Towards a formal language for systemic requirements

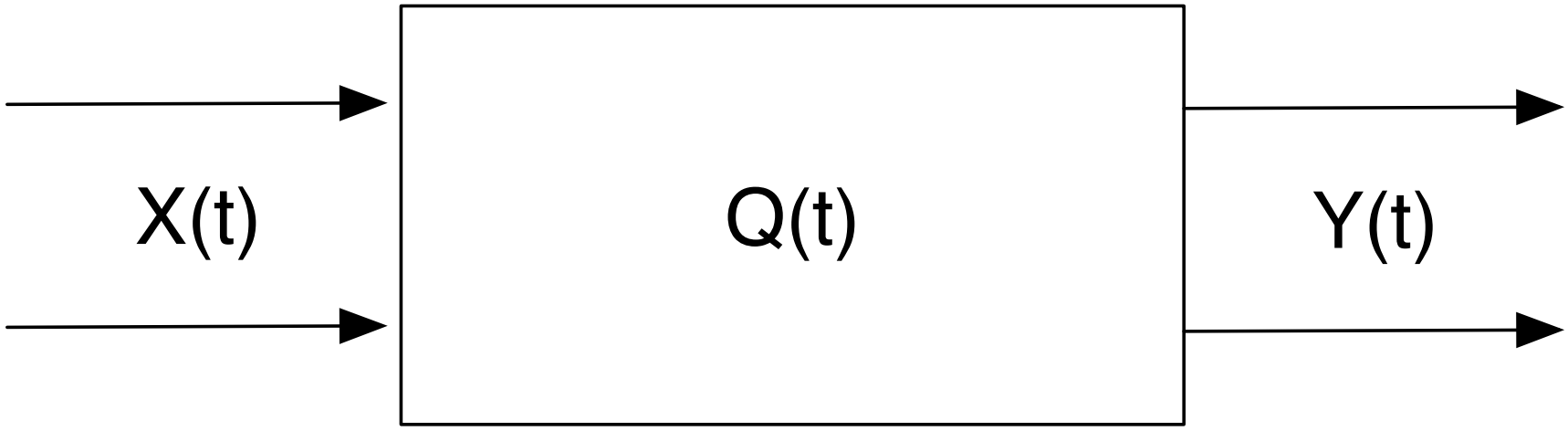
Yann Hourdel

LIX, École Polytechnique

yann.hourdel@polytechnique.edu

http://www.hourdel.fr

Our definition of a system



$$\int = (\mathbb{T}, X, Y, Q, q_0, \mathcal{F}, \delta)$$

state of $\int$: $s = (x, q, y) \in X \times Q \times Y$

execution of $\int$: $(s_0, s_1, \ldots) \in exec(\int)$

Core conditions

$$\phi ::= input(x)$$
$$\phi ::= istate(q)$$
$$\phi ::= ouput(y)$$

Minimal set of operators

$$\phi ::= \neg\, \phi'$$
$$\phi ::= \phi_1 \ \wedge \ \phi_2$$
$$\phi ::= \bigcirc\, \phi'$$
$$\phi ::= \phi_1\, \mathcal{U}\, \phi_2$$

Additionnal operators

$$\phi ::= \top$$
$$\phi ::= \bot$$
$$\phi ::= \phi_1 \ \vee \ \phi_2$$
$$\phi ::= \phi_1 \ \Rightarrow \ \phi_2$$
$$\phi ::= \phi_1 \ \otimes \ \phi_2$$
$$\ldots$$
$$\phi ::= \Diamond\, \phi'$$
$$\phi ::= \phi_1\, \mathcal{R}\, \phi_2$$

Computation rules

$$\frac{}{\big((x_0, \_, \_), \ldots\big) \vDash \mathit{input}(x_0)}\ [\mathrm{AI}]$$

$$\frac{}{\big((\_, q_0, \_), \ldots\big) \vDash \mathit{istate}(q_0)}\ [\mathrm{AS}]$$

$$\frac{}{\big((\_, \_, y_0), \ldots\big) \vDash \mathit{output}(y_0)}\ [\mathrm{AO}]$$

$$\frac{\big(e_1, e_2, \ldots\big) \vDash \phi}{\big(\_, e_1, e_2, \ldots\big) \vDash \bigcirc\phi}\ [\mathrm{AC}]$$

$$\frac{[e \vDash \phi] \Rightarrow \bot}{e \vDash \neg\phi}\ [\text{AN}] \qquad \frac{e \vDash \phi_1 \qquad e \vDash \phi_2}{e \vDash \phi_1 \wedge \phi_2}\ [\text{AW}]$$

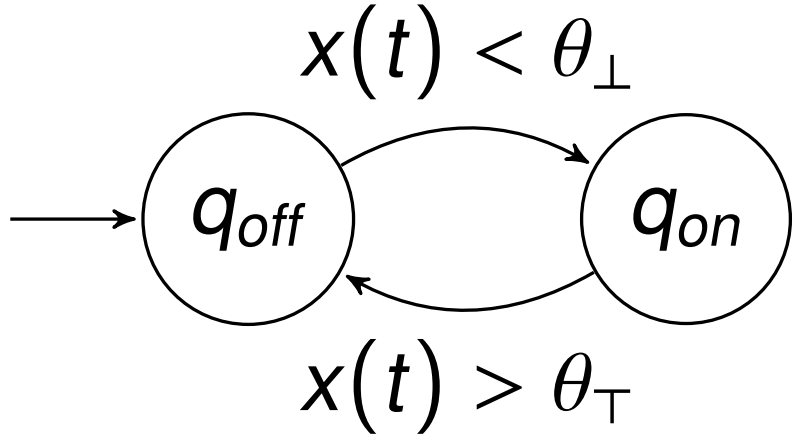
$$\frac{\exists i \leq 0, \left[\begin{array}{l}\Big((e_i, e_{i+1}, \ldots) \vDash \phi_2\Big) \\ \Big(\forall k \in \{0, \ldots, i\}, \big(e_k, e_{k+1}, \ldots\big) \vDash \phi_1\Big)\end{array}\right]}{\Big(e_0, e_1, \ldots\Big) \vDash \phi_1 \mathcal{U} \phi_2}\ [\text{AU}]$$

$\int$ satisfies ϕ iif

$$\int \vDash \phi \Leftrightarrow \forall e \in exec\Big(\int\Big), e \vDash \phi$$

Example: simple radiator

- $T \sim \mathbb{N}$
- $X =$ room temperature $\sim R$
- $Y = \{heat, nothing\}$
- $Q = \{q_{on}, q_{off}\}$, $q_0 = q_{off}$
- $\mathcal{F}(x(t), q(t)) = \begin{cases} heat \text{ if } q(t) = q_{on} \\ \varnothing \text{ otherwise} \end{cases}$



Some wanted properties for $\theta_\perp = 15$ and $\theta_\top = 20$

$$\int \vDash \neg\Diamond\Big(\mathit{istate}(q_{\mathit{off}}) \wedge \mathit{output}(\mathit{heat})\Big)$$

$$\int \vDash \neg\Diamond\Big(\mathit{input}(10) \wedge \bigcirc\mathit{istate}(q_{\mathit{off}})\Big)$$

$$\forall\theta > \theta_\top, \int \vDash \neg\Diamond\Big(\mathit{input}(\theta) \wedge \bigcirc\mathit{istate}(q_{\mathit{on}})\Big)$$

Conclusion

Built: a semantics of systems + formal definition of "properties" as timed behaviour constraints.

Next step: more advanced refinement computation language that could let modelers obtain a system from a set of such constraints.