

Real-Time Systems

Lecture 04: Duration Calculus II

2012-05-09

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- Started DC Syntax and Semantics: Symbols, State Assertions

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
 - Read (and at best also write) Duration Calculus terms.
- **Content:**
 - Duration Calculus continued

Duration Calculus Cont'd

Duration Calculus: Overview

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

$$I: \text{Obs} \rightarrow (\text{Time} \rightarrow \mathcal{D})$$

$$\left| \begin{array}{l} X_I: \text{Time} \rightarrow \mathcal{D}(X) \end{array} \right.$$

(i) **Symbols:**

$$0, 1, 3, 4, \dots, f, g, \text{ true, false, } =, <, >, \leq, \geq, x, y, z, X, Y, Z, d$$

(ii) **State Assertions:** $\sqrt{\quad} I \llbracket P \rrbracket: \text{Time} \rightarrow \{0, 1\}$

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

(iii) **Terms:**

$$\sqrt{\quad} I \llbracket \theta \rrbracket: \text{Intr} \times \text{Val} \rightarrow \mathbb{R}$$

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

(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:**

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

Terms: Syntax

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

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

where x is a global variable, ℓ and f 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**.

Example: $x + (y \cdot z) - 27$ is 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: $[b, b]$

- Let $GVar$ be the set of global variables.
A valuation of $GVar$ is a function

$$V: GVar \rightarrow \mathbb{R}$$

We use Val to denote the set of all valuations of $GVar$, i.e. $Val = (GVar \rightarrow \mathbb{R})$.

Terms: Semantics

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

$$\mathcal{I}[\theta] : \text{Val} \times \text{Intv} \rightarrow \mathbb{R}$$

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 :

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

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

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

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

Terms: Semantics Well-defined?

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

$$P_{\mathcal{I}}(t) = \begin{cases} 1 & , \text{ if } t \in \mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \right\} \\ 0 & , \text{ if } t \notin \mathbb{Q} \end{cases}$$

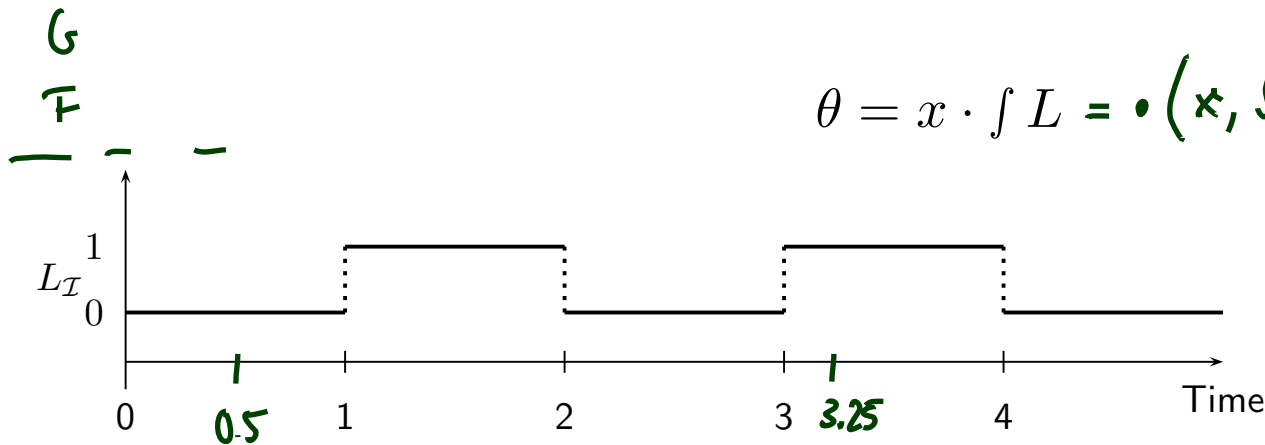
- To exclude such functions, DC considers only interpretations \mathcal{I} satisfying the following condition of **finite variability**:

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**.

Terms: Example

$$L = G \wedge \neg F$$



$$\theta = x \cdot \int L = \bullet(x, \int L)$$

$$V(x) = 20.$$

$$\bullet \theta_1 = \int 0 + x = +(\int 0, x)$$

$$\mathbb{I}[\theta_1] (V, [1, 2]) = \hat{+}(\mathbb{I}[\int 0] (V, [1, 2]), \mathbb{I}[x] (V, [1, 2])) = \hat{+}(0, 20) = 20 \in \mathbb{R}$$

$$\mathbb{I}[\int 0] (V, [1, 2]) = \int_1^2 \frac{0_{\mathbb{I}}(t)}{\mathbb{I}} dt = \int_1^2 \frac{\mathbb{I}[0](t)}{\mathbb{I}} dt = 0 \in \mathbb{R}$$

$$\mathbb{I}[x] (V, [1, 2]) = V(x) = 20 \in \mathbb{R}$$

$$\bullet \mathbb{I}[\int L] (V, [0.5, 3.25]) = \int_{0.5}^{3.25} L_I(t) dt = 1.25$$

$$\mathbb{I}[\theta] (V, [0.5, 3.25]) = \hat{\bullet}(20, 1.25) = 25$$

$:\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$

$\mathbb{I} \in \mathbb{R}$

$\mathbb{I} \in \mathbb{R}$

$\mathbb{I} \in \mathbb{R}$
 $:\text{Time} \rightarrow \mathbb{R}$

Terms: Remarks

"finitely many points don't matter"

Remark 2.5. The semantics $\mathcal{I}[\theta]$ of a term is insensitive against changes of the interpretation \mathcal{I} at individual time points.

Let $\mathcal{I}_1, \mathcal{I}_2$ be interpretations such that $\mathcal{I}_1(x)(t) = \mathcal{I}_2(x)(t)$ for all x for all $t \in \text{Time}$ except for $t_0 \in \text{Time}$.

Then $\mathcal{I}_1[\theta](\mathcal{V}, [b, e]) = \mathcal{I}_2[\theta](\mathcal{V}, [b, e])$.

Remark 2.6. The semantics $\mathcal{I}[\theta](\mathcal{V}, [b, e])$ of a rigid term does not depend on the interval $[b, e]$.

Duration Calculus: Overview

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

(i) **Symbols:**

0, 1, 3.14, $a \in \mathbb{R}$, f, g , *true*, *false*, =, <, >, ≤, ≥, 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:** $\Gamma \llbracket F \rrbracket: \text{Val} \times \text{Val} \rightarrow \{\text{tt}, \text{ff}\}$

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

(v) **Abbreviations:**

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

Formulae: Syntax

- The set of **DC formulae** is defined by the following grammar:

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

where p is a predicate symbol, θ_i a term, x a global variable.

- **chop operator**: ‘;’
 - **atomic formula**: $p(\theta_1, \dots, \theta_n)$
 - **rigid formula**: all terms are rigid
 - **chop free**: ‘;’ doesn’t occur
 - usual notion of **free** and **bound** (global) variables
-
- Note: quantification only over (**first-order**) global variables, not over (**second-order**) state variables.

Formulae: Priority Groups

- To avoid parentheses, we define the following five priority groups from highest to lowest priority:

- \neg

(negation)

- $;$

(chop)

- \wedge, \vee

(and/or)

- \implies, \iff

(implication/equivalence)

- \exists, \forall

(quantifiers)

Examples:

- $\neg F ; F \vee H$

$(\neg F ; F) \vee H$

$((\neg F) ; F) \vee H$ ✓

$(\neg F) ; (F \vee H)$

- $\forall x \bullet (F \wedge G)$

Syntactic Substitution...

...of a term θ for a variable x in a formula F .

- We use

$$F[x := \theta]$$

to denote the formula that results from performing the following steps:

- (i) transform F into \tilde{F} by (consistently) renaming bound variables such that no free occurrence of x in \tilde{F} appears within a quantified subformula $\exists z \bullet G$ or $\forall z \bullet G$ for some z occurring in θ ,
- (ii) textually replace all free occurrences of x in \tilde{F} by θ .

Examples: $F := (x \geq y \implies \exists z \bullet z \geq 0 \wedge x = y + z)$, $\theta_1 := l$, $\theta_2 := l + z$,

- $F[x := \theta_1] = (l \geq y \implies \exists z \bullet z \geq 0 \wedge l = y + z)$
- $F[x := \theta_2] = (l + z \geq y \implies \exists \tilde{z} \bullet \tilde{z} \geq 0 \wedge l + z = y + \tilde{z})$

Formulae: Semantics

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

$$\mathcal{I}[[F]] : \text{Val} \times \text{Intv} \rightarrow \{\text{tt}, \text{ff}\}$$

i.e. $\mathcal{I}[[F]](\mathcal{V}, [b, e])$ is the truth value of F under interpretation \mathcal{I} and valuation \mathcal{V} in the interval $[b, e]$.

- This value is defined **inductively** on the structure of F :

$$\mathcal{I}[[p(\theta_1, \dots, \theta_n)]](\mathcal{V}, [b, e]) = \hat{p}\left(\mathcal{I}[[\theta_1]](\mathcal{V}, [b, e]), \dots, \mathcal{I}[[\theta_n]](\mathcal{V}, [b, e])\right)$$

$$\mathcal{I}[[\neg F_1]](\mathcal{V}, [b, e]) = \text{tt} \text{ iff } \mathcal{I}[[F_1]](\mathcal{V}, [b, e]) = \text{ff}$$

$$\mathcal{I}[[F_1 \wedge F_2]](\mathcal{V}, [b, e]) = \text{tt} \text{ iff } \mathcal{I}[[F_i]](\mathcal{V}, [b, e]) = \text{tt}, \quad i=1,2$$

$$\mathcal{I}[[\forall x \bullet F_1]](\mathcal{V}, [b, e]) = \text{tt} \text{ iff for all } a \in \mathbb{R} \text{ the symbol!}$$

$$\mathcal{I}[[F_1[x:=a]]](\mathcal{V}, [b, e]) = \text{tt}$$

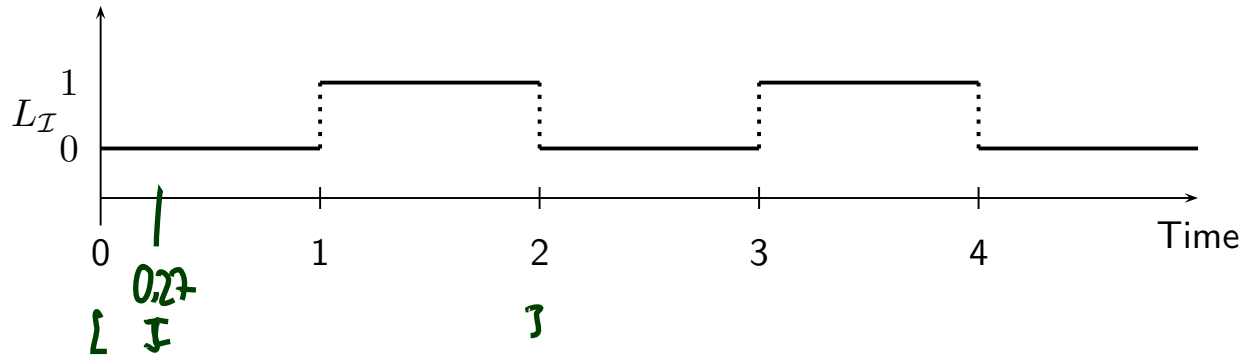
$$\mathcal{I}[[F_1 ; F_2]](\mathcal{V}, [b, e]) = \text{tt} \text{ iff there is an } m \in [b, e] \text{ such that } \mathcal{I}[[F_1]](\mathcal{V}, [b, m]) = \text{tt} \text{ and } \mathcal{I}[[F_2]](\mathcal{V}, [m, e]) = \text{tt}.$$

Formulae: Example

$$F := \int^{L=1} (L) = 0; \int^{L=1} (L) = 1$$

$$\int (X = \text{open}) > 1$$

$$\int (L=1) > 2$$



- $\mathcal{I}[F](\mathcal{V}, [0, 2]) = \#$ (*)
 choose $m=1.0$: $\mathcal{I}[\mathcal{L}=0](\mathcal{V}, [0, 1]) = \#$ because $\mathcal{I}[\mathcal{L}=0](\mathcal{V}, [0, 1]) = \int_0^1 \mathcal{L}_I(t) dt = 0$
 and $\mathcal{I}[\mathcal{L}=0](\mathcal{V}, [0, 1]) = \hat{=} (0, 0) = \#$
 $\mathcal{I}[\mathcal{L}=1](\mathcal{V}, [1, 2]) = \hat{=} (1, 1) = \#$
 all math., not DC symbols

what about

$m = 0.27$: witness for (*) \rightarrow chop point not necessarily unique

$m = 1.75$: no witness for (*)

References

References

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