

Real-Time Systems

Lecture 03: Duration Calculus I

2013-04-23

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 $(\text{Time} \rightarrow \times_{i=1}^n \mathcal{D}(\text{obs}_i))$, 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

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

If 'Req' and 'Des' are described by formulae of first-order predicate logic, proving the design correct amounts to proving that 'Des \implies Req' is valid.

Classes of Timed Properties

Safety Properties

$$\begin{aligned} \forall x \in \mathbb{N} : x \geq 0 \\ \forall x \in \mathbb{N} . x \geq 0 \\ \forall x \in \mathbb{N} \bullet x \geq 0 \end{aligned}$$

- A **safety property** states that **something bad must never happen** [Lamport].

- Example: train inside level crossing with gates open.

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

- More general, assume observable $C : \text{Time} \rightarrow \{0, 1\}$ where $C(t) = 1$ represents a critical system state at time t .

Then

or "bad"

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

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

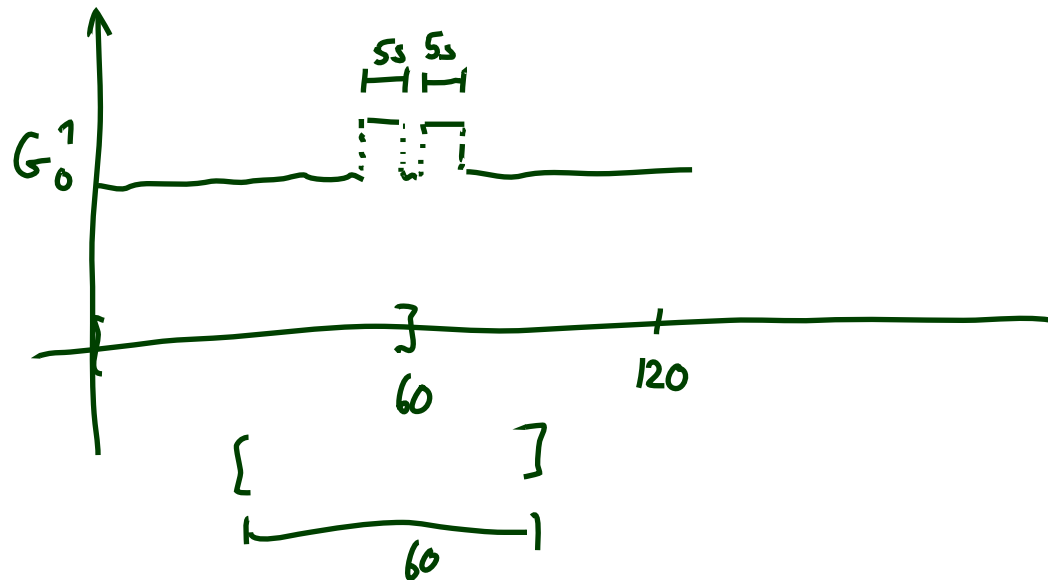
$$\forall t_1 \in \text{Time} \bullet (R(t_1) \implies \exists t_2 \in [t_1 + \overset{b}{\cancel{10}}, t_1 + \overset{e}{\cancel{15}}] \bullet G(t_2))$$

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.



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.

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

Then

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

is a duration property.

- This property can again be falsified in finite time.

gas burner:

$$A(b, e) := e - b \geq 60$$
$$u(b, e) := \frac{e-b}{20} = \frac{1}{20}(e-b)$$

Riemann Integral



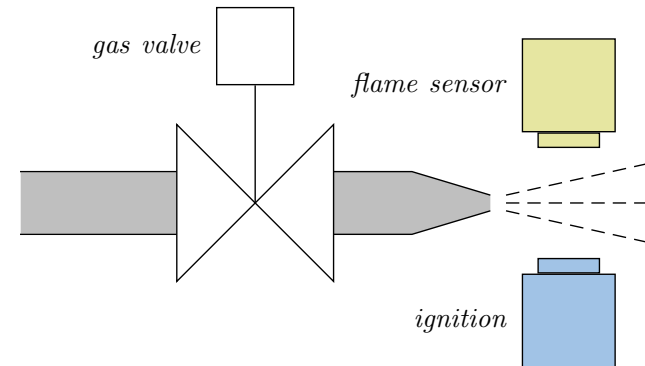
Duration Calculus

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 $G \wedge \neg F$.



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

global variables
state variables
domain values

(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:**

$\theta ::= x \mid \ell \mid \underline{f}P \mid f(\theta_1, \dots, \theta_n)$

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 \mathbb{tt}, \mathbb{ff}

(v) **Abbreviations:**

$\llbracket \cdot \rrbracket, \llbracket P \rrbracket, \llbracket P \rrbracket^t, \llbracket P \rrbracket^{\leq t}, \diamond F, \square F$

Symbols: Syntax

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

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

Assume: constants $0, 1, \dots \in \mathbb{N}_0$; binary '+' and '.'; ternary symbol ↕

$n=2$

$n=3$

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

Assume: constants *true*, *false*; binary =, <, >, ≤, ≥.

- $x, y, z \in \text{GVar}$: **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 $\{0, 1\}$.

e.g. T
 $\mathcal{D}(T) = \{\text{red}, \text{green}, \text{yellow}\}$

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

e.g. red
green
yellow

Symbols: Semantics

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

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

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

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

- 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:

- $\hat{true} = tt, \hat{false} = ff$

- $\hat{0} \in \mathbb{R}$ is the (real) number **zero**, etc.

- $\hat{+} : \mathbb{R}^2 \rightarrow \mathbb{R}$ is the **addition** of real numbers, etc.

- $\hat{=} : \mathbb{R}^2 \rightarrow \mathbb{B}$ is the **equality** relation on real numbers,

- $\hat{<} : \mathbb{R}^2 \rightarrow \mathbb{B}$ 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 $\hat{0}, \hat{1}, \hat{+}, \hat{\cdot}, \hat{=}, \hat{<}.$ ”

$$\hat{\phi}, n=3$$

$$\hat{\phi} : \mathbb{R}^3 \rightarrow \mathbb{R}$$

my choice: maximum

$$(a,b,c) \mapsto \begin{cases} a & \text{if } a > b \text{ and } a > c \\ b & \text{if } b > a \text{ and } b > c \\ c & \text{if } c > a \text{ and } c > b \end{cases}$$

$$\hat{\phi} := \text{or } \max(\cdot, \cdot, \cdot)$$

your choice maybe: average

$$(a,b,c) \mapsto \frac{a+b+c}{3}$$

$\hat{+} := +$
math-addition
fun.

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 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 $t \in \text{Time}$.

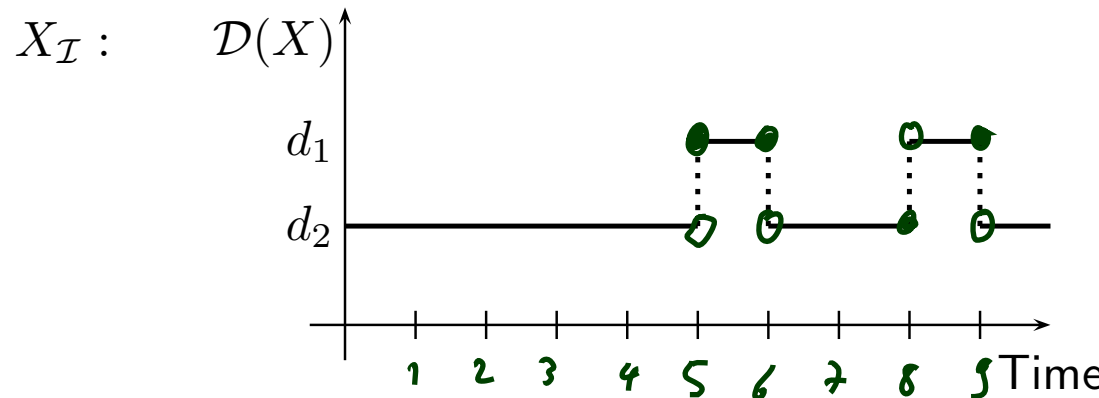
$$\mathcal{I}(T) : \text{Time} \rightarrow \{\text{red, green, yellow}\}$$

$$\mathcal{I}(T)(13, 27) = \text{red}$$

Symbols: Representing State Variables

- For convenience, we shall abbreviate $\mathcal{I}(X)$ to $X_I: \text{Time} \rightarrow \mathcal{D}(X)$ e.g.
 T_I
- An **interpretation** (of a state variable) can be displayed in form of a **timing diagram**. *and defined*

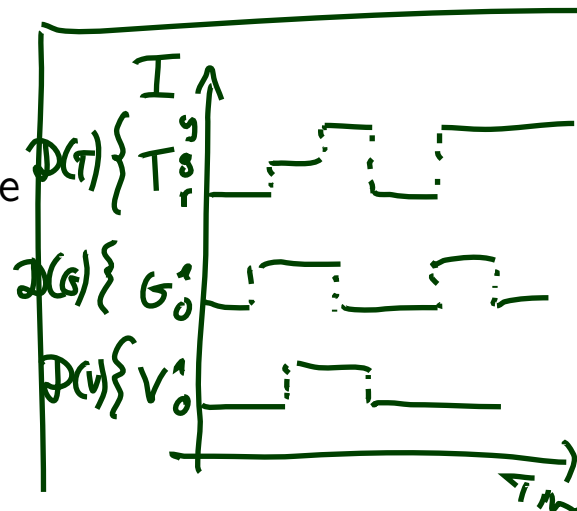
For instance,



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

$$X_I(5) = d_1$$

$$X_I(t) = \begin{cases} d_2 & \text{if } t \in [0, 5) \\ d_1 & \text{if } t \in [6, 8] \\ d_2 & \text{if } t > 9 \\ d_1 & \text{otherwise} \end{cases}$$



Duration Calculus: Overview

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

(i) **Symbols:**

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

(ii) **State Assertions:**

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

(iii) **Terms:**

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

(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:**

$\lceil \rceil, \lceil P \rceil, \lceil P \rceil^t, \lceil P \rceil^{\leq t}, \diamond F, \square F$

State Assertions: Syntax

the constant 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 $d \in \mathcal{D}(X)$.

$\in \text{Obs}$

$\in \mathcal{D}(X)$

(P_1, P_2)

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

$$[X, d], X^d, X \heartsuit d$$

- Abbreviations:**

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

State Assertions: Semantics

- Given an evolution \mathcal{I} .
- 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 :

$$\mathcal{I}[[0]](t) = \hat{0} \in \mathbb{R}, \quad \hat{0} = 0 \leftarrow \text{math.}$$

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

the same

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

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

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

State Assertions: Notes

- $\mathcal{I}[[X]](t) = \mathcal{I}[[X = 1]](t) = \mathcal{I}(X)(t) = X_{\mathcal{I}}(t)$, if X boolean, i.e. $\mathcal{D}(X) = \{0, 1\}$
abbrev. *by def on prev. slide* *abbrev.*
- $\mathcal{I}[[P]]$ 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

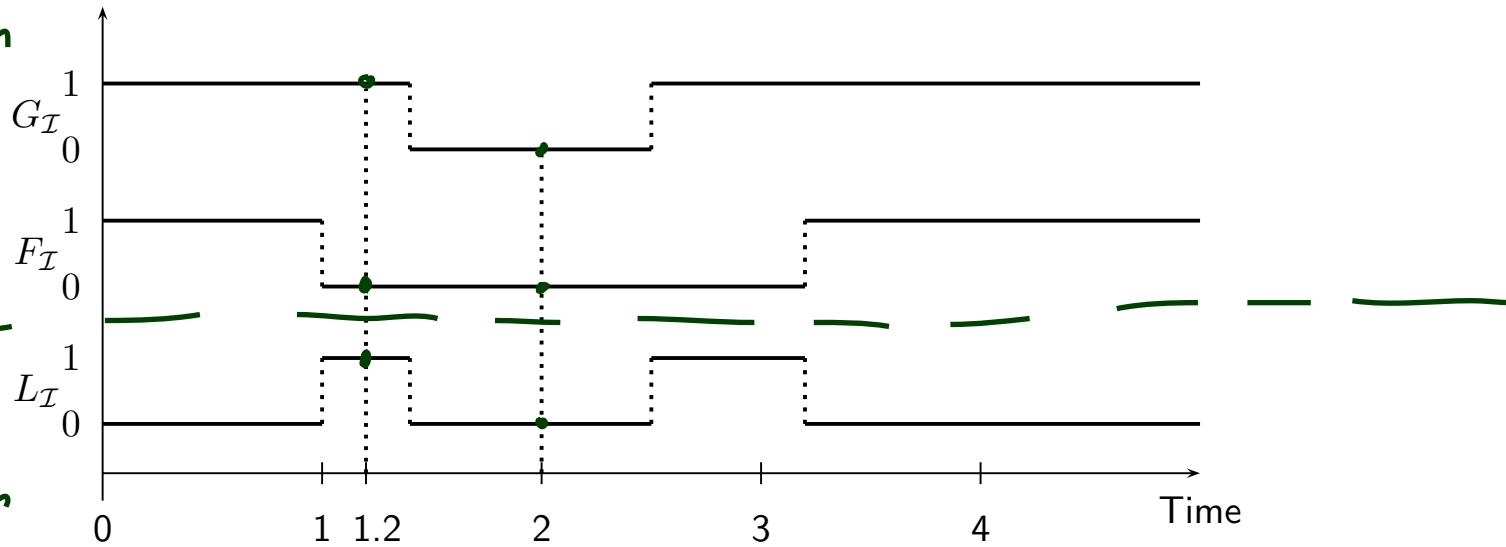
- Boolean observables G and F .
- State assertion $L := G \wedge \neg F$,

abbrev. for $(G=1) \wedge \neg(F=1)$

state variables F, G

interpretation
of
state
variables

interpretation
of
state
assertion
 $F \wedge \neg G$



- $L_I(1.2) = 1$, because

$$I[L](1.2) = I[G \wedge \neg F](1.2) = I[G=1 \wedge \neg(F=1)](1.2) = 1$$

$I[G=1](1.2) = 1$ because $I(G)(1.2) = 1 = \hat{1}$
 $I[F=1](1.2) = 0$ because $I(F)(1.2) = 0 \neq \hat{1} = 1$
 $I[\neg(F=1)](1.2) = 1 - I[F=1](1.2) = 1 - 0 = 1$

- $L_I(2) = 0$, because

References

References

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