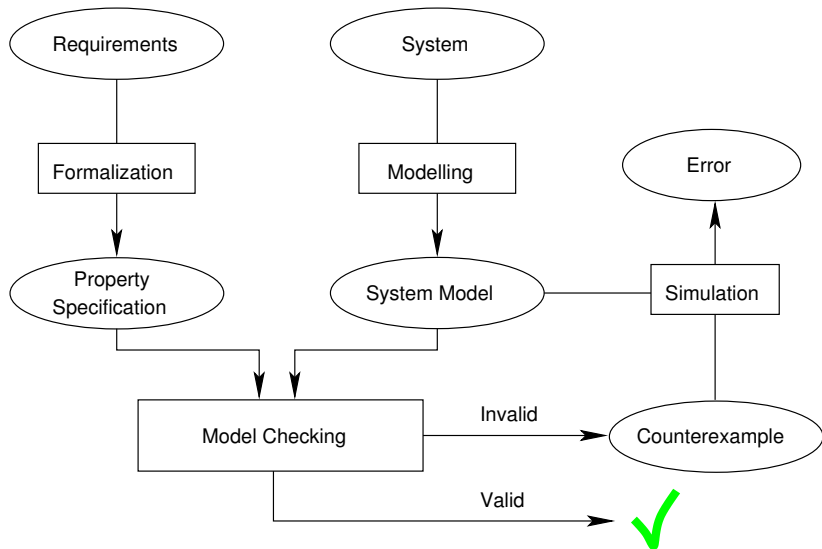


Model Checking – Schema



Model Checkers

- Software tools that can decide validity of a formula over a model of system under verification.
- SPIN, UppAal, SMV, Prism, DIVINE ...

Modelling Languages

- Processes described as extended finite state machines.
- Extension allows to use shared or local variables and guard execution of a transition with a Boolean expression.
- Optionally, some transitions may be synchronised with transitions of other finite state machines/processes.

Temporal Operators of LTL

- $F \varphi$ — φ holds true eventually (Future).
- $G \varphi$ — φ holds true all the time (Globally).
- $\varphi U \psi$ — φ holds true until eventually ψ holds true (Until).
- $X \varphi$ — φ is valid after execution of one transition (Next).
- $\varphi R \psi$ — ψ holds true until $\varphi \wedge \psi$ holds true (Release).
- $\varphi W \psi$ — until, but ψ may never become true (Weak Until).

Graphical Representation of LTL Temporal Operators

$$X\varphi : \bullet \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \dots$$

$$\varphi U \psi : \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \bullet \dots$$

$$F\varphi : \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \bullet \dots$$

$$G\varphi : \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \dots$$

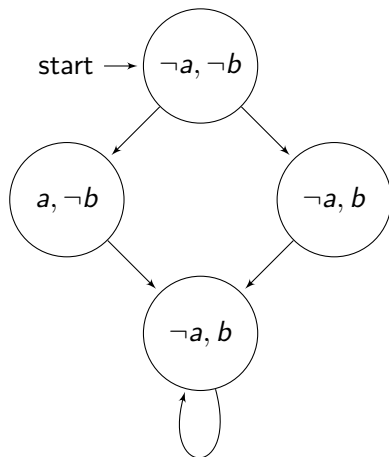
$$\begin{array}{l} \varphi R \psi : \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\varphi \wedge \psi}{\bullet} \longrightarrow \bullet \dots \quad \text{or} \\ \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \dots \end{array}$$

$$\begin{array}{l} \varphi W \psi : \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\psi}{\bullet} \longrightarrow \bullet \dots \quad \text{or} \\ \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \longrightarrow \overset{\varphi}{\bullet} \dots \end{array}$$

What is true in this system?

- $\neg a \wedge b$
- $F a$
- $\neg a U b$
- $G b$
- $F G b$

If not, show a counterexample.



- $X \text{ rain}$
- $F \text{ rain}$
- $\text{pick-up } R \text{ kin-gar}$
- $G(\text{drop-off} \implies (\text{kin-gar } U \text{ pick-up}))$
- $G(\neg(cs_1 \wedge cs_2))$
- $G(\text{req} \implies F \text{ resp}) \dots$ Does it guarantee that $\#_{\text{req}} = \#_{\text{resp}}$?
- $G F \text{ chocolate}$
- $(G F \text{ req}) \implies (G F \text{ resp})$
- $\text{sin} \implies (F G \text{ hell})$
- $F(\text{sin} \wedge (\neg \text{confession } U \text{ death})) \implies (F G \text{ hell})$

You have two fish, say Alice (A) and Bob (B). There is an aquarium divided into two parts: left (L) and right (R). Both fish start on the right side of the aquarium and do the following sequence of steps (independently): They move to the left, eat, move back to the right. Formulate using LTL:

- Whenever Alice eats, she is on the left
- Whenever Bob is on the left, he will eat eventually
- Whenever Bob eats, he will immediately go to the left
- If Alice do not eat before Bob, she will never eat
- Alice and Bob will never be on the same side from some point
- Bob chases Alice until they both eat together

Note and discuss that

- $\psi \implies \varphi \text{ U } \psi$
- $\psi \text{ U } \psi \equiv \psi$
- $\text{true U } \varphi \equiv \text{F } \varphi$
- $(\neg \psi) \text{ U } \psi \equiv \text{F } \psi$
- $\neg(\text{X } \varphi) \equiv \text{X } \neg \varphi$
- $\neg(\text{G } \varphi) \equiv \text{F } \neg \varphi$
- $\varphi \text{ W } \psi \equiv \varphi \text{ U } \psi \vee \text{G } \varphi$
- $\neg(\varphi \text{ R } \psi) \equiv \neg \varphi \text{ U } \neg \psi$
- $\varphi \text{ R } \psi \equiv \psi \text{ W } (\varphi \wedge \psi)$

Note and discuss that

- $F \varphi \equiv F (F \varphi)$
- $G \varphi \equiv G (G \varphi)$
- $\varphi U \psi \equiv \varphi U (\varphi U \psi)$
- $\varphi U \psi \equiv \psi \vee (\varphi \wedge X (\varphi U \psi))$
- $\varphi W \psi \equiv \psi \vee (\varphi \wedge X (\varphi W \psi))$
- $\varphi R \psi \equiv \psi \wedge (\varphi \vee X (\varphi R \psi))$
- $G \varphi \equiv \varphi \wedge X (G \varphi)$
- $F \varphi \equiv \varphi \vee X (F \varphi)$
- $X F \varphi \equiv F (X \varphi)$
- $X G \varphi \equiv G (X \varphi)$
- $X(\varphi U \psi) \equiv (X \varphi) U (X \psi)$

LTL properties - distributivity

Is it true that ...

$$\bullet X(\varphi \vee \psi) \stackrel{?}{\equiv} X\varphi \vee X\psi$$

$$\bullet X(\varphi \wedge \psi) \stackrel{?}{\equiv} X\varphi \wedge X\psi$$

$$\bullet F(\varphi \vee \psi) \stackrel{?}{\equiv} F\varphi \vee F\psi$$

$$\bullet F(\varphi \wedge \psi) \stackrel{?}{\equiv} F\varphi \wedge F\psi$$

$$\bullet G(\varphi \vee \psi) \stackrel{?}{\equiv} G\varphi \vee G\psi$$

$$\bullet G(\varphi \wedge \psi) \stackrel{?}{\equiv} G\varphi \wedge G\psi$$

$$\bullet \varphi U (\psi_1 \vee \psi_2) \stackrel{?}{\equiv} (\varphi U \psi_1) \vee (\varphi U \psi_2)$$

$$\bullet \varphi U (\psi_1 \wedge \psi_2) \stackrel{?}{\equiv} (\varphi U \psi_1) \wedge (\varphi U \psi_2)$$

$$\bullet (\varphi_1 \vee \varphi_2) U \psi \stackrel{?}{\equiv} (\varphi_1 U \psi) \vee (\varphi_2 U \psi)$$

$$\bullet (\varphi_1 \wedge \varphi_2) U \psi \stackrel{?}{\equiv} (\varphi_1 U \psi) \wedge (\varphi_2 U \psi)$$

$$GF(\varphi \vee \psi) \stackrel{?}{\equiv} GF\varphi \vee GF\psi$$

$$GF(\varphi \wedge \psi) \stackrel{?}{\equiv} GF\varphi \wedge GF\psi$$

$$FG(\varphi \vee \psi) \stackrel{?}{\equiv} FG\varphi \vee FG\psi$$

$$FG(\varphi \wedge \psi) \stackrel{?}{\equiv} FG\varphi \wedge FG\psi$$