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

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

Strangest operators:

almost everywhere — Example: \([G] \]
(Holds in a given interval \([b, c]\) 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.)

\(G, F, I, H : \{0, 1\}\)
Define \(L : \{0, 1\}\) as \(G \land \neg F\).
Duration Calculus: Overview

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

(i) Symbols:

• \( f, g \): function symbols, each with arity \( n \in \mathbb{N}_0 \).
  Called constant if \( n = 0 \).
  Assume: constants \( 0, 1, \cdots \in \mathbb{N}_0 \); binary ‘+’ and ‘.’.

• \( p, q \): predicate symbols, also with arity.
  Assume: constants \( \text{true}, \text{false} \); binary \( =, <, >, \leq, \geq \).

(ii) State Assertions:

• \( x, y, z \in \text{GVar} \): global variables.

(iii) Terms:

• \( X, Y, Z \in \text{Obs} \): state variables or observables, each of a data type \( D \) (or \( D(X), D(Y), D(Z) \) to be precise).
  Called boolean observable if data type is \( \{0, 1\} \).

(iv) Formulae:

• \( d \): elements taken from data types \( D \) of observables.
Symbols: Semantics

- **Semantical domains** are
  - the **truth values** $\mathbb{B} = \{tt, ff\}$,
  - the **real numbers** $\mathbb{R}$,
  - **time** $\text{Time}$,
    (mostly $\text{Time} = \mathbb{R}^+$ (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.
  $$\hat{p} : \mathbb{R}^n \rightarrow \mathbb{B}.$$

Symbols: Examples

- The **semantics** of the function and predicate symbols **assumed above** is fixed throughout the lecture:
  - $\text{true} = \text{tt}$, $\text{false} = \text{ff}$
  - $\hat{0} \in \mathbb{R}$ 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, +, ·, =, < 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

\[ \mathcal{V} : \text{GVar} \rightarrow \mathbb{R} \]

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.

\[ \{x, y, z\} \]

\[ \mathcal{V} = \{x \mapsto 3, y \mapsto 0, z \mapsto 2\} \]

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 \( \text{Val} \) 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 $I(X)$ to $X_I$.

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

For instance,

\[ X_I : \ D(X) \]

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

Duration Calculus: Overview

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

(i) **Symbols**:

- \( f, g, \ true, false, =, <, >, \leq, \geq \)
- \( x, y, z, X, Y, Z, d \)

(ii) **State Assertions**:

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

(iii) **Terms**:

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

(iv) **Formulae**:

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

(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:

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

with \( d \in \mathcal{D}(X) \), \( X \in \text{Obs} \).

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

- Abbreviations:
  - We shall write \( X \) instead of \( X = 1 \) if \( \mathcal{D}(X) = B \).
  - Define \( \lor, \Rightarrow, \iff \) as usual.

\[
\begin{align*}
\text{Ex.} & \quad \text{The light is red} \\
I[0](t) &= 0 \\
I[1](t) &= 1 \\
I[X = d](t) &= \begin{cases} 
1, & \text{if } I[X](t) = d \\
0, & \text{otherwise}
\end{cases} \\
I[\neg P_1](t) &= 1 - I[P_1](t) \\
I[P_1 \land P_2](t) &= \begin{cases} 
1, & \text{if } I[P_1](t) = I[P_2](t) = 1 \\
0, & \text{otherwise}
\end{cases}
\end{align*}
\]

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 \( t \in \text{Time} \).

- The value is defined inductively on the structure of \( P \):

\[
\begin{align*}
I[0](t) &= 0 \quad \text{ER} \\
I[1](t) &= 1 \quad \text{ER} \\
I[X = d](t) &= \begin{cases} 
1, & \text{if } I[X](t) = d \\
0, & \text{otherwise}
\end{cases} \\
I[\neg P_1](t) &= 1 - I[P_1](t) \\
I[P_1 \land P_2](t) &= \begin{cases} 
1, & \text{if } I[P_1](t) = I[P_2](t) = 1 \\
0, & \text{otherwise}
\end{cases}
\end{align*}
\]
State Assertions: Notes

- \( I[X](t) = I[X = 1](t) = I(X)(t) = X_I(t) \), if \( X \) boolean.

- \( I[P] \) is also called interpretation of \( P \).

We shall write \( P_I \) 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 \( L := G \wedge \neg F. \) \( (G=1) \wedge (F=1) \)

\[ \begin{array}{c|c|c|c|c|c|c|c|c} 
& G & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\hline 
F & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\hline 
L & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\end{array} \]

- \( L_I(1.2) = 1 \), because
  \[ I[G](1.2) = I[G=1](1.2) = 1 \quad \text{because} \quad f_G(1.2) = 1 \]
  \[ I[F](1.2) = I[F=1](1.2) = 0 \quad \text{because} \quad f_F(1.2) = 0 \]
  \[ I[L](1.2) = I[(G=1) \wedge \neg F](1.2) = 1 \quad \text{because} \quad I[L](1.2) = 1 \]

- \( L_I(2) = 0 \), because
  \[ I[G](2) = I[G=1](2) = 0 \quad \text{because} \quad f_G(2) = 0 \]
  \[ I[F](2) = I[F=1](2) = 1 \quad \text{because} \quad f_F(2) = 1 \]
  \[ I[L](2) = I[(G=1) \wedge \neg F](2) = 1 \quad \text{because} \quad I[L](2) = 1 \]
Duration Calculus: Overview

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

(i) **Symbols:**
\[ f, g, \text{true, false, } =, <, >, \leq, \geq, \quad x, y, z, \quad X, Y, Z, \quad d \]

(ii) **State Assertions:**
\[ P ::= 0 \mid 1 \mid X = d \mid \neg P_1 \mid P_1 \land P_2 \]

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

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

(v) **Abbreviations:**
\[ [], \quad [P], \quad [P]^t, \quad [P]^{\leq t}, \quad \Diamond F, \quad \square F \]

Terms: Syntax

- **Duration terms** (DC terms or just terms) are defined by the following grammar:
\[ \theta ::= x \mid \ell \mid \int P \mid f(\theta_1, \ldots, \theta_n) \]
where \( x \) is a global variable, \( \ell \) and \( \int \) are special symbols, \( P \) is a state assertion, and \( f \) a function symbol (of arity \( n \)).

- \( \ell \) 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

- Closed intervals in the time domain

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

Point intervals: \([b, b]\)
\[ \theta = x \cdot \int L \]

\[ V(x) = 20. \]

\[ \text{Terms: Semantics Well-defined?} \]

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

\[ P_I(t) = \begin{cases} 
1 & \text{if } t \in \mathbb{Q} \\
0 & \text{if } t \notin \mathbb{Q}
\end{cases} \]

- 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 \( X_I \) is constant on each part.

Thus on each interval \([b, e]\) the function \( X_I \) has only finitely many points of discontinuity.