Real-Time Systems

Lecture 03: Duration Calculus I

2014-05-08

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

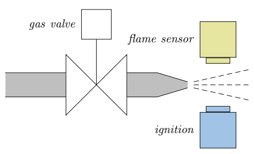
- Model of timed behaviour: state variables and their interpretation
- First order predicate-logic for requirements and system properties
- Classes of requirements (safety, liveness, etc.)

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
  - Read (and at best also write) Duration Calculus formulae.
- **Content:**
  - Duration Calculus:
    Assertions, Terms, Formulae, Abbreviations, Examples

Duration Calculus

Duration Calculus: Preview



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

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

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:**

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

(ii) **State Assertions:**

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

(iii) **Terms:**

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

(iv) **Formulae:**

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

(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 $\underbrace{0}_{n=0}, 1, \dots \in \mathbb{N}_0$; $\underbrace{\text{binary}}_{n=2}$ '$+$' and '$\cdot$'. : 3 (ternary)
- p, q: **predicate symbols**, also with arity.
  Assume: constants $true, false$; binary $=, <, >, \leq, \geq$. ♡: 2 (binary)
- $x, y, z \in$ GVar: **global variables**.
- $X, Y, Z \in$ Obs: **state variables** or **observables**, each of a data type $\mathcal{D}$ TrfLight
  (or $\mathcal{D}(X), \mathcal{D}(Y), \mathcal{D}(Z)$ to be precise). $\mathcal{D}$(TrfLight):
  Called **boolean observable** if data type is $\{0, 1\}$.
- d: **elements** taken from data types $\mathcal{D}$ of observables. red, green

Symbols: Semantics

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

✿ : 3

- 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.

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

$\hat{✿} : \mathbb{R}^3 \longrightarrow \mathbb{R}$

$(a,b,c) \mapsto \frac{a+}{}$

$\hat{♡} : \mathbb{R}^2 \to \mathbb{B}$

$(a,b) \mapsto \begin{cases} \mathsf{tt}, & b = a+1 \\ \mathsf{ff}, & \text{else} \end{cases}$

$\hat{0} : \mathbb{R}$

0

$\hat{\pi} : \mathbb{R}$

$3.1415\ldots$

$\hat{true} : \mathbb{B}$

tt

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

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

Symbols: Examples

- The **semantics** of the function and predicate symbols **assumed above** is fixed throughout the lecture:

  - $\hat{true} = \mathsf{tt}$, $\hat{false} = \mathsf{ff}$
  - $\hat{0} \in \mathbb{R}$ 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.

- "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

- 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.

$\mathsf{GVar} = \{x, y, z\}$

e.g. $\mathcal{V} = \{x \mapsto 3, y \mapsto 0, z \mapsto 27\}$

Symbols: Semantics

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

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

$\pi : \mathsf{Time} \to \mathcal{D}_1 \times \mathcal{D}_2$ (G, F)

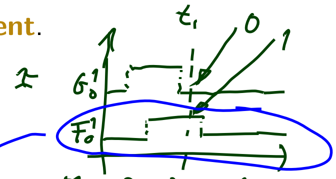
assigning each global variable $x \in \mathsf{GVar}$ a real number $\mathcal{V}(x) \in \mathbb{R}$.

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

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



$\mathsf{Obs} = \{F, G\}$

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

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

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

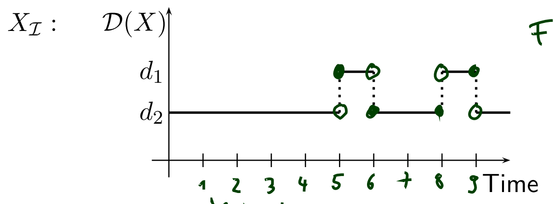
$\mathcal{I}(F)(t_0) = 1$

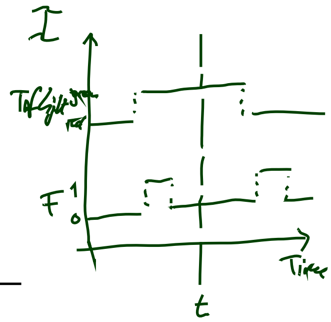
such that $(\mathcal{I}(X))(t) \in \mathcal{D}(X)$ denotes the value that X has at time $t \in \mathsf{Time}$.

Symbols: Representing State Variables

- For convenience, we shall abbreviate $\mathcal{I}(X)$ to $X_\mathcal{I}$. e.g. $\mathcal{F}_x$
- An **interpretation** (of a state variable) can be displayed in form of a **timing diagram**.

  For instance,





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

$\mathcal{I}(X)(3) = d_2$

$\mathcal{I}(X)(5) = d_1$

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:**

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

(iii) **Terms:**

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

(iv) **Formulae:**

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

(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

not the function symbol

- 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 $d \in \mathcal{D}(X)$, $X \in Obs$.

could also write: $[X, d]$, X^d, $X \odot d$

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

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

E.g. TrfLight = red

F = 1

F (an abbrev.)

1 = 1 NOT! (if 1 is not an observable)

State Assertions: Semantics

I-int-of-P: Time → {0,1

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

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

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

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

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

$$\mathcal{I}[\![1]\!](t) = 1 \;(\in \mathbb{R})$$

symbols, syntax

maths, semantics

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

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

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

State Assertions: Notes

by def. on prev. slide (needs proof)

- $\mathcal{I}[\![X]\!](t) = \mathcal{I}[\![X = 1]\!](t) = \mathcal{I}(X)(t) = X_{\mathcal{I}}(t)$, if X boolean.

  abbrev. from before — abbrev. from before

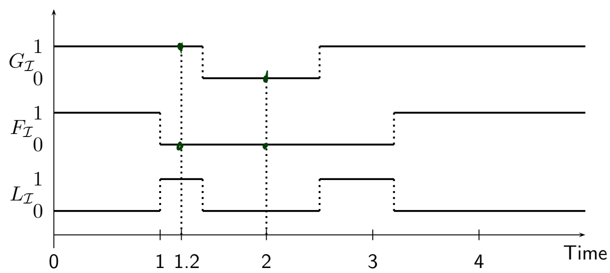
- $\mathcal{I}[\![P]\!]$ is also called **interpretation** of P.

  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 $L := G \wedge \neg F$. $((G=1) \wedge \neg(F=1))$



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

  $\mathcal{I}[\![G]\!](1.2) = \mathcal{I}[\![G=1]\!](1.2) = 1$ because $G_{\mathcal{I}}(1.2) = 1$
  $\mathcal{I}[\![F]\!](1.2) = \mathcal{I}[\![F=1]\!](1.2) = 0$ because $F_{\mathcal{I}}(1.2) = 0$
  $\mathcal{I}[\![\neg F]\!](1.2) = 1 - \mathcal{I}[\![F]\!](1.2) = 1 - 0 = 1$
  $\mathcal{I}[\![L]\!](1.2) = 1$

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

Duration Calculus: Overview

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

(i) **Symbols:**

$$f, g, \quad \mathit{true}, \mathit{false}, =, <, >, \leq, \geq, \quad x, y, z, \quad X, Y, Z, \quad d$$

(ii) **State Assertions:**

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

yields 0 or 1

(iii) **Terms:**

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

yields $\mathbb{R}$

(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:**

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

Terms: Syntax

- **Duration terms** (DC terms or just terms) are defined by the following grammar:

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

  where x is a global variable, ℓ and $\int$ are special symbols, P is a state assertion, and f a function symbol (of arity n).

- ℓ is called **length operator**, $\int$ is called **integral operator**

- Notation: we may write function symbols in **infix notation** as usual, i.e. write $\theta_1 + \theta_2$ instead of $+(\theta_1, \theta_2)$.

> **Definition 1.** [*Rigid*]
> A term **without** length and integral symbols is called rigid.

Terms: Semantics

begin end

- Closed **intervals** in the time domain

$$\mathsf{Intv} := \{[b,e] \mid b,e \in \mathsf{Time} \text{ and } b \leq e\}$$

Point intervals: $[b,b]$

Terms: Semantics

- The **semantics** of a **term** is a function

$$\mathcal{I}[\![\theta]\!] : \mathsf{Val} \times \mathsf{Intv} \to \mathbb{R}$$

i.e. $\mathcal{I}[\![\theta]\!](\mathcal{V},[b,e])$ is the real number that θ denotes under interpretation $\mathcal{I}$ and valuation $\mathcal{V}$ in the interval $[b,e]$.

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

classical Riemann integral

$$\mathcal{I}[\![x]\!](\mathcal{V},[b,e]) = \mathcal{V}(x) \in \mathbb{R}$$

$$\mathcal{I}[\![\ell]\!](\mathcal{V},[b,e]) = e - b$$

$$\mathcal{I}[\![\textstyle\int P]\!](\mathcal{V},[b,e]) = \int_b^e P_{\mathcal{I}}(t)\,dt$$

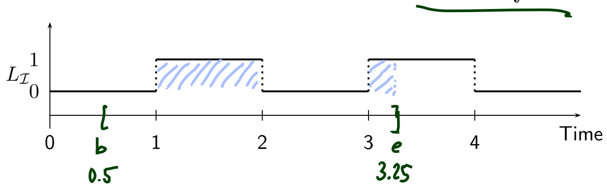
$\mathcal{I}[\![P]\!] : \mathsf{Time} \to \{0,1\}$

$$\mathcal{I}[\![f(\theta_1,\dots,\theta_n)]\!](\mathcal{V},[b,e]) = \hat{f}(\mathcal{I}[\![\theta_1]\!](\mathcal{V},[b,e]),\dots,\mathcal{I}[\![\theta_n]\!](\mathcal{V},[b,e]))$$

Terms: Example

$\Big(\cdot(x, \textstyle\int L) \;\; R := G \wedge \neg F \Big)$

$\theta = x \cdot \int L$



$\mathcal{V}(x) = 20.$

math. mult.

$\mathcal{I}[\![\theta]\!](\mathcal{V}, [b,e]) = \hat{\cdot}\big(\mathcal{I}[\![x]\!](\mathcal{V}, [b,e]), \mathcal{I}[\![\textstyle\int L]\!](\mathcal{V}, [b,e])\big) = 20 \cdot 1.25 = 25$

$\mathcal{I}[\![x]\!](\mathcal{V}, [b,e]) = \mathcal{V}(x) = 20$

$\mathcal{I}[\![\textstyle\int L]\!](\mathcal{V}, [b,e]) = \int_b^e L_\mathcal{I}(t)\,dt = \int_{0.5}^{3.25} L_\mathcal{I}(t)\,dt = 1.25$

Terms: Semantics Well-defined?

- So, $\mathcal{I}[\![\int P]\!](\mathcal{V}, [b,e])$ is $\displaystyle\int_b^e P_\mathcal{I}(t)\,dt$ — but does the integral always exist?
- IOW: is there a $P_\mathcal{I}$ which is not (Riemann-)integrable? Yes. For instance

$$P_\mathcal{I}(t) = \begin{cases} 1 & \text{, if } t \in \mathbb{Q} \\ 0 & \text{, if } t \notin \mathbb{Q} \end{cases}$$

- To exclude such functions, DC considers only interpretations $\mathcal{I}$ satisfying the following condition of **finite variability**:

  For each state variable X and each interval $[b,e]$ there is a **finite partition** of $[b,e]$ such that the interpretation $X_\mathcal{I}$ is **constant on each part**.

  Thus on each interval $[b,e]$ the function $X_\mathcal{I}$ has only **finitely many points of discontinuity**.

References

[Olderog and Dierks, 2008] Olderog, E.-R. and Dierks, H. (2008). *Real-Time Systems - Formal Specification and Automatic Verification*. Cambridge University Press.