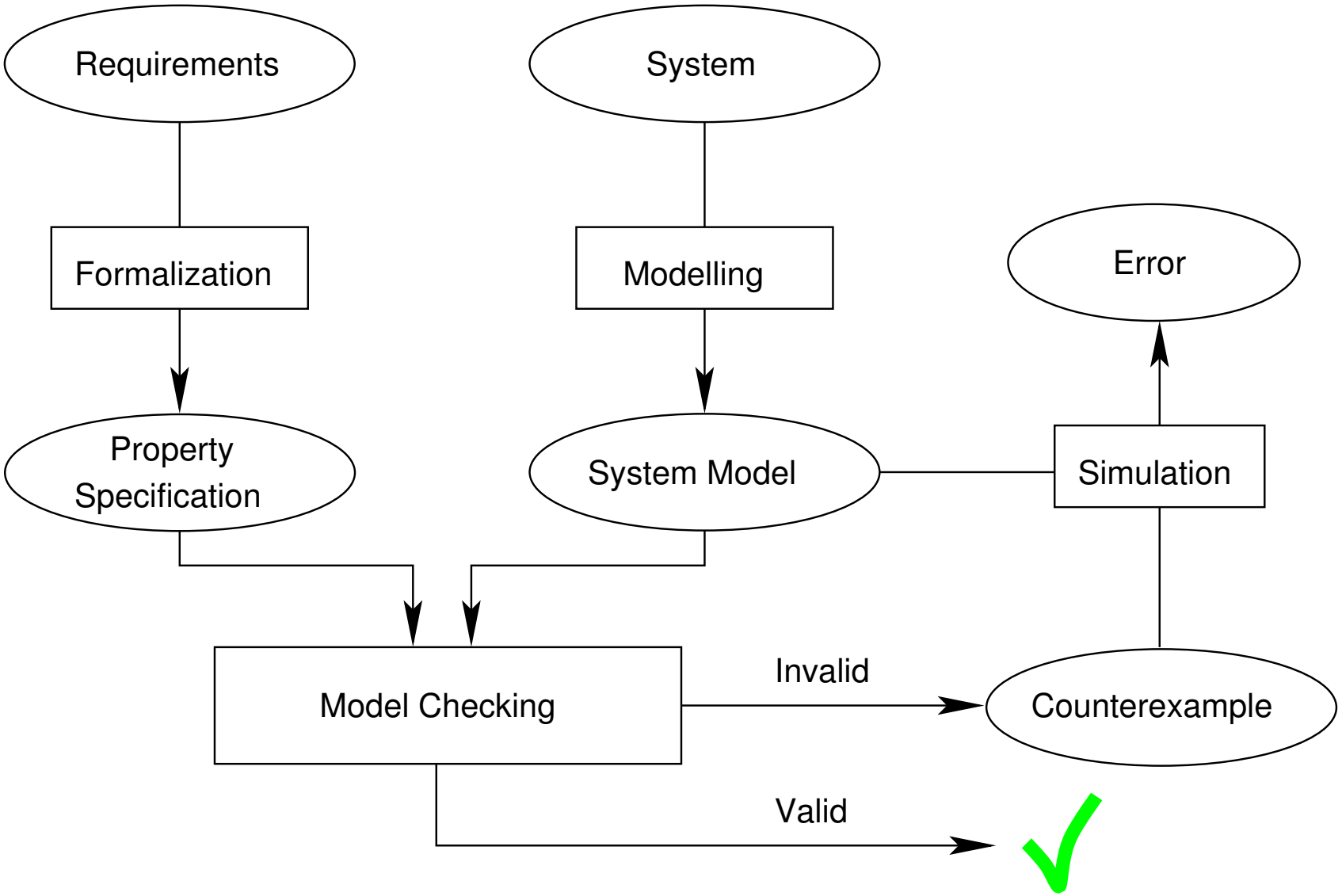
Model Checking – Schema



Automated Tools for Model Checking

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

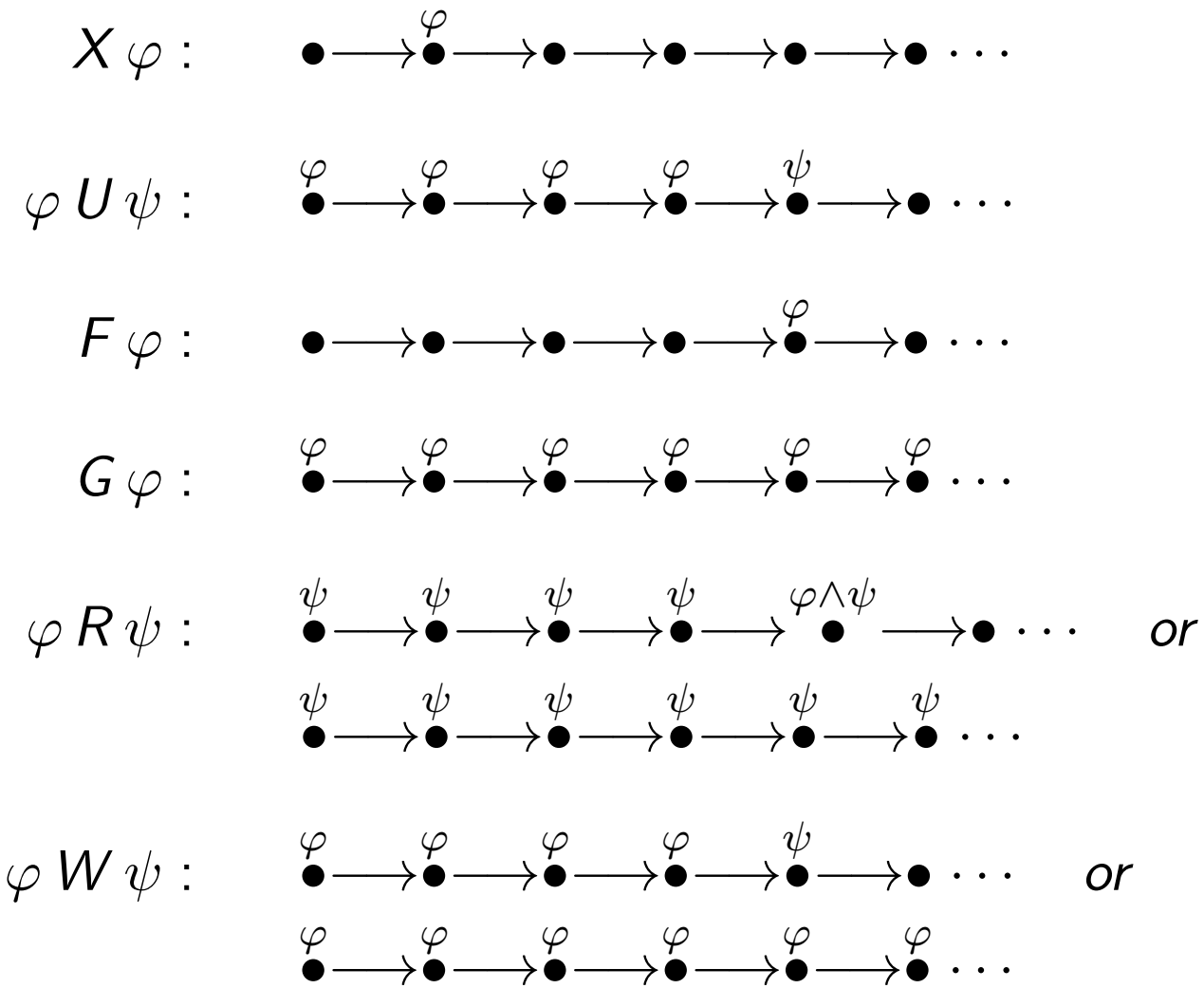
- Processes described as extended finite state machines.
- Extension allows to use shared or local variables and guard execution of a transition with a Boolean expression.
- Optionally, some transitions may be synchronised with transitions of other finite state machines/processes.

Linear Temporal Logic (LTL) Informally

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

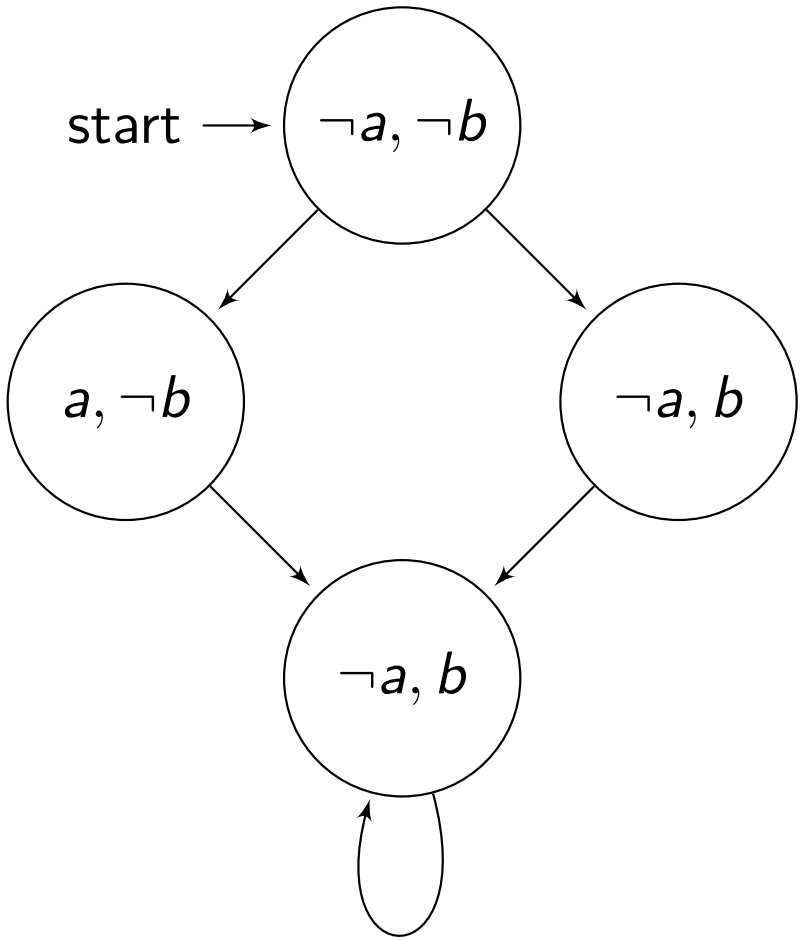


LTL examples

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.



LTL examples

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

LTL properties - example

You have two fishes, 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.

LTL properties - negation

Note and discuss that

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

LTL - temporal properties

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 questions

Is it true that ...

- $X(\varphi \vee \psi) \stackrel{?}{\equiv} X\varphi \vee X\psi$
- $X(\varphi \wedge \psi) \stackrel{?}{\equiv} X\varphi \wedge X\psi$
- $F(\varphi \vee \psi) \stackrel{?}{\equiv} F\varphi \vee F\psi$
- $F(\varphi \wedge \psi) \stackrel{?}{\equiv} F\varphi \wedge F\psi$
- $G(\varphi \vee \psi) \stackrel{?}{\equiv} G\varphi \vee G\psi$
- $G(\varphi \wedge \psi) \stackrel{?}{\equiv} G\varphi \wedge G\psi$
- $GF(\varphi \vee \psi) \stackrel{?}{\equiv} GF\varphi \vee GF\psi$
- $GF(\varphi \wedge \psi) \stackrel{?}{\equiv} GF\varphi \wedge GF\psi$
- $FG(\varphi \vee \psi) \stackrel{?}{\equiv} FG\varphi \vee FG\psi$
- $FG(\varphi \wedge \psi) \stackrel{?}{\equiv} FG\varphi \wedge FG\psi$
- $\varphi \, U \, (\psi_1 \vee \psi_2) \stackrel{?}{\equiv} (\varphi \, U \, \psi_1) \vee (\varphi \, U \, \psi_2)$
- $\varphi \, U \, (\psi_1 \wedge \psi_2) \stackrel{?}{\equiv} (\varphi \, U \, \psi_1) \wedge (\varphi \, U \, \psi_2)$
- $(\varphi_1 \vee \varphi_2) \, U \, \psi \stackrel{?}{\equiv} (\varphi_1 \, U \, \psi) \vee (\varphi_2 \, U \, \psi)$
- $(\varphi_1 \wedge \varphi_2) \, U \, \psi \stackrel{?}{\equiv} (\varphi_1 \, U \, \psi) \wedge (\varphi_2 \, U \, \psi)$