Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste
II Semestre 2019

Lecture 9: Signal Temporal Logic

[Many Slides due to J. Deshmukh, A. Donzé]

Linear Temporal Logic (LTL) specification

It is a logic interpreted over infinite discrete-time traces

E.g. **For the next 3 days** the highest temperature will be below 75 degree and the lowest temperature will be above 60 degree

$X\,(p \wedge q) \wedge X\,X\,(p \wedge q) \wedge X\,X\,X\,(p \wedge q)$ with $p = T<75$, $q=T>60$

Metric Interval Temporal Logic (STL)

Invented by R. Alur, T.Feder, T.A. Henzinger (1991)
It extended LTL by adding **dense time intervals**:

$$G_{[0,3]}(\mathrm{p} \wedge q)$$

Signal Temporal Logic (STL)

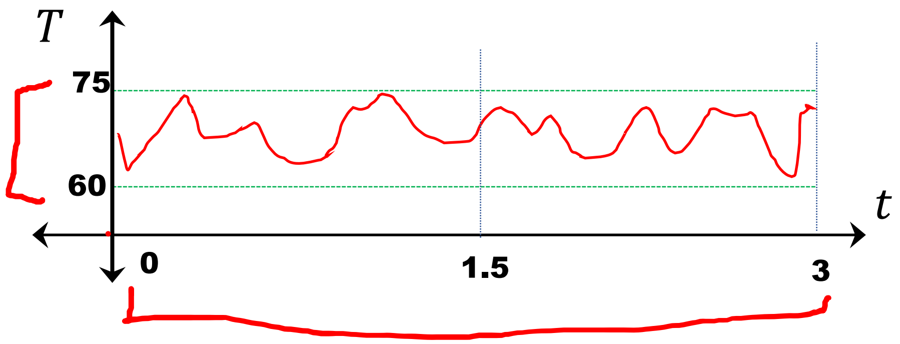
Invented by D. Nickovic and O. Maler from Verimag (2004)
It extended MITL by having **signal predicates over real values as atomic formulas:**

$$G_{[0,3]}(T < 75 \wedge T > 60)$$

Expressing specifications in STL

$\mathbf{Always}_{[0,3]}\ (60 < T < 75)$

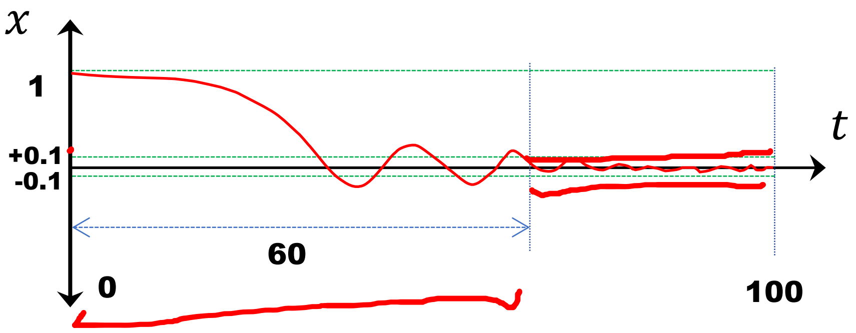
Always between time 0 and 3



$\mathbf{Eventually}_{[0,60]}(\mathbf{Always}\ (|x| < 0.1)\ )$

Eventually at **some time** ***t*** between time 0 and 60

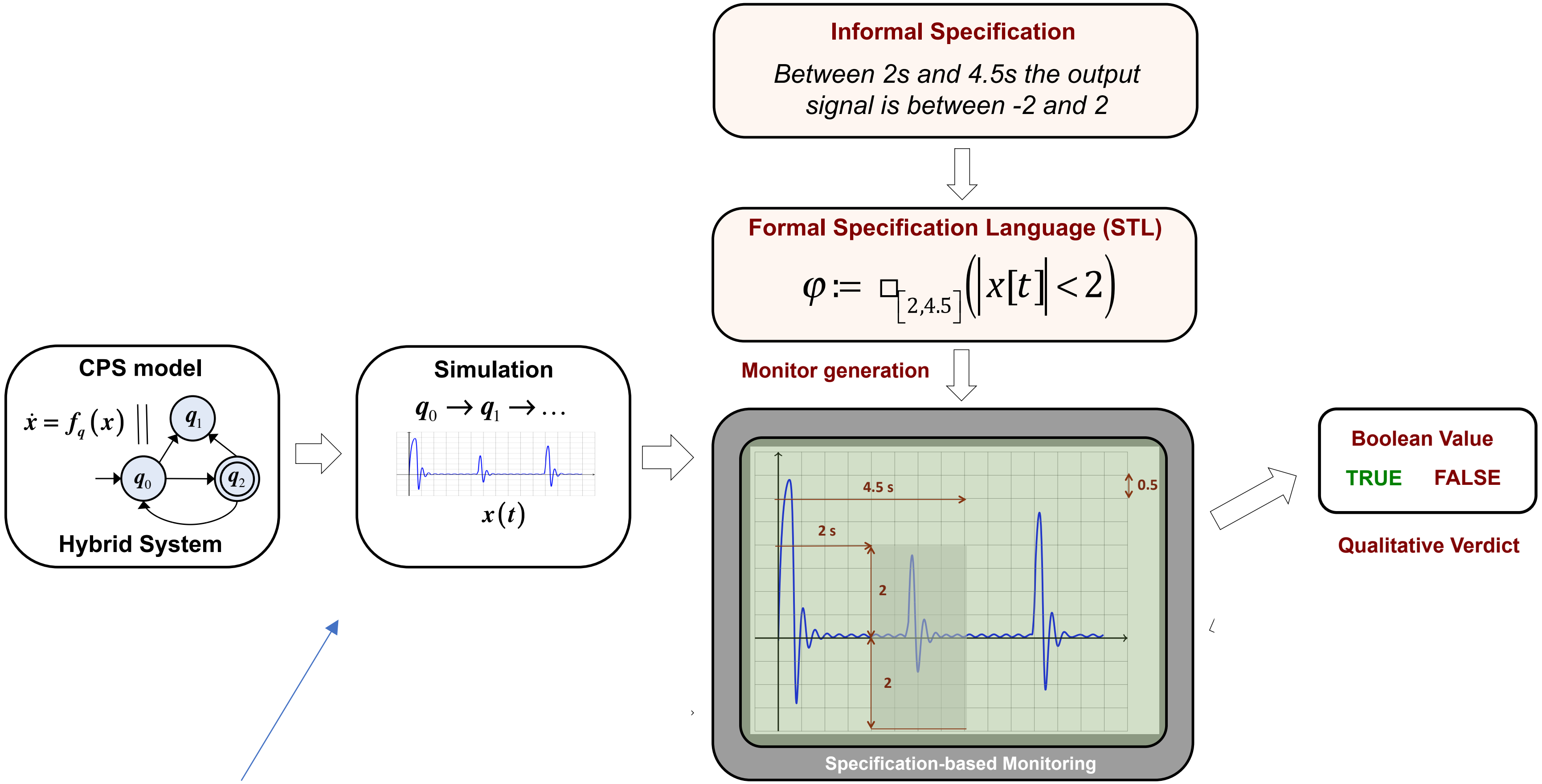
From that time ***t*,** always till the end of the signal trace



STL Syntax

Syntax of STL		
$\varphi ::= f(\mathbf{x}) \sim 0$	$\vert$	$f: \mathbb{D} \to \mathbb{R}$ is a function over the signal $\mathbf{x}$: $\mathbb{T} \to \mathbb{D}$,
		$\sim \in \{\leq, <, >, \geq, =, \neq\}$
$\neg\varphi$	$\vert$	Negation
$\varphi \wedge \varphi$	$\vert$	Conjunction
$\mathbf{F}_{[a,b]}\varphi$	$\vert$	At some **F**uture step in the interval $[a, b]$
$\mathbf{G}_{[a,b]}\varphi$	$\vert$	**G**lobally in all times in the interval $[a, b]$
$\varphi\ \mathbf{U}_{[a,b]}\ \varphi$	$\vert$	In all steps **U**ntil in interval $[a, b]$
$\varphi\ \boldsymbol{S}_{[a,b]}\ \varphi$	$\vert$	In all steps **S**ince in interval $[a, b]$

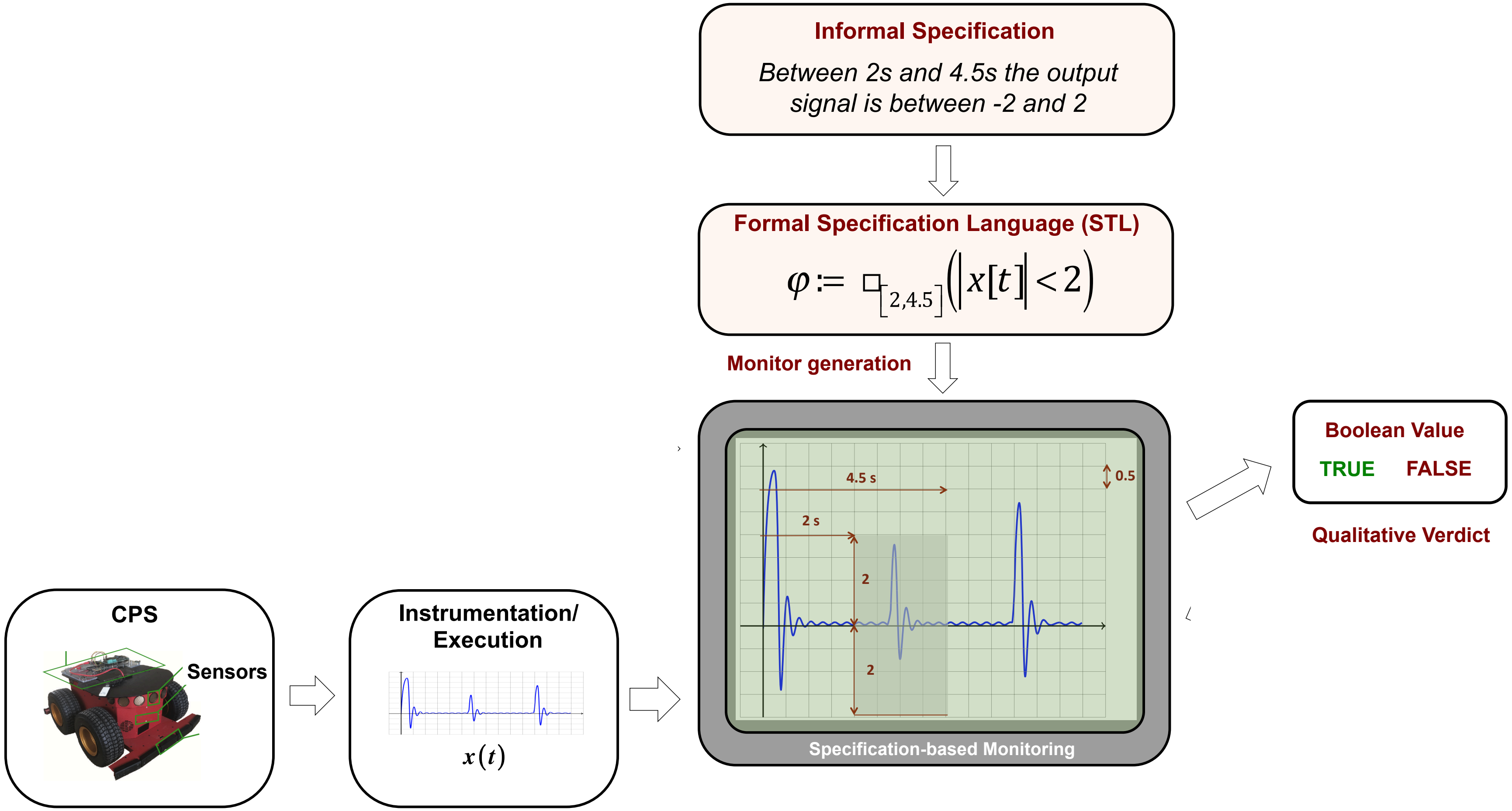
Specification-based Monitoring



Complex behaviours

Low dimensional vectors

Specification-based Monitoring



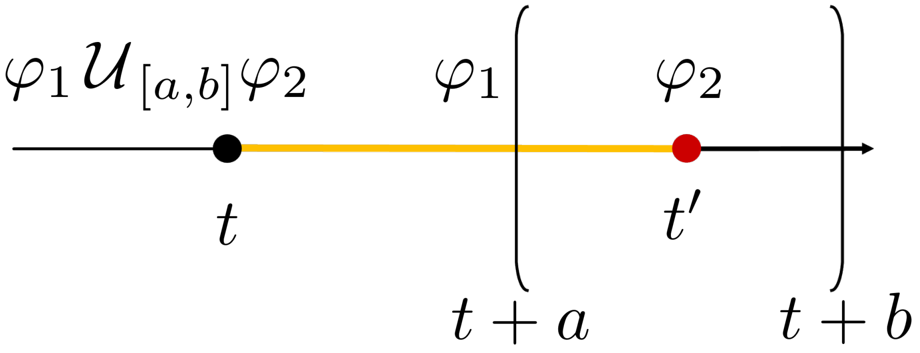
Recursive Boolean Semantics of STL

φ	$\beta(\varphi, \mathbf{x}, t)$
$f(\mathbf{x}) \sim 0$	$f(\mathbf{x}(t)) \sim 0$, $\quad \sim \in \{\leq, <, >, \geq, =, \neq\}$
$\neg\varphi$	$\neg\beta(\varphi, \mathbf{x}, t)$
$\varphi_1 \wedge \varphi_2$	$\beta(\varphi_1, \mathbf{x}, \mathrm{t}) \wedge \beta(\varphi_2, \mathbf{x}, \mathrm{t})$
$\mathbf{F}_{[a,b]}\varphi$	$\exists\tau \in [t+a, t+b]\ \beta(\varphi, \mathbf{x}, \tau)$
$\mathbf{G}_{[a,b]}\varphi$	$\forall\tau \in [t+a, t+b]\ \beta(\varphi, \mathbf{x}, \tau)$
$\varphi\ \mathbf{U}_{[a,b]}\ \psi$	$\exists\tau \in [t+a, t+b]\left(\beta(\psi, \mathbf{x}, \tau) \wedge \forall\tau' \in [t, \tau)\ \beta(\varphi, x, \tau')\right)$
$\varphi\ \mathbf{S}_{[a,b]}\ \psi$	$\exists\tau \in [t-a, t-b]\left(\beta(\psi, \mathbf{x}, \tau) \wedge \forall\tau' \in (\tau, t]\ \beta(\varphi, x, \tau')\right)$

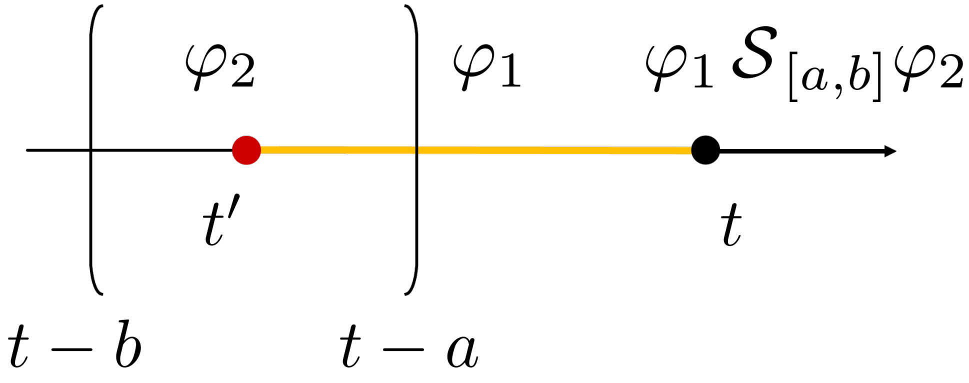
$$\beta(\varphi, \mathbf{x}) = \beta(\varphi, \mathbf{x}, 0)$$

Since and Until Operators

- Until



- Since

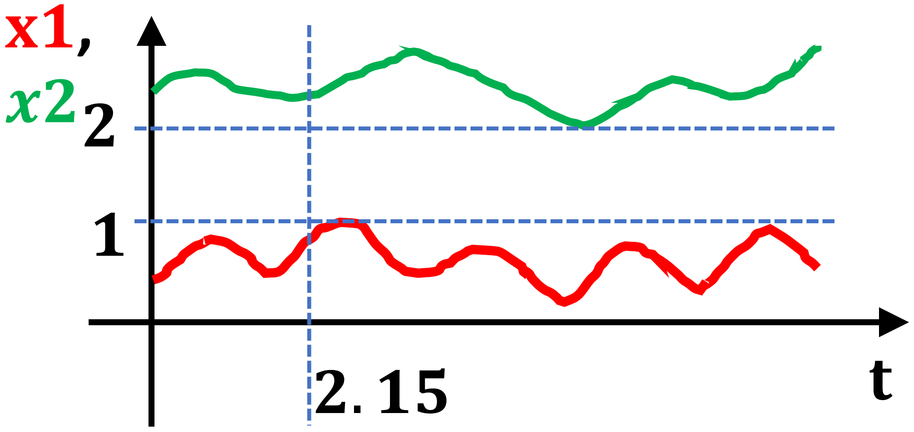


STL semantics

- Semantics of STL specified recursively over a signal $\mathbf{x}\colon \mathbb{T} \to \mathbb{D}$ at each time,

For each STL formula φ, here's how we define it's semantics:

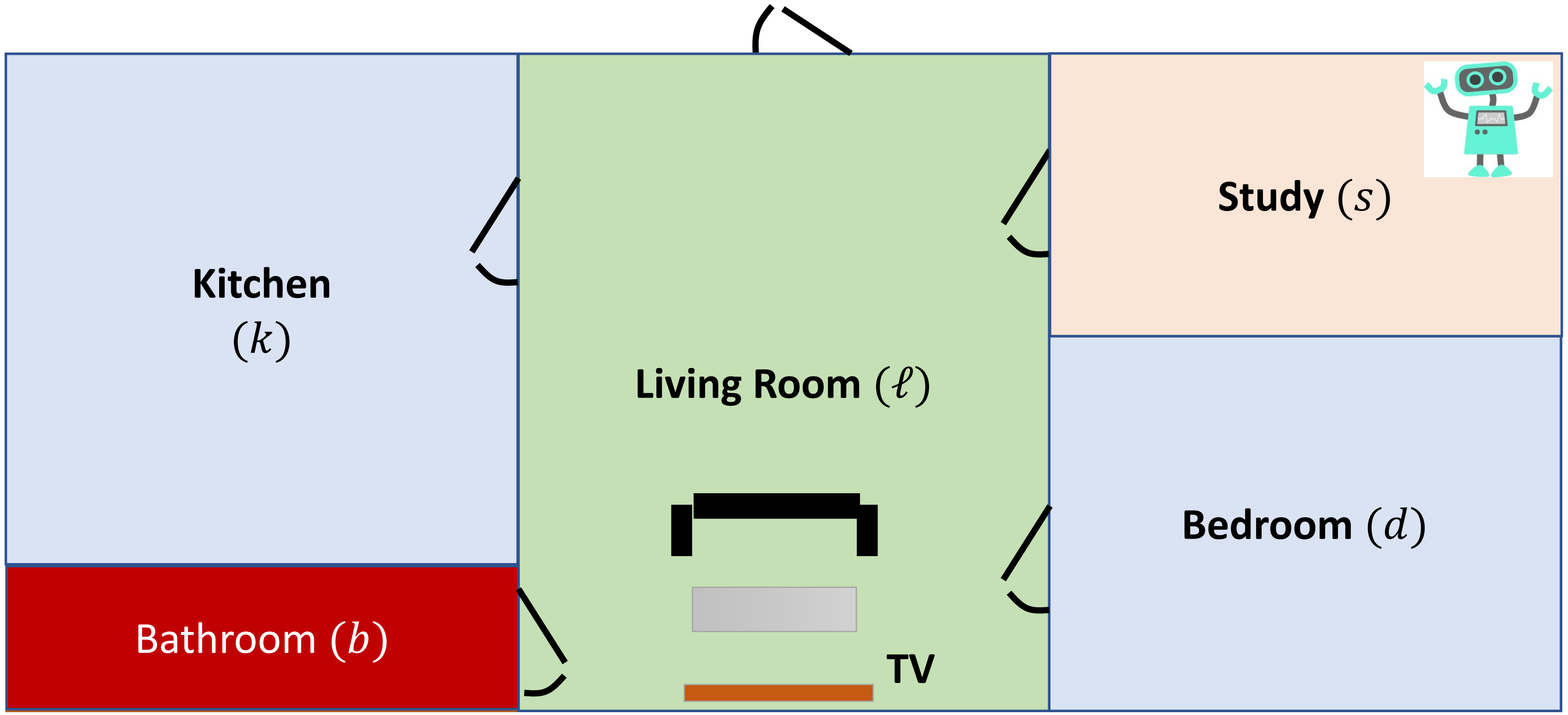
- If φ is the signal predicate $\mu = f(\mathbf{x}) > 0$, then
  $\beta(\varphi, \mathbf{x}, t) = true$ iff $f\big(\mathbf{x}(t)\big) > 0$



$$\mathbf{x} = (x1, x2)$$
$$\boldsymbol{f} = x2 - x1 - 1$$
$$\beta(f(\mathbf{x}) > 0, \mathbf{x}, 2.15)?$$

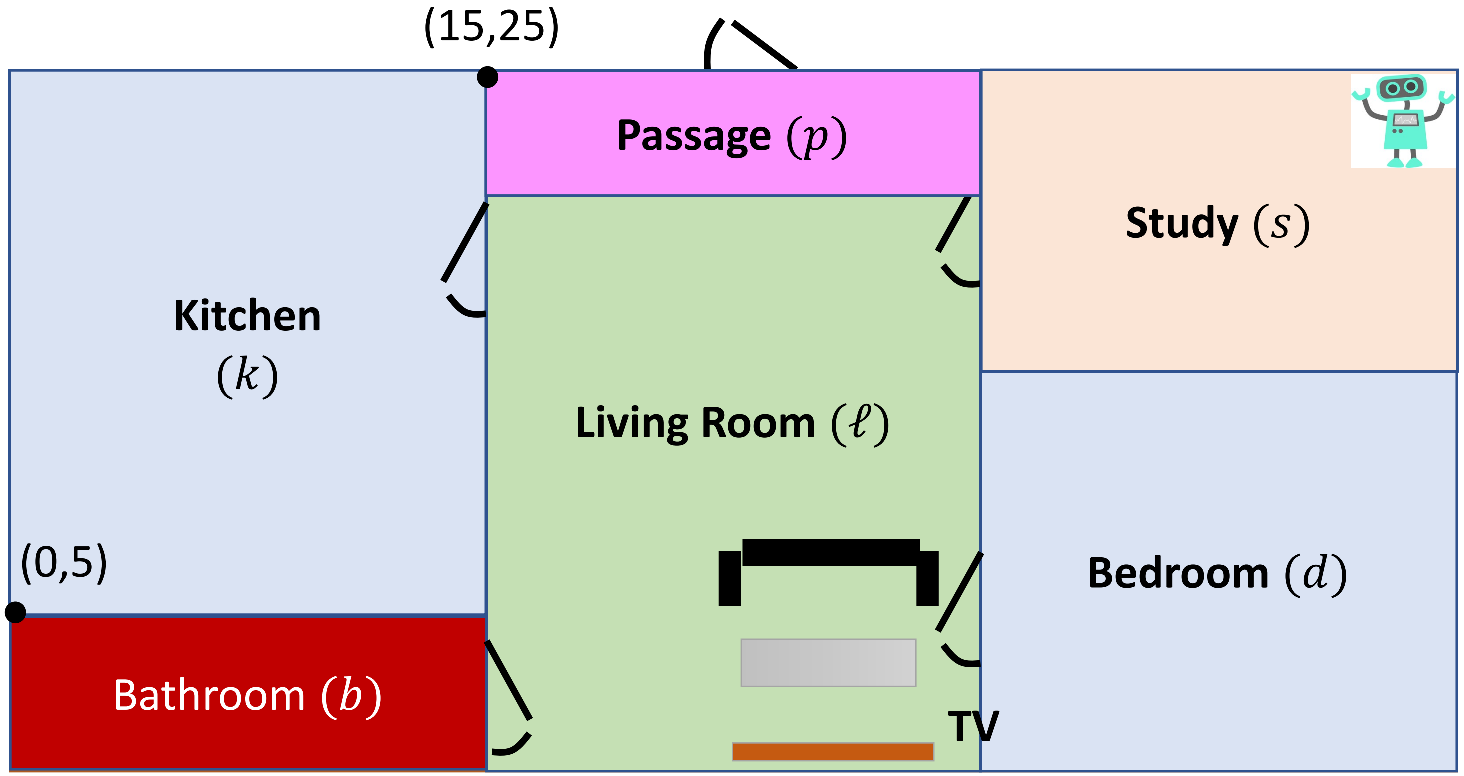
Example specifications in LTL

- Suppose you are designing a robot that has to do a number of missions



- Whenever the robot visits the kitchen, it should visit the bedroom after.
  $$\mathbf{G}(k_r \Rightarrow \mathbf{F}\ d_r)$$
- Robot should never go to the bathroom.
  $$\mathbf{G}\neg b_r$$
- The robot should keep working until its battery becomes low
  $$working\ \mathbf{U}\ low\_battery$$

Robot Path Specification



$$p(t) \in B_k \;:\; (0 < p_x(t) < 15) \wedge \left(5 < p_y(t) < 25\right)$$

- Whenever the robot visits the kitchen, it should visit the bedroom within the next 15 mins.

$$\mathbf{G}\left((p(t) \in B_k) \Rightarrow \mathbf{F}_{[0,15]}(p(t) \in B_b)\right)$$

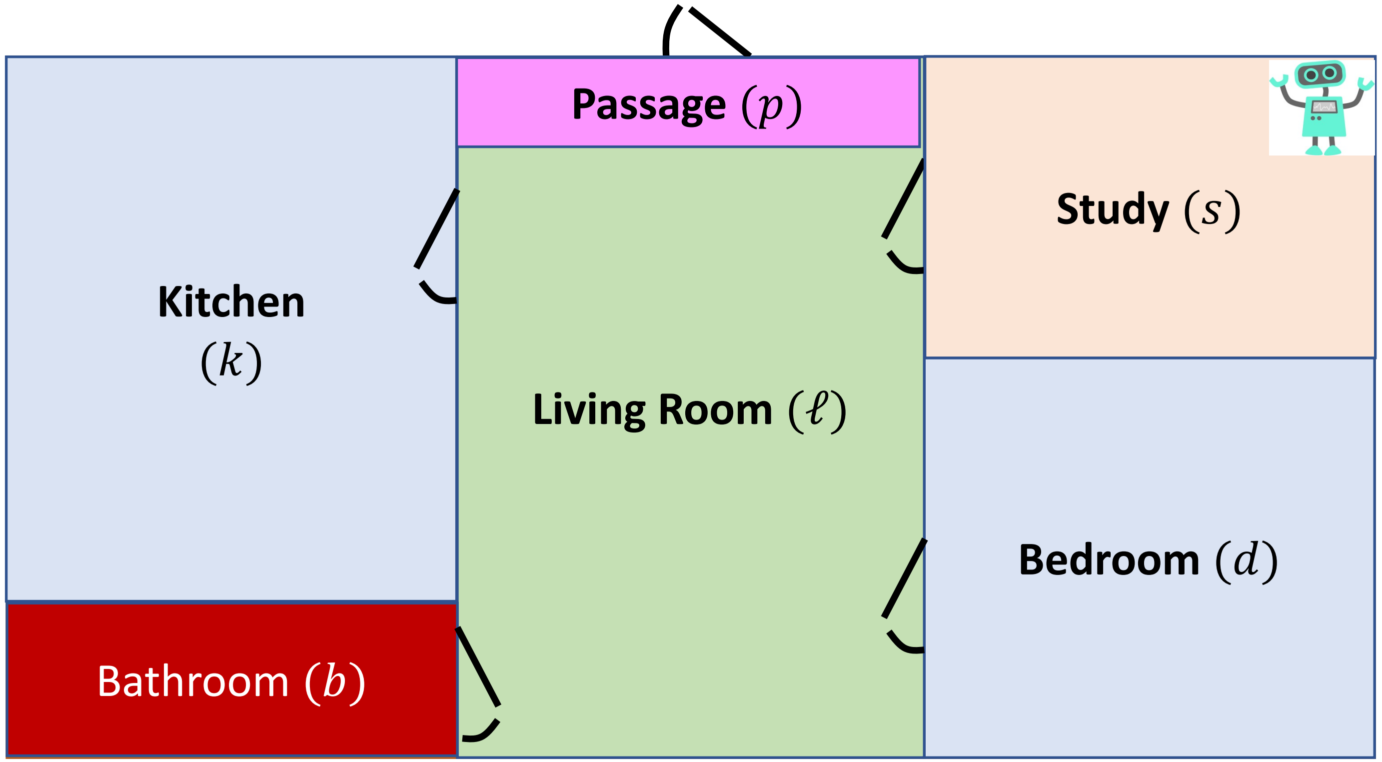
B_r: Box describing room r

$p(t)$: Position of robot at time t

- Robot should not go to the bathroom in the first 60 mins.

$$\mathbf{G}_{[0,60]}(p(t) \notin B_{bath})$$

Robot Path Specification



- The robot battery should last between 4 hours and 6 hours
  $(Q(t) \geq Q_{low})\ \mathbf{U}_{[240,360]}(Q(t) < Q_{low})$

- For the first 10 hours, the robot is never in any room for more than 30 minutes

$$\mathbf{G}_{[0,600]}\left(\bigwedge_r \big((p(t) \in B_r) \Rightarrow \mathbf{F}_{[0,30]}(p(t) \notin B_r)\big)\right)$$