Recall: Correctness

Let 'Req' be a requirement, 'Des' be a design, and 'Impl' be an implementation. Each is a set of evolutions, i.e. a subset of $(\text{Time} \rightarrow \times_{i=1}^{n} \mathbb{D}(\text{obs}_i))$, described in any form. We say

- 'Des' is a correct design (wrt. 'Req') if and only if $\text{Des} \subseteq \text{Req}$.
- 'Impl' is a correct implementation (wrt. 'Des' (or 'Req')) if and only if $\text{Impl} \subseteq \text{Des}$ (or $\text{Impl} \subseteq \text{Req}$).

If 'Req' and 'Des' are described by formulae of first-order predicate logic, proving the design correct amounts to proving that $\text{Des} = \Rightarrow \text{Req}$ is valid.

Classes of Timed Properties

Safety Properties

- A safety property states that something bad must never happen [Lamport].
- Example: train inside level crossing with gates open.
- More general, assume observable $C : \text{Time} \rightarrow \{0, 1\}$ where $C(t) = 1$ represents a critical system state at time $t$.
- Then $\forall t \in \text{Time} \cdot \neg C(t)$ is a safety property.
- In general, a safety property is characterised as a property that can be falsified in bounded time.
- But safety is not everything...
LivenessProperties

• The simplest form of a liveness property states that something good eventually does happen.
  
  Example: gates open for road traffic.

• More general, assume observable \( G : \text{Time} \rightarrow \{0, 1\} \) such that \( G(t) = 1 \) represents a good system state at time \( t \).

  \[ \exists t \in \text{Time} \quad G(t) \]

  is a liveness property.

• Note: not falsified in infinite time.

• With real-time, liveness is too weak...

DurationProperties

• A duration property states that for observation interval \( [b, e] \) characterised by a condition \( A(b, e) \), the accumulated time in which the system is in a certain critical state has an upper bound \( u(b, e) \).

  Example: leakage in gas burner.

• More general, reconsider critical thing \( C : \text{Time} \rightarrow \{0, 1\} \).

  \[ \forall b, e \in \text{Time} \quad (A(b, e) \Rightarrow \int_{e}^{b} C(t) \, dt \leq u(b, e)) \]

  is a duration property.

• This property can again be falsified in infinite time.

DurationCalculus: Preview

• Duration Calculus is an interval logic. Formulae are evaluated in an (implicitly given) interval.

Back to our gas burner:

• \( G, F, I, H : \text{Time} \rightarrow \{0, 1\} \): gas valve, flame sensor, ignition, heat.

• Define \( L : \text{Time} \rightarrow \{0, 1\} \) as \( G \land \neg F \).

Strangest operators:

• everywhere — Example: \( \lceil G \rceil \) (Hold in a given interval \( [b, e] \) iff the gas valve is open almost everywhere.)

• chop — Example: \( (\lceil \neg I \rceil; \lceil I \rceil; \lceil \neg I \rceil) \Rightarrow \ell \geq 1 \) (Ignition phases last at least once time unit.)

• integral — Example: \( \ell \geq 60 \Rightarrow \int L \leq \ell \) (At most 5% leak time in intervals of at least 60 time units.)
Semantic domains

Symbols: Semantics

Formulae:

State Assertions:

Duration Calculus: Overview
Duration Calculus: Overview

We will introduce three (or five) syntactical "levels":

(i) Symbols: $f, g, \text{true}, \text{false}, =, <, >, \leq, \geq, x, y, z, X, Y, Z, d$

(ii) State Assertions: $P ::= 0 | 1 | X = d | \neg P | P_1 \land P_2$

(iii) Terms: $\theta ::= x | \ell | \int P | f(\theta_1, \ldots, \theta_n)$

(iv) Formulae: $F ::= p(\theta_1, \ldots, \theta_n) | \neg F_1 | F_1 \land F_2 | \forall x \cdot F_1 | F_1; F_2$

(v) Abbreviations: $\lceil \cdot \rceil, \lceil P \rceil^t, \lceil P \rceil\leq t, \ Diamond F, \ Box F$