWC} := \text{Green} \]
\[ \text{EWY} \quad \text{EWC} = \text{Green} \rightarrow \text{EWC} := \text{Yellow} \]
\[ \text{EWR} \quad \text{EWC} = \text{Yellow} \rightarrow (\text{Turn, EWC}) := (\text{NS, Red}) \]

\[ \text{init} = (\text{NSC} = \text{Red} \land \text{EWC} = \text{Red} \land (\text{Turn} = \text{NS} \lor \text{Turn} = \text{EW})) \]
Example: Traffic Lights

- **2GG**
  - $\{ \text{Turn} = \text{NS} \}
  - $\{ \text{NSC} = \text{Red} \}
  - $\{ \text{EWC} = \text{Red} \}$

- **2GY**
  - $\{ \text{Turn} = \text{EW} \}
  - $\{ \text{NSC} = \text{Red} \}
  - $\{ \text{EWC} = \text{Green} \}$

- **2YY**
  - $\{ \text{Turn} = \text{EW} \}
  - $\{ \text{NSC} = \text{Red} \}
  - $\{ \text{EWC} = \text{Yellow} \}$

- **2YR**
  - $\{ \text{Turn} = \text{EW} \}
  - $\{ \text{NSC} = \text{Red} \}
  - $\{ \text{EWC} = \text{Green} \}$

- **1GY**
  - $\{ \text{Turn} = \text{NS} \}
  - $\{ \text{NSC} = \text{Green} \}
  - $\{ \text{EWC} = \text{Red} \}$

- **1YY**
  - $\{ \text{Turn} = \text{NS} \}
  - $\{ \text{NSC} = \text{Yellow} \}
  - $\{ \text{EWC} = \text{Red} \}$

- **1YR**
  - $\{ \text{Turn} = \text{NS} \}
  - $\{ \text{NSC} = \text{Red} \}
  - $\{ \text{EWC} = \text{Green} \}$

- **1RG**
  - $\{ \text{Turn} = \text{NS} \}
  - $\{ \text{NSC} = \text{Red} \}
  - $\{ \text{EWC} = \text{Red} \}$
Examples (cont)

- LTS for traffic light has $3 \times 3 \times 2 = 18$ possible well-typed states
  - Is it possible to reach a state where $NSC \neq Red \land EWC \neq Red$ from an initial state?
  - If so, what sequence of actions allows this?
  - Do all the immediate predecessors of a state where $NSC = Green \lor EWC = Green$ satisfy $NSC = Red \land EWC = Red$?
  - If not, are any of those offend states reachable from an initial state, and if so, how?

- LTS for Mutual Exclusion has $6 \times 6 \times 2 \times 2 = 144$ possible well-typed states.
  - Is it possible to reach a state where $pc_1 = m5 \land pc_2 = n5$?

- How can we state these questions rigorously, formally?
- Can we find an algorithm to answer these types of questions?
Linear Temporal Logic - Syntax

\[ \varphi ::= p \mid (\varphi) \mid \neg \varphi \mid \varphi \land \varphi' \mid \varphi \lor \varphi' \mid \varnothing \varphi \mid \varphi U \varphi' \mid \varphi V \varphi' \mid \square \varphi \mid \lozenge \varphi \]

- \( p \) – a proposition over state variables
- \( \varnothing \varphi \) – “next”
- \( \varphi U \varphi' \) – “until”
- \( \varphi V \varphi' \) – “releases”
- \( \square \varphi \) – “box”, “always”, “forever”
- \( \lozenge \varphi \) – “diamond”, “eventually”, “sometime”
LTL Semantics: The Idea

\[ p \rightarrow p \]

\[ \circ \varphi \rightarrow \varphi \]

\[ \varphi U \psi \rightarrow \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \psi \]

\[ \varphi V \psi \rightarrow \psi \psi \psi \psi \psi \psi \varphi, \psi \]

\[ \Box \varphi \rightarrow \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \varphi \]

\[ \Diamond \varphi \rightarrow \varphi \]

Elsa L Gunter ()

CS477 Formal Software Development Method
Formal LTL Semantics

Given:

- $G = (V, F, af, R, ar)$ signature expressing state propositions
- $Q$ set of states,
- $M$ modeling function over $Q$ and $G$: $M(q, p)$ is true iff $q$ models $p$. Write $q \models p$.
- $\sigma = q_0 q_1 \ldots q_n \ldots$ infinite sequence of state from $Q$.
- $\sigma^i = q_i q_{i+1} \ldots q_n \ldots$ the $i^{th}$ tail of $\sigma$

Say $\sigma$ models LTL formula $\varphi$, write $\sigma \models \varphi$ as follows:

- $\sigma \models p$ iff $q_0 \models p$
- $\sigma \models \neg \varphi$ iff $\sigma \not\models \varphi$
- $\sigma \models \varphi \land \psi$ iff $\sigma \models \varphi$ and $\sigma \models \psi$.
- $\sigma \models \varphi \lor \psi$ iff $\sigma \models \varphi$ or $\sigma \models \psi$. 

Elsa L Gunter (CS477 Formal Software Development Methods) April 11, 2014
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 \( i \), \( \sigma^i \models \psi \)
- \( \sigma \models \Diamond \varphi \) if for some \( i \), \( \sigma^i \models \psi \)
Some Common Combinations

- $\square \Diamond p$ “$p$ will hold infinitely often”
- $\Diamond \Box p$ “$p$ will continuously hold from some point on”
- $(\square p) \Rightarrow (\Box q)$ “if $p$ happens infinitely often, then so does $q$"
Some Equivalences

- $\Box(\varphi \land \psi) = (\Box \varphi) \land (\Box \psi)$
- $\Diamond(\varphi \lor \psi) = (\Diamond \varphi) \lor (\Diamond \psi)$
- $\Box \varphi = F \lor \varphi$
- $\Diamond \varphi = T \lor \varphi$
- $\varphi \lor \psi = \neg((\neg \varphi) \lor (\neg \psi))$
- $\varphi \lor \psi = \neg((\neg \varphi) \lor (\neg \psi))$
- $\neg(\Diamond \varphi) = \Box(\neg \varphi)$
- $\neg(\Box \varphi) = \Diamond(\neg \varphi)$
Some More Equivalences

- $\square \varphi = \varphi \land \circ \square \varphi$
- $\Diamond \varphi = \varphi \lor \circ \Diamond \varphi$
- $\varphi \lor \psi = (\varphi \land \psi) \lor (\psi \land \circ (\varphi \lor \psi))$
- $\varphi \cup \psi = \psi \lor (\varphi \land \circ (\varphi \lor \psi))$

- $\square$, $\Diamond$, $\cup$, $\lor$ may all be understood recursively, by what they state about right now, and what they state about the future.

- Caution: $\square$ vs $\Diamond$, $\cup$ vs $\lor$ differ in their limit behavior
Basic Behavior:

- $\Box(( NSC = \text{Red} ) \lor ( NSC = \text{Green} ) \lor ( NSC = \text{Yellow} ))$
- $\Box(( NSC = \text{Red} ) \Rightarrow (( NSC \neq \text{Green} ) \land ( NSC \neq \text{Yellow} )))$
- Similarly for \text{Green} and \text{Red}

- $\Box(( ( NCS = \text{Red} ) \land \Diamond ( NCS \neq \text{Red} )) \Rightarrow \Diamond ( NCS = \text{Green} ))$
- Same as $\Box(( NCS = \text{Red} ) \Rightarrow (( NCS = \text{Red} ) \cup ( NCS = \text{Green} )))$
- $\Box(( ( NCS = \text{Green} ) \land \Diamond ( NCS \neq \text{Green} )) \Rightarrow \Diamond ( NCS = \text{Yellow} ))$
- $\Box(( ( NCS = \text{Yellow} ) \land \Diamond ( NCS \neq \text{Yellow} )) \Rightarrow \Diamond ( NCS = \text{Red} ))$
- Same for \text{EWC}
Traffic Light Example

Basic Safety

- $\Box((\text{NSC} = \text{Red}) \lor (\text{EWC} = \text{Red}))$
- $\Box((\text{NSC} = \text{Red}) \land (\text{EWC} = \text{Red})) \lor ((\text{NSC} \neq \text{Green}) \Rightarrow (\Diamond(\text{NSC} = \text{Green}))))$

Basic Liveness

- $(\Diamond(\text{NSC} = \text{Red})) \land (\Diamond(\text{NSC} = \text{Green})) \land (\Diamond(\text{NSC} = \text{Yellow})))$
- $(\Diamond(\text{EWC} = \text{Red})) \land (\Diamond(\text{EWC} = \text{Green})) \land (\Diamond(\text{EWC} = \text{Yellow})))$
Proof System for LTL

- First step: View $\varphi V \psi$ as macro: $\varphi V \psi = \neg((\neg \varphi) U (\neg \psi))$
- Second Step: Extend all rules of Prop Logic to LTL
- Third Step: Add one more rule: $\square \varphi$ Gen $\varphi$
- Fourth Step: Add a collection of axioms (a sufficient set of 8 exists)
  - A1: $\square \varphi \iff \neg (\Diamond (\neg \varphi))$
  - A2: $\square (\varphi \Rightarrow \psi) \Rightarrow (\square \varphi \Rightarrow \square \psi)$
  - A3: $\square \varphi \Rightarrow (\varphi \land \circ \square \varphi)$
  - A4: $\circ \neg \varphi \iff \neg \circ \varphi$
  - A5: $\circ (\varphi \Rightarrow \psi) \Rightarrow (\circ \varphi \Rightarrow \circ \psi)$
  - A6: $\square (\varphi \Rightarrow \circ \varphi) \Rightarrow (\varphi \Rightarrow \square \varphi)$
  - A7: $\varphi U \psi \iff (\varphi \land \psi) \lor (\varphi \land \circ (\varphi V \psi))$
  - A8: $\varphi U \psi \Rightarrow \Diamond \psi$

- 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; or A a proof system, B a subsystem.
Exercise: $\varphi \land \psi \Rightarrow \Box \varphi \land \Box \psi$
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 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 $M$ and logical property $\varphi$ of $M$, does $M \models \varphi$?

- Given transition system with states $Q$, transition relation $\delta$ and initial state 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 $(Q, \delta, I)$, $L(Q, \delta, I)$ (or $L(Q)$ for short) is set of runs in $Q$.
- Language of $\varphi$, $L\varphi = \{\sigma | \sigma \models \varphi\}$
- Question: $L(Q) \subseteq L(\varphi)$?
- Same as: $L(Q) \cap L(\neg \varphi) = \emptyset$?