Real-Time Systems

Lecture 04: Duration Calculus II

2013-04-24

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 and formulae.
- **Content:**
  - Duration Calculus Terms
  - Duration Calculus Formulae

Duration Calculus Cont'd

Duration Calculus: Overview

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

(i) **Symbols:**

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

(ii) **State Assertions:**

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

evaluated to 0,1

(iii) **Terms:**

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

evaluated to $\mathbb{R}$

(iv) **Formulae:**

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

evaluate to tt, ff

(v) **Abbreviations:**

$$\lceil\rceil, \quad \lceil P \rceil, \quad \lceil P \rceil^t, \quad \lceil P \rceil^{\leq t}, \quad \Diamond F, \quad \Box F$$

Terms: Syntax

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

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

where x is a global variable, ℓ and $\int$ 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: $x + (y-z) \cdot 3 + 27$ is rigid

$\ell + x \cdot 3$ is not rigid

Terms: Semantics

"begin" "end"

- Closed **intervals** in the time domain

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

Point intervals: $[b, b]$

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

  $$\mathcal{V} : GVar \longrightarrow \mathbb{R}$$

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

Terms: Semantics

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

$$\mathcal{I}[\![\theta]\!] : \mathsf{Val} \times \mathsf{Intv} \to \mathbb{R}$$

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:

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

classical Riemann integral

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

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

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

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

ternary $(x, \int P, \ell)$ syntax | $: \mathbb{R}^3 \to \mathbb{R}$ semantic

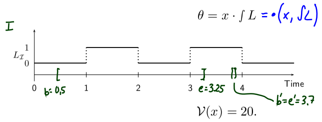
$: \mathbb{R}^n \to \mathbb{R}$

Terms: Example

$L : G \wedge \neg T$

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

$\mathcal{I}$



$$\mathcal{V}(x) = 20.$$

- $\mathcal{I}[\![\theta]\!](\mathcal{V}, [b,e]) = \hat{\bullet}\left(\mathcal{I}[\![x]\!](\mathcal{V}, [b,e]), \mathcal{I}[\![\int L]\!](\mathcal{V}, [b,e])\right) = \hat{\bullet}(20, 1.25) = 25$

  $\mathcal{I}[\![x]\!](\mathcal{V}, [b,e]) = \mathcal{V}(x) = 20$

  $\mathcal{I}[\![\int L]\!](\mathcal{V}, [b,e]) = \int_b^e L_{\mathcal{I}}(t)\, dt = \int_{0.5}^{3.25} L_{\mathcal{I}}(t)\, dt = 1.25$

- $\mathcal{I}[\![\theta]\!](\mathcal{V}, [b',e']) = \cancel{20}$ 0 because $\int_{3.7}^{3.7} L_{\mathcal{I}}(t)\, dt = 0$

Terms: Semantics Well-defined?

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

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

- 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: Remarks

"finitely many points do not 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 except for one $t_0 \in \mathrm{Time}$.
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:**

$$a \in \mathbb{R}, f, g, \quad \mathit{true}, \mathit{false}, =, <, >, \leq, \geq, \quad x, y, z, \quad X, Y, Z, \quad d$$

(ii) **State Assertions:**

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

(iii) **Terms:**

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

(iv) **Formulae:**

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

(v) **Abbreviations:**

$$\lceil\,\rceil, \quad \lceil P \rceil, \quad \lceil P \rceil^t, \quad \lceil P \rceil^{\leq t}, \quad \Diamond F, \quad \Box F$$

Formulae: Syntax

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

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

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

- **chop operator**: '**;**'
- **atomic formula**: $p(\theta_1, \ldots, \theta_n)$
- **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: $F := (x \geq y \implies \exists z \bullet z \geq 0 \wedge x = y + z)$, $\quad \theta_1 := \ell$, $\quad \theta_2 := \ell + z$,

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

Formulae: Semantics

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

$$\mathcal{I}[\![F]\!] : \mathsf{Val} \times \mathsf{Intv} \to \{\mathrm{tt}, \mathrm{ff}\}$$

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 $[b,e]$.

$: \mathbb{R}^n \to \{tt, ff\}$ $\quad \in \mathbb{R}$ $\quad \in \mathbb{R}$

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

$$\mathcal{I}[\![p(\theta_1, \ldots, \theta_n)]\!](\mathcal{V}, [b,e]) = \hat{p}(\mathcal{I}[\![\theta_1]\!](\mathcal{V}, [b,e]), \ldots, \mathcal{I}[\![\theta_n]\!](\mathcal{V}, [b,e]))$$

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

$$\mathcal{I}[\![F_1 \wedge F_2]\!](\mathcal{V}, [b,e]) = \mathrm{tt} \text{ iff } \mathcal{I}[\![F_1]\!](\mathcal{V}, [b,e]) = \mathcal{I}[\![F_2]\!](\mathcal{V}, [b,e]) = tt$$

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

the symbol

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

Formulae: Example

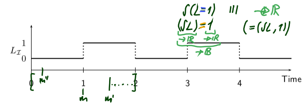
$p ::= x = d$

$$F := \textstyle\int L = 0 \,;\, \int L = 1$$

$\int (L = 1)$ ||| $\to \mathbb{R}$

$\underbrace{\underbrace{(\int L)}_{\to \mathbb{R}} = \underbrace{1}_{\to \mathbb{R}}}_{\to \mathbb{B}}$ $\quad (= (\int L, 1))$

$\underbrace{\underbrace{(\int \underbrace{G = 1}_{StA})}_{term} = 3}_{formula}$



- $\mathcal{I}[\![F]\!](\mathcal{V}, [0,2]) = tt$

Proof: Choose $m = 1$

$\mathcal{I}[\![\int L = 0]\!](\mathcal{V}, [0,1]) = \hat{=}(0, \hat{0}) = tt$

$\mathcal{I}[\![\int L]\!](\mathcal{V}, [0,1]) = 0$

$\mathcal{I}[\![\int L = 1]\!](\mathcal{V}, [1,2]) = \hat{=}(1, \hat{1}) = tt$

$\mathcal{I}[\![\int L]\!](\mathcal{V}, [1,2]) = 1$

- The chop point is not unique here. All $m \in [0,1]$ are proper chop points.
- $\int \neg L = 1 \,;\, \int L = 1$

References

References

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