Application: System Specification and Relations

Relations are useful for modelling systems and components because we often do not know the exact function.

- Consider a digital thermometer which reports temperature in whole degrees.
  - ∗ An ideal model of the behavour would be a function from $\mathbb{R}$ to $\mathbb{Z}$. For example
    $$f(x) = \lfloor x + 0.5 \rfloor$$
  - ∗ However, in real life, sensors have only finite precision and finite operating ranges.
  - ∗ Suppose the thermometer is always right to within 0.6°
    $$\mathrm{dom}(R) = [-50, +200], \quad \mathrm{rng}(R) = \mathbb{Z}$$
    $$xRn \text{ iff } x - 0.6 \le n \le x + 0.6$$

* Often inputs and outputs are functions of time. We might specify a thermometer with up to a 1 second lag by

$$\mathrm{dom}(R) = (\mathbb{R} \to [-50, +200]), \quad \mathrm{rng}(R) = (\mathbb{R} \to \mathbb{Z})$$

$$xRn \text{ iff } \forall t \in \mathbb{R}, \exists t' \in \mathbb{R}, t-1 \leq t' \leq t \wedge x(t') - 0.6 \leq n(t) \leq x(t') + 0.6$$

  This is a relation relating two functions of time, where time is in seconds.

* If an actual thermometer behaves "better" than this specification then the actual system built will not be worse than the the system analysed using the specification.

* "Better" means the set of behaviours is a subset. E.g. a thermometer that is better, might obey the model

$$\mathrm{dom}(R) = (\mathbb{R} \to [-50, +200]), \quad \mathrm{rng}(R) = (\mathbb{R} \to \mathbb{Z})$$

$$xRn \text{ iff } \forall t \in \mathbb{R}, \exists t' \in \mathbb{R}, t-0.5 \leq t' \leq t \wedge x(t') - 0.55 \leq n(t) \leq x(t') + 0.55$$

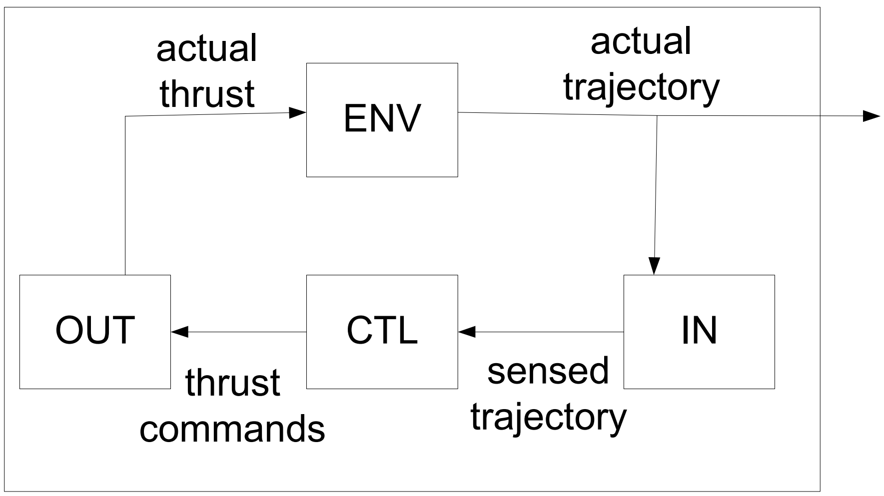
Relations for systems

We can often describe a system in terms of relations

- *IN*: relates actual values in the environment to their sensed values
- *CTL*: relates sensed values to commands to actuators. This relation often is implemented in software.
- *OUT*: relates commands to actuators to the actual effect on the environment.
- *ENV*: describes how the environment behaves.

Example

A rocket with various thrusters that can be either on or off.



The set of trajectories possible is

$$S = \{x \mid x(\mathit{ENV} \circ \mathit{OUT} \circ \mathit{CTL} \circ \mathit{IN})x\}$$

If the requirement is specified as a set of allowable trajectories, R, then we must design the system so that

$$S \subseteq R$$