Contents & Goals

Last Lecture:
- Model of timed behaviour: state variables and their interpretation
- First order predicate-logic for requirements and system properties

This Lecture:
- Educational Objectives: Capabilities for following tasks/questions.
  - Read (and at best also write) Duration Calculus formulae.

- Content:
  - Classes of requirements (safety, liveness, etc.)
  - Duration Calculus:
    Assertions, Terms, Formulae, Abbreviations, Examples
Let ‘Req’ be a requirement,

‘Des’ be a design, and

‘Impl’ be an implementation.

Recall: each is a set of evolutions, i.e. a subset of \( \text{Time} \rightarrow \times_{i=1}^{n} D(\text{obs}_i) \), 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
  \[ \text{Impl} \subseteq \text{Des} \text{ (or Impl} \subseteq \text{Req)} \]

If ‘Req’ and ‘Des’ are described by formulae of first-oder predicate logic, proving the design correct amounts to proving that ‘Des \implies\ 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

  $\forall t \in \text{Time} \bullet \neg C(t)$

  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...
**Liveness Properties**

- The simplest form of a liveness property states that something good eventually does happen.
- Example: gates open for road traffic.
- More general, assume observable $G : \text{Time} \rightarrow \{0, 1\}$ where $G(t) = 1$ represents a good system state at time $t$.
  
  Then
  \[ \exists t \in \text{Time} \bullet G(t) \]
  is a liveness property.
- Note: not falsified in finite time.
- With real-time, liveness is too weak...

**Bounded Response Properties**

- A bounded response property states that the desired reaction on an input occurs in time interval $[b, e]$.
- Example: from request to secure level crossing to gates closed.
- More general, re-consider good thing $G : \text{Time} \rightarrow \{0, 1\}$ and request $R : \text{Time} \rightarrow \{0, 1\}$.
  
  Then
  \[ \forall t_1 \in \text{Time} \bullet (R(t_1) \implies \exists t_2 \in [t_1 + b, t_1 + e] \bullet G(t_2)) \]
  is a bounded liveness property.
- This property can again be falsified in finite time.
- With gas burners, this is still not everything...
Duration Properties

- 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.

\[
\int_b^e C(t) \, dt \leq u(b, e)
\]

More general, re-consider critical thing $C : \text{Time} \to \{0, 1\}$.

Then

\[
\forall b, e \in \text{Time} \cdot \left( A(b, e) \implies \int_b^e C(t) \, dt \leq u(b, e) \right)
\]

is a duration property.

This property can again be falsified in finite time.

\[
\begin{align*}
A(b, e) :&= e - b \geq 60 \\
\nu(b, e) :&= \frac{e-b}{20} \times f_0(e-b)
\end{align*}
\]
Duration Calculus

Duration Calculus: Preview

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

Back to our gas burner:
- $G, F, I, H : \text{Time} \rightarrow \{0, 1\}$
- Define $L : \text{Time} \rightarrow \{0, 1\}$ as $G \land \neg F$.

Strangest operators:
- **everywhere** — Example: $[G]$  
  (Holds in a given interval $[b, e]$ iff the gas valve is open almost everywhere.)

- **chop** — Example: $(\lceil \neg I \rfloor \land \lceil I \rfloor \land \lceil \neg I \rfloor) \implies \ell \geq 1$  
  (Ignition phases last at least one time unit.)

- **integral** — Example: $\ell \geq 60 \implies \int L \leq \frac{\ell}{20}$  
  (At most 5% leakage time within intervals of at least 60 time units.)
Duration Calculus: Overview

We will introduce three (or five) syntactical “levels”:

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

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

(iii) Terms:
- $\theta ::= x \mid 0 \mid P \mid f(\theta_1, \ldots, \theta_n)$

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

(v) Abbreviations:
- $[\ ]$, $[P]$, $[P]^t$, $[P]^{\leq t}$, $\diamond F$, $\Box F$

Symbols: Syntax

- $f, g$: function symbols, each with arity $n \in \mathbb{N}_0$.
  Called constant if $n = 0$.
  Assume: constants $0, 1, \cdots \in \mathbb{N}_0$; binary ‘+’ and ‘·’.
- $p, q$: predicate symbols, also with arity.
  Assume: constants $true, false$; binary $=, <, >, \leq, \geq$.
- $x, y, z \in GVar$: global variables.
- $X, Y, Z \in \text{Obs}$: state variables or observables, each of a data type $\mathcal{D}$ (or $\mathcal{D}(X), \mathcal{D}(Y), \mathcal{D}(Z)$ to be precise).
  Called boolean observable if data type is $\{0, 1\}$.
- $d$: elements taken from data types $\mathcal{D}$ of observables.
Symbols: Semantics

- **Semantical domains** are
  - the **truth values** \( B = \{tt, ff\} \),
  - the **real numbers** \( \mathbb{R} \),
  - **time** \( \text{Time} \),
    (mostly \( \text{Time} = \mathbb{R}_+ \) (continuous), exception \( \text{Time} = \mathbb{N}_0 \) (discrete time))
  - and **data types** \( D \).

- The **semantics** of an \( n \)-ary **function symbol** \( f \) is a (mathematical) function from \( \mathbb{R}^n \) to \( \mathbb{R} \), denoted \( \hat{f} \), i.e.
  \[
  \hat{f} : \mathbb{R}^n \to \mathbb{R}.
  \]

- The semantics of an \( n \)-ary **predicate symbol** \( p \) is a function from \( \mathbb{R}^n \) to \( B \), denoted \( \hat{p} \), i.e.
  \[
  \hat{p} : \mathbb{R}^n \to B.
  \]

- For constants (arity \( n = 0 \)) we have \( \hat{f} \in \mathbb{R} \) and \( \hat{p} \in B \).

Symbols: Examples

- The **semantics** of the function and predicate symbols **assumed above** is fixed throughout the lecture:
  - \( \text{true} = tt, \text{false} = ff \)
  - \( \hat{0} \in \mathbb{R} \) is the (real) number **zero**, etc.
  - \( \hat{+} : \mathbb{R}^2 \to \mathbb{R} \) is the **addition** of real numbers, etc.
  - \( \hat{=} : \mathbb{R}^2 \to B \) is the **equality** relation on real numbers,
  - \( \hat{<} : \mathbb{R}^2 \to B \) is the **less-than** relation on real numbers, etc.

- “Since the semantics is the expected one, we shall often simply use the symbols \( 0, 1, +, -, =, < \) when we mean their semantics \( \hat{0}, \hat{1}, \hat{+}, \hat{-}, \hat{=}, \hat{<} \).”
Symbols: Semantics

- The semantics of a **global variable** is not fixed (throughout the lecture) but given by a **valuation**, i.e. a mapping
  \[ \mathcal{V} : \text{GVar} \rightarrow \mathbb{R} \]
  assigning each global variable \( x \in \text{GVar} \) a real number \( \mathcal{V}(x) \in \mathbb{R} \).
  We use \( \text{Val} \) to denote the set of all valuations, i.e. \( \text{Val} = (\text{GVar} \rightarrow \mathbb{R}) \).
  Global variables are though **fixed over time** in system evolutions.

- The semantics of a **state variable** is **time-dependent**. It is given by an interpretation \( \mathcal{I} \), i.e. a mapping
  \[ \mathcal{I} : \text{Obs} \rightarrow (\text{Time} \rightarrow \mathcal{D}) \]
  assigning each state variable \( X \in \text{Obs} \) a function
  \[ \mathcal{I}(X) : \text{Time} \rightarrow \mathcal{D}(X) \]
  such that \( \mathcal{I}(X)(t) \in \mathcal{D}(X) \) denotes the value that \( X \) has at time \( t \in \text{Time} \).

Symbols: Representing State Variables

- For convenience, we shall abbreviate \( \mathcal{I}(X) \) to \( X_{\mathcal{I}} : \text{Time} \rightarrow \mathcal{D}(X) \).

- An interpretation (of a state variable) can be displayed in form of a **timing diagram**.

For instance,

- With \( \mathcal{D}(X) = \{d_1, d_2\} \),

\[ X_{\mathcal{I}} : \text{Time} \rightarrow \mathcal{D}(X) \]

\[ X_{\mathcal{I}}(t) = \begin{cases} 
  d_2 & \text{if } t \in [9.5) \cap \mathcal{E} \mathcal{C}(e, 9.5) \\
  d_1 & \text{if } t \in [9.5, 10] \\
  d_1 & \text{otherwise}
\end{cases} \]
Duration Calculus: Overview

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

(i) **Symbols:**

\[ f, g, \quad true, false, =, <, \leq, \geq, \quad x, y, z, \quad X, Y, Z, \quad d \]

(ii) **State Assertions:**

\[ P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \land P_2 \]

(iii) **Terms:**

\[ \theta ::= x \mid \ell \mid \int P \mid f(\theta_1, \ldots, \theta_n) \]

(iv) **Formulae:**

\[ F ::= p(\theta_1, \ldots, \theta_n) \mid \neg F_1 \mid F_1 \land F_2 \mid \forall x \bullet F_1 \mid F_1 ; F_2 \]

(v) **Abbreviations:**

\[ [\cdot], [P], [P]^t, [P]^{\leq t}, \Diamond F, \Box F \]

---

State Assertions: Syntax

- The set of state assertions is defined by the following grammar:

\[ P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \land P_2 \]

with \( d \in D(X) \).

We shall use \( P, Q, R \) to denote state assertions.

\[ [\cdot], X^{\downarrow}, X^{\uparrow}, X^{\Box} \]

- **Abbreviations:**

  - We shall write \( X \) instead of \( X = 1 \) if \( D(X) \) = \( \emptyset \).
  - Define \( \forall, \implies, \iff \) as usual.
State Assertions: Semantics

- Given an evolution $\mathcal{E}$.
- The semantics of state assertion $P$ is a function

$$\mathcal{I}[P] : \text{Time} \rightarrow \{0, 1\}$$

i.e. $\mathcal{I}[P](t)$ denotes the truth value of $P$ at time $t \in \text{Time}$.

- The value is defined inductively on the structure of $P$:

$$\mathcal{I}[0](t) = 0 \in \mathbb{R}, \quad \mathcal{I}[1](t) = 2 - 1 \in \mathbb{R}$$

$$\mathcal{I}[X = d](t) = \begin{cases} 1, & \text{if } X(t) = d \\ 0, & \text{otherwise} \end{cases}$$

$$\mathcal{I}[\neg P_1](t) = 1 - \mathcal{I}[P_1](t)$$

$$\mathcal{I}[P_1 \land P_2](t) = \begin{cases} 1, & \text{if } \mathcal{I}[P_1](t) = 1 \land \mathcal{I}[P_2](t) = 1 \\ 0, & \text{otherwise} \end{cases}$$

State Assertions: Notes

- $\mathcal{I}[X](t) = \mathcal{I}[X = 1](t) = \mathcal{I}(X)(t) = X(t)$, if $X$ boolean, i.e. $\mathcal{I}X = \{0, 1\}$

- $\mathcal{I}[P]$ is also called interpretation of $P$.

  We shall write $P_\mathcal{I}$ for it.

- Here we prefer 0 and 1 as boolean values (instead of tt and ff) — for reasons that will become clear immediately.
State Assertions: Example

- Boolean observables $G$ and $F$.
- State assertion $L := G \land \neg F$.

**Abbreviations:**
- $G$ and $F$:
- $L := G \land \neg F$

**Interpretation of state variables**

- $G_1 = 1$
- $F_0 = 1$
- $L_0 = 1$

**Interpretation of state assertion $L$**

- $L_I(1.2) = 1$, because
  - $T[I G \land \neg F](1.2) = T[I G \land \neg F](0) = 1$
  - $T[I G](1.2) = 1$ because $T(I(1.2)) = 1$
  - $T[I \neg F](1.2) = 0$ because $T(I(1.2)) = 0$

- $L_I(2) = 0$, because
  - $T[I \neg F](1.2) = 0$ because $T(I(1.2)) = 0$
  - $T[I G \land \neg F](0) = 1$

References
References