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

Classes of Timed Properties

Safety Properties

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

- 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 : Time $\to \{0, 1\}$ where $C(t) = 1$ represents a critical system state at time t.
  or "bad"

  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 $G : \mathsf{Time} \to \{0, 1\}$ where $G(t) = 1$ represents a good system state at time t.

  Then

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

  is a liveness property.

- Note: not falsified in finite time.

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

– 03 – 2013-04-23 – Sclasses –

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 $G : \mathsf{Time} \to \{0, 1\}$ and request $R : \mathsf{Time} \to \{0, 1\}$.

  Then

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

  is a bounded liveness property.

- This property can again be falsified in finite time.

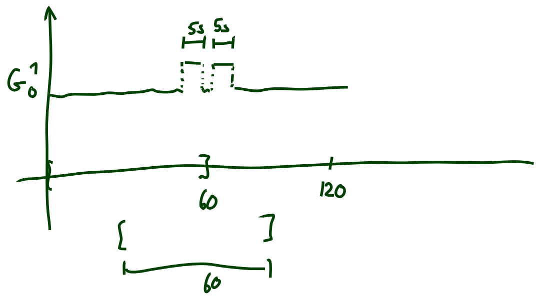
- With gas burners, this is still not everything...

– 03 – 2013-04-23 – Sclasses –

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.

Riemann Integral

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

  Then

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

  is a duration property.

- This property can again be falsified in finite time.

gas burner: $A(b,e) := e - b \geq 60$

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

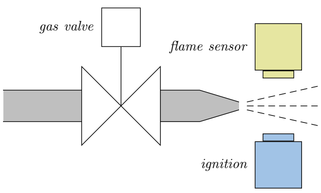
Duration Calculus

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 $\to \{0,1\}$
- Define L : Time $\to \{0,1\}$ 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":

global variables

state variables

domain values

(i) **Symbols:**

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

(ii) **State Assertions:**

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

yield 0, 1

(iii) **Terms:**

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

yield $\mathbb{R}$

(iv) **Formulae:**

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

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 '$\cdot$'; $\underbrace{\text{ternary}}_{n=3}$ symbol ?
- p, q: **predicate symbols**, also with arity.
  Assume: constants $\mathit{true}, \mathit{false}$; 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).
  Called **boolean observable** if data type is $\{0, 1\}$.

  e.g. T
  $\mathcal{D}(T) = \{$red, green, yellow$\}$
- d: **elements** taken from data types $\mathcal{D}$ of observables.

  e.g. red
  green
  yellow

Symbols: Semantics

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

- 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:

g, $n=3$

$\hat{g} : \mathbb{R}^3 \to \mathbb{R}$

my choice: maximum

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

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

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

$\hat{+} := +$

math. addition fun.

- "Since the semantics is the expected one, we shall often simply use the symbols $0, 1, +, \cdot, =, <$ when we mean their semantics $\hat{0}, \hat{1}, \hat{+}, \hat{\cdot}, \hat{=}, \hat{<}$."

your choice maybe: average

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

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.

- 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

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

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

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

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

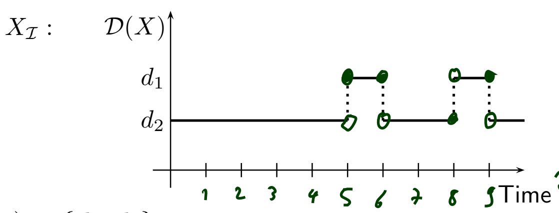
- For convenience, we shall abbreviate $\mathcal{I}(X)$ to $X_\mathcal{I}$: Time → $\mathcal{D}(X)$

e.g. $T_\mathcal{I}$

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

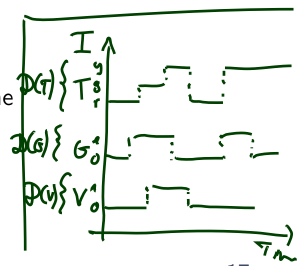
For instance,

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



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

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



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:**

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

(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

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 $d \in \mathcal{D}(X)$. $\in Obs$ $\in \mathcal{D}(X)$ (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 $\underbrace{X = 1}$ if $\mathcal{D}(X) = \cancel{\mathbb{B}}.\ \{0,1\}$.
  - Define $\vee$, $\implies$, $\iff$ as usual.

State Assertions: Semantics

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

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

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:

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

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

the same

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

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

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

State Assertions: Notes

by def on prev. slide

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

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.

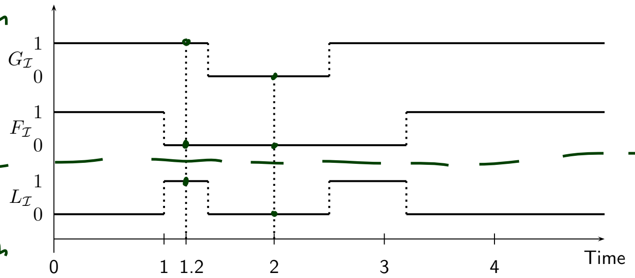
State Assertions: Example

- Boolean observables G and F.
- State assertion $L := \underbrace{G \land \neg F}_{}$, abbrev. for $(G=1) \land \neg(F=1)$

state variables F, G

interpretation of state variables

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



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

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

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

$$\mathcal{I}[\![F=1]\!](1.2) = 0 \quad \text{because} \quad \mathcal{I}(F)(1.2) = 0 \neq \hat{1} = 1$$

$$\mathcal{I}[\![\neg(F=1)]\!](1.2) = 1 - \mathcal{I}[\![F=1]\!](1.2) = 1 - 0 = 1$$

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