Real-Time Systems

Lecture 03: Duration Calculus I

2011-05-03

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

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

Recall: Correctness

Recall: Correctness

- 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 $\big(\mathsf{Time} \to \times_{i=1}^{n} \mathcal{D}(obs_i)\big)$, described in any form.

We say

- 'Des' is a **correct design** (wrt. 'Req') if and only if

$$\mathsf{Des} \subseteq \mathsf{Req}.$$

- 'Impl' is a **correct implementation** (wrt. 'Des' (or 'Req')) if and only if

$$\mathsf{Impl} \subseteq \mathsf{Des} \quad (\text{or } \mathsf{Impl} \subseteq \mathsf{Req})$$

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.

Recall: Kinds of Requirements and System Properties

Recall: Kinds of Requirements and System Properties

Assume observables

- $C : \{0,1\}$, $C(t) = 1$ represents a **critical system state** at time t;
- $G : \{0,1\}$, $G(t) = 1$ represents a **good system state** at time t;
- $R : \{0,1\}$, $R(t) = 1$ represents a **request** at time t.

- Typical **safety** property:

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

- Typical **liveness** property:

$$\exists\, t \in \mathsf{Time} \bullet G(t)$$

characterise interval, e.g. $|b-e| \geq 60$

expression over b, e, e.g. $0{,}05 \cdot |b-e|$

- Typical **bounded response** property:

$$\forall\, t_1 \in \mathsf{Time} \bullet (R(t_1) \implies \exists\, t_2 \in [t_1 + 10, t_1 + 15] \bullet G(t_2))$$

- Typical **duration property**:

$$\forall\, b, e \in \mathsf{Time} \bullet \left(A(b,e) \implies \int_b^e C(t)\, dt \leq u(b,e) \right)$$

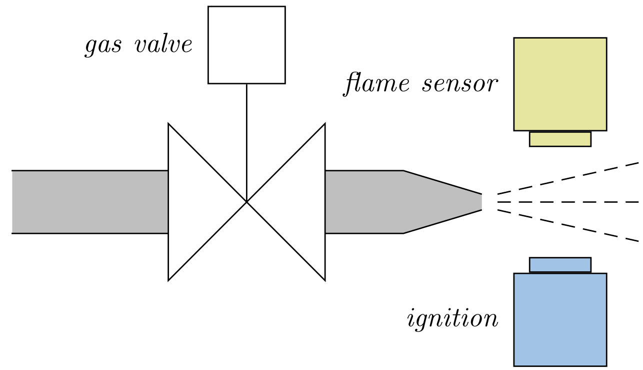
Duration Calculus

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 : Time $\rightarrow \{0, 1\}$
- Define L : Time $\rightarrow \{0, 1\}$ as $G \wedge \neg F$.



Strangest operators:

- almost **everywhere** — Example: $\lceil G \rceil$

  (Holds in a given interval $[b, e]$ iff the gas valve is open almost everywhere.)

- **chop** — Example: $(\lceil \neg I \rceil \,;\, \lceil I \rceil \,;\, \lceil \neg I \rceil) \implies \ell \geq 1$

  (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:**

P_1 $f, g,$ $true, false, =, <, >, \leq, \geq,$ $x, y, z,$ $X, Y, Z,$ d

(ii) **State Assertions:**

$$P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \wedge P_2$$ yield 0,1

(iii) **Terms:**

$$\theta ::= x \mid \ell \mid \int P \mid f(\theta_1, \dots, \theta_n)$$ yield $\mathbb{R}$

(iv) **Formulae:**

$$F ::= p(\theta_1, \dots, \theta_n) \mid \neg F_1 \mid F_1 \wedge F_2 \mid \forall x \bullet F_1 \mid F_1 \,;\, F_2$$ yield tt, ff

(v) **Abbreviations:**

$$\lceil\,\rceil, \quad \lceil P \rceil, \quad \lceil P \rceil^t, \quad \lceil P \rceil^{\leq t}, \quad \Diamond F, \quad \Box F$$

Symbols: Syntax

- f, g: **function symbols**, each with arity $n \in \mathbb{N}_0$.

  Called **constant** if $n = 0$.

  Assume: constants $0, 1, \dots \in \mathbb{N}_0$; $\underbrace{\text{binary}}_{n=2}$ '$+$' and '$\cdot$'.; $\underbrace{\text{ternary}}_{n=3}$

- p, q: **predicate symbols**, also with arity.

  Assume: constants $true, false$; binary $=, <, >, \leq, \geq$.

- $x, y, z \in$ GVar: **global variables**.

- $X, Y, Z \in$ 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). T: {red, green, yellow}

  Called **boolean observable** if data type is $\{0, 1\}$.

- d: **elements** taken from data types $\mathcal{D}$ of observables.

  e.g. red, green, yellow

Symbols: Semantics

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

- 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 $\mathbb{B}$, denoted $\hat{p}$, i.e.

$$\hat{p} : \mathbb{R}^n \to \mathbb{B}.$$

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

Symbols: Examples

- The **semantics** of the function and predicate symbols **assumed above** is fixed throughout the lecture:
  - $\hat{true} = \mathsf{tt}$, $\hat{false} = \mathsf{ff}$ • $\hat{\cdot} : \mathbb{R}^2 \to \mathbb{R}$ is multiplication
  - $\hat{0} \in \mathbb{R}$ is the (real) number **zero**, etc.
  - $\hat{+} : \mathbb{R}^2 \to \mathbb{R}$ is the **addition** of real numbers, etc.
  - $\hat{=} : \mathbb{R}^2 \to \mathbb{B}$ is the **equality** relation on real numbers,
  - $\hat{<} : \mathbb{R}^2 \to \mathbb{B}$ is the **less-than** relation on real numbers, etc.
  - $\hat{\text{ß}} : \mathbb{R}^3 \to \mathbb{R}$: we choose the maximum, so

    $$\hat{\text{ß}}(a,b,c) = \begin{cases} c & \text{if } c \geq b \wedge c \geq a \\ b & \text{if } b \geq a \wedge b \geq c \\ a & \text{if } a \geq b \wedge a \geq c \end{cases}$$
- "Since the semantics is the expected one, we shall often simply use the symbols $0, 1, +, \cdot, =, <$ when we mean their semantics $\hat{0}, \hat{1}, \hat{+}, \hat{\cdot}, \hat{=}, \hat{<}$."

Symbols: Semantics

x, y, z

- The semantics of a **global variable** is not fixed (throughout the lecture) but given by a **valuation**, i.e. a mapping

$$\mathcal{V} : \mathsf{GVar} \to \mathbb{R}$$

assigning each global variable $x \in \mathsf{GVar}$ a real number $\mathcal{V}(x) \in \mathbb{R}$.

We use Val to denote the set of all valuations, i.e. $\mathsf{Val} = (\mathsf{GVar} \to \mathbb{R})$.

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

$$\mathcal{I} : \mathsf{Obs} \to (\mathsf{Time} \to \mathcal{D})$$

assigning each state variable $X \in \mathsf{Obs}$ a function

$$\mathcal{I}(X) : \mathsf{Time} \to \mathcal{D}(X)$$

such that $\mathcal{I}(X)(t) \in \mathcal{D}(X)$ denotes the value that X has at time $t \in \mathsf{Time}$.

as before:

$\pi : \mathsf{Time} \to \mathcal{D}(obs_1) \times \ldots \times \mathcal{D}(obs_n)$

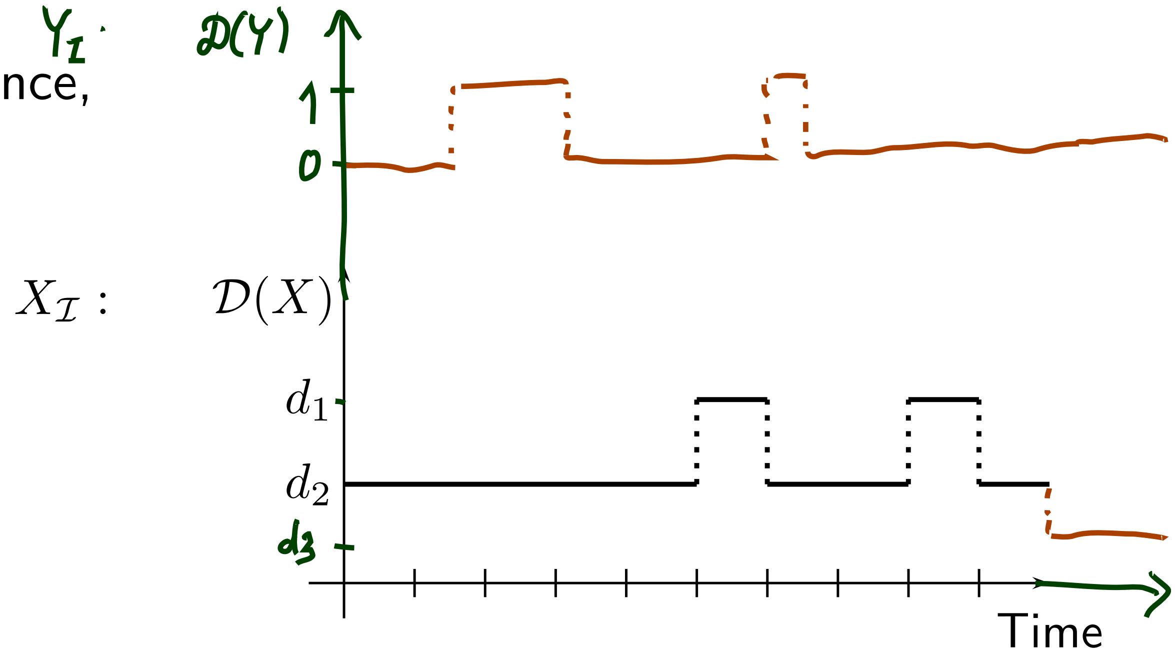
$\pi_{obs} : \mathsf{Time} \to \mathcal{D}(obs)$

Symbols: Representing State Variables

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

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

For instance,



with $\mathcal{D}(X) = \{d_1, d_2\} \cup \{d_3\}$

$\mathcal{D}(Y) = \{0, 1\}$

Duration Calculus: Overview

could be X ☺ d or X/d or X⋯d

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

√ (i) **Symbols:** (DC-)

$$0, 1, 3.14, f, g, \quad true, false, =, <, >, \leq, \geq, \quad x, y, z, \quad X, Y, Z, \quad d$$

(ii) **State Assertions:**

$$P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \wedge P_2$$

(iii) **Terms:**

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

(iv) **Formulae:**

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

(v) **Abbreviations:**

$$\lceil\,\rceil, \quad \lceil P \rceil, \quad \lceil P \rceil^t, \quad \lceil P \rceil^{\leq t}, \quad \Diamond F, \quad \Box F$$

State Assertions: Syntax

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

$$P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \wedge P_2$$

with $d \in \mathcal{D}(X)$, X obserbavle ,

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

- **Abbreviations**:
  - We shall write X instead of $X = 1$ if $\mathcal{D}(X) =$ ~~B~~ $\{0,1\}$
  - Define $\vee$, $\implies$, $\iff$ as usual.

State Assertions: Semantics

$I : Obs \to (time \to \mathcal{D})$

- The **semantics** of **state assertion** P is a function

$$\mathcal{I}[\![P]\!] : \mathsf{Time} \to \{0, 1\}$$

or $\bullet[\![\cdot]\!](\cdot) : (Obs \to (Time \to \mathcal{D})) \times \text{State Ass} \times \text{Time} \to \{0,1\}$

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

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

$$\mathcal{I}[\![0]\!](t) = 0 \in \mathbb{R} \text{ (semantical domain)}$$

$$\mathcal{I}[\![1]\!](t) = 1$$

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

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

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

State Assertions: Notes

by def. on prev. slide

- $\mathcal{I}[\![\underbrace{X}_{}]\!](t) = \mathcal{I}[\![\underbrace{X = \mathbf{1}}_{}]\!](t) = \mathcal{I}(X)(t) = X_{\mathcal{I}}(t)$, if X boolean, i.e. $\mathcal{D}(X) = \{0, 1\}$

  abbrev. abbrev. "1"

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

  We shall write $P_{\mathcal{I}}$ for it. $: \mathrm{Time} \to \{0,1\}$

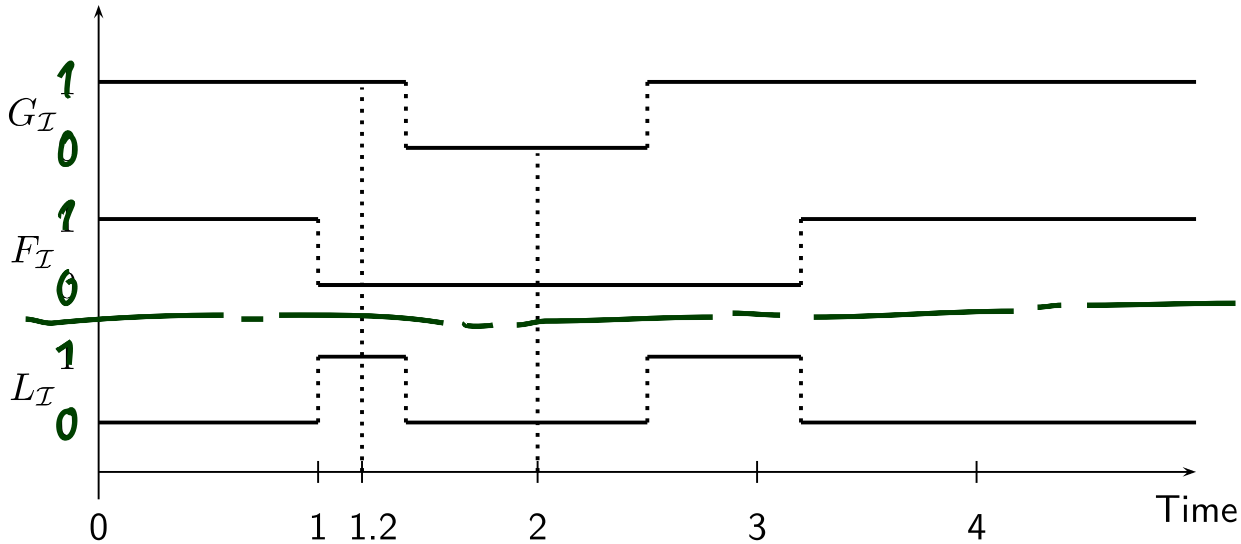
- Here we prefer 0 and 1 as boolean values (instead of tt and ff) — for reasons that will become clear immediately.

State Assertions: Example

- Boolean observables G and F.
- State assertion $L := G \wedge \neg F$. (unabbr.: $(G=1) \wedge \neg(F=1)$)

interpretations of state variable

interpretation of state assertions



- $L_\mathcal{I}(1.2) = 1$, because

  $\mathcal{I}[\![G \wedge \neg F]\!](1.2) = 1$

  because $\mathcal{I}[\![G]\!](1.2) = \mathcal{I}(G)(1.2) = 1$

  $\mathcal{I}[\![\neg F]\!](1.2) = 1 - \mathcal{I}(F)(1.2) = 1$

- $L_\mathcal{I}(2) = 0$, because

  $\mathcal{I}[\![G]\!](2) = 0$

References