Temporal Logic

Specifications

&

Intro. Verification.

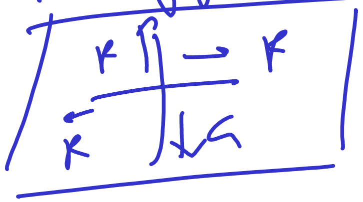
Temporal operators: X, G, F, U

Object: Specification over "behaviors"

behaviors: Sequence of states; each state satisfies some prop.

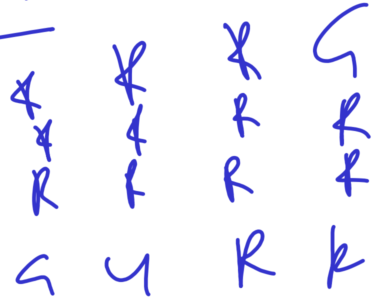
Infinite length

Traffic light



$G(\phi)$

$b_1 =$



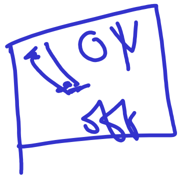
$b \models X(\phi)$

if $b[2]\ b[3]$ ——

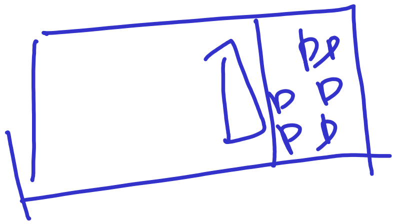
$\models \phi$

$b \models G(\phi)$ iff $\forall i: b[i] \models \phi$

Examples



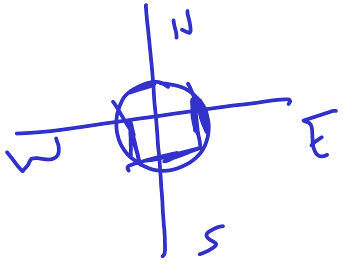
$\models G(state = on \lor state = off)$



$\models G(timer = 0 \Rightarrow state = off)$

$G((door = open) \Rightarrow (state = off))$

$G((state = on) \Rightarrow ((door = close) \land (timer > 0)))$



G (only one green) $\rightarrow$ G (atmost one green)

↳ Combined '$\vee$'

$(E = G \Rightarrow S \neq G \wedge W \neq G \wedge N \neq G) \wedge \ldots$ ( )

$\boxed{\text{Yellow}}$

$G(E = \text{Yellow} \Rightarrow X(E = \text{Red}))$

$G(\text{Green} \Rightarrow X\ \text{Yellow})$

a model b that

$b \models G(\phi)$ iff $\forall i$ $b[i]\ b[i+1] \ldots \models \phi$

Eventually: $F(\phi)$, $b \models F(\phi)$ iff

$\exists i: b[i] \ldots b[i+1] \ldots$

$\models \phi$ iff ϕ is s.t. $b[i:] \models \phi$

$F(\text{timer} = \text{done})$

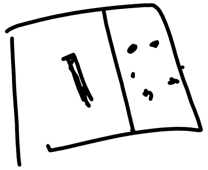
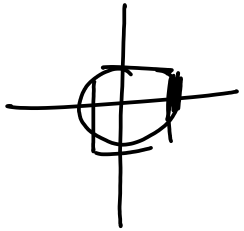
$\text{mode} = \text{on} \Rightarrow F(\text{timer} = \text{done})$

$E = \text{green}$? $F(E = \ldots)$

$F(E = \text{Green})$

$F(E = \text{Red})$

Toyota:

multiple

$\textcircled{G} F(E \wedge \text{Green})$ & $F(E \wedge \text{Green})$ $\rightarrow$ unreachable

$b \models G(\phi)$ iff $\forall i$ $b[i]\,b[i+1]\ldots \models \phi$

$\forall$ $b[i]\,b[i+1]\ldots$ —— $\models F(E \wedge \text{Green})$

$GF(\phi) \rightarrow$ ensure that ϕ is true multiple times

infinitely many

$t=1 \rightarrow t=2 \rightarrow t=3$ ——

$t=20$

$GF(\phi)$ is called infinitely often ϕ.

$GF(\phi)$ dual $FG(\phi)$ $\neg\phi$ $\neg\phi$ - ϕ ϕ ϕ -

Fairness

Weak

$$\boxed{GF(\phi) \equiv \neg FG(\neg\phi)}$$

Until Operator

X, G, F ϕ_1 : True

$\boxed{\phi_1 - -}$ ϕ_1 ϕ_2 - -

ϕ_2

$\sigma \models \phi_1 U \phi_2$ iff $\exists k$

$\forall i \leq k-1$ $b[i] \models \phi_1$

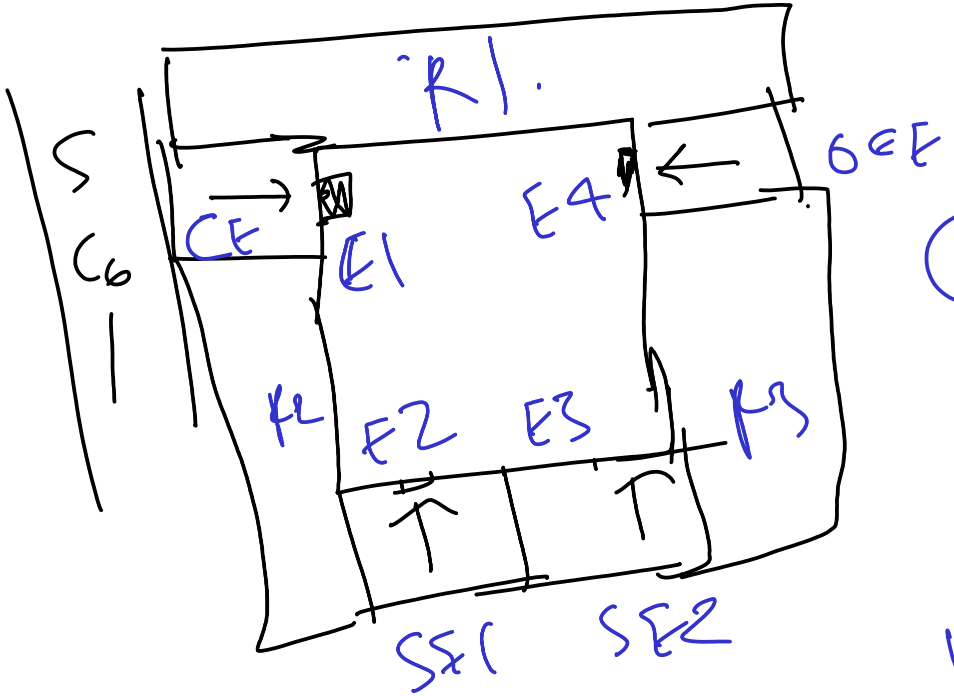
$b[k] \models \phi_2$

Factoid X, G, F, U, $\boxed{R, W,}$

X, U suffice

Reason : Capturing behavior in rigorous mathematical ways is a challenge.

Example



* How to specify the "correctness" of the drone behavior.

Using temporal logic

Specify Behaviors

(1) Input Output Spec

(1) Model of System $\Phi(I, O)$

(2) Spec $\Rightarrow$ $R(I, O)$

implementation

Requirement

$$\forall I, \Phi(I, O) \Rightarrow R(I, O)$$

$\forall I.\ \Phi(I, O) \Rightarrow R(I, O)$; I & O

Collection of Booleans.

affir

$\boxed{\exists I\ \ \phi(I, O) \land \neg R(I, O)}$

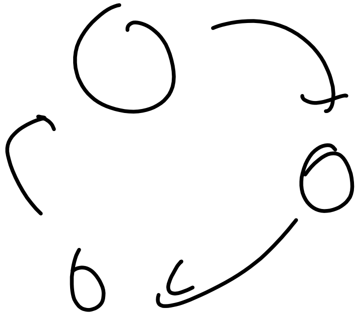
Search

SAT solvers

$\exists I\ \phi.\ \ \phi(I, O) \land \neg R(I, O)$

Satisfying assign

② Temporal logic Spec

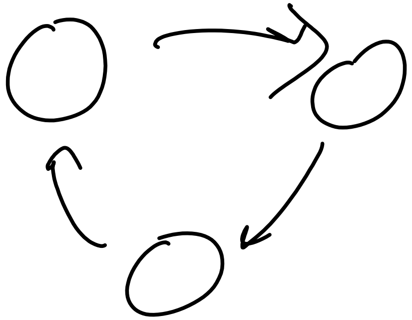
 $\models \Phi'$ → Linear Temporal Logic

Model Checking

$\text{System} \models M_{\Phi}$

Finite state m/c

Automata

$\Phi \xrightarrow{\text{monitor signals}}$  M_{Φ}