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 \((\text{Time} \rightarrow \times_{i=1}^{n} D(\text{obs}_i))\), 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
  \[ \text{Impl} \subseteq \text{Des} \quad (\text{or } \text{Impl} \subseteq \text{Req}) \]

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

- Typical liveness property:
  $$\exists t \in \text{Time} \bullet G(t)$$

- Typical bounded response property:
  $$\forall t_1 \in \text{Time} \bullet (R(t_1) \implies \exists t_2 \in [t_1 + 10, t_1 + 15] \bullet G(t_2))$$

- Typical duration property:
  $$\forall b, e \in \text{Time} \bullet \left( A(b, e) \implies \int_b^e C(t) \, dt \leq u(b, e) \right)$$
Duration Calculus
Duration Calculus: Preview

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

Back to our gas burner:

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

Strangest operators:

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

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

\( f, g, \text{true, false, } \leq, \geq, x, y, z, X, Y, Z, d \)

(ii) State Assertions:

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

(iii) Terms:

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

(iv) Formulae:

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

(v) Abbreviations:

\[ \left[ \right], \left[ P \right], \left[ P \right]^t, \left[ P \right]^{\leq t}, \Diamond F, \Box F \]
Symbols: Syntax

- $f, g$: **function symbols**, each with arity $n \in \mathbb{N}_0$.
  Called **constant** if $n = 0$.
  Assume: constants $0, 1, \ldots \in \mathbb{N}_0$; binary `+` and `·`.

- $p, q$: **predicate symbols**, also with arity.
  Assume: constants $true, false$; binary $=, <, >, \leq, \geq$.

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

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

- **Semantical domains** are
  - the **truth values** \( \mathbb{B} = \{tt, ff\} \),
  - the **real numbers** \( \mathbb{R} \),
  - **time** \( \text{Time} \),
    (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:
  - \( \hat{\text{true}} = \text{tt}, \hat{\text{false}} = \text{ff} \)
  - \( \hat{0} \in \mathbb{R} \) 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.
  - \( \hat{\max} : \mathbb{R}^3 \to \mathbb{R} : \text{we choose the maximum, so} \)

- “Since the semantics is the expected one, we shall often simply use the symbols 0, 1, +, \cdot, =, < when we mean their semantics \( \hat{0}, \hat{1}, \hat{+}, \hat{\cdot}, \hat{=}, \hat{<} \).”
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 $X_{\mathcal{I}}$.

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

For instance, $Y_{\mathcal{I}}$:

\[ X_{\mathcal{I}} : \mathcal{D}(X) \]
\[ Y_{\mathcal{I}} : \mathcal{D}(Y) \]

\[ \mathcal{D}(X) = \{d_1, d_2\} \cup \{d_3\} \]
\[ \mathcal{D}(Y) = \{0, 1\} \]
Duration Calculus: Overview

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

(i) Symbols:

\(0, 1, \pi, f, g, \text{true, false}, =, <, >, \leq, \geq, x, y, z, X, Y, Z, d\)

(ii) State Assertions:

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

(iii) Terms:

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

(iv) Formulae:

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

(v) Abbreviations:

\([\_], [P], [P]^t, [P]^{\leq t}, \Diamond F, \Box F\)
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 \( d \in D(X), \ X \text{ observable}, \)

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

• **Abbreviations**:
  - We shall write \( X \) instead of \( X = 1 \) if \( D(X) = \{0,1\} \)
  - Define \( \lor, \implies, \iff \) as usual.
State Assertions: Semantics

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

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

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

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

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

$$I[1](t) = 1$$

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

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

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

- $\mathcal{I}[P]$ 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 $L := G \land \neg F$. ($\text{unsat. } : (G=1) \land \neg (F=1)$)

$L_I(1.2) = 1$, because

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

because

$I[G](1.2) = I(G)(1.2) = 1$

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

$L_I(2) = 0$, because

$I[G](2) = 0$
References