Real-Time Systems

Lecture 04: Duration Calculus II

2014-05-15

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 Formulae
  - Duration Calculus Abbreviations
  - Satisfiability, Realisability, Validity

Duration Calculus Cont'd

Duration Calculus: Overview

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

(i) **Symbols:**

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

(ii) **State Assertions:**

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

(iii) **Terms:**

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

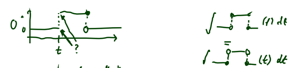
(iv) **Formulae:**

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

(v) **Abbreviations:**

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

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 of Obs such that $\mathcal{I}_1(X)(t) = \mathcal{I}_2(X)(t)$ for all $X \in Obs$ and all $t \in Time \setminus \{t_0, \dots, t_n\}$.
Then $\mathcal{I}_1[\![\theta]\!]((b,e),\mathcal{V}) = \mathcal{I}_2[\![\theta]\!]((b,e),\mathcal{V})$.

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:**

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

(ii) **State Assertions:**

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

(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:**

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

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

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

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 $[b,e]$.

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

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

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

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

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

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

used as symbol! strings/symbols denoting reals

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

symbols | Math.

one | $\hat{one} = 1$

onedotone | $\widehat{onedotone} = 1.01$

pi | $\mathbb{R} = \{1, 1.01, \pi, \dots\}$

...

$1^{\circledast}$ | $\hat{1^{\circledast}} = 1$

$1.01^{\circledast}$

$\pi^{\circledast}$

$\hat{1} = 1$

$\mathbb{R} \begin{cases} 1 \\ 1.01 \\ \pi \\ \dots \end{cases}$

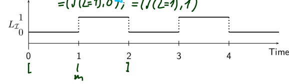
Formulae: Example

$F ::= p(\dots) \mid \neg \dots$
$F_1 ; F_2$

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

$0^{\circledast}$ and $1^{\circledast}$, fun. symbols

$(\int(L=1)) = 0 \,;\, (\int(L=1)) = 1$
$= (\int(L=1), 0) \,;\, = (\int(L=1), 1)$



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

Proof: Choose $m = 1$ as chop point.

$\mathcal{I}[\![\int L = 0]\!](\mathcal{V}, [0,1]) = \hat{=}\big(\mathcal{I}[\![\int L]\!](\mathcal{V}, [0,1]), \hat{0}\big) = \hat{=}\big(\int_0^1 L_{\mathcal{I}}(t)\,dt, \hat{0}\big) = \hat{=}(0,0) = \mathrm{tt}$ $\quad \in \mathbb{R}$

$\mathcal{I}[\![\int L = 1]\!](\mathcal{V}, [1,2]) = \quad \hat{=}\big(\int_1^2 L_{\mathcal{I}}(t)\,dt, 1\big) = \hat{=}(1,1) = \mathrm{tt}$

- The chop point here is not unique! All $m \in [0,1]$ are proper chop points.
- For $\int \neg L = 1 ; \int L = 1$ on $[0,2]$ $m = 1$ is unique

Formulae: Remarks

Remark 2.10. [*Rigid and chop-free*] Let F be a duration formula, $\mathcal{I}$ an interpretation, $\mathcal{V}$ a valuation, and $[b,e] \in$ Intv.

- If F is **rigid**, then

$$\forall\, [b',e'] \in \mathsf{Intv} : \mathcal{I}[\![F]\!](\mathcal{V},[b,e]) = \mathcal{I}[\![F]\!](\mathcal{V},[b',e']).$$

- If F is **chop-free** or θ is **rigid**, then in the calculation of the semantics of F, every occurrence of θ denotes the same value.

e.g. $\underbrace{f(\ell)}_{\theta} > 3\ ;\ \underbrace{f(\ell)}_{\theta} > 5$

not e.g. $\underbrace{\ell}_{\theta} > 0\ ;\ \underbrace{\ell}_{\theta} > 1$

Substitution Lemma

syntactic subst.

function modification

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

$\mathcal{V}[x:=a] := \begin{cases} a, & \text{if } y = x \\ \mathcal{V}(y), & \text{else} \end{cases}$ (y)

Lemma 2.11. [*Substitution*]
Consider a formula F, a global variable x, and a term θ such that F is **chop-free** or θ is **rigid**.
Then for all interpretations $\mathcal{I}$, valuations $\mathcal{V}$, and intervals $[b,e]$,

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

where $a = \mathcal{I}[\![\theta]\!](\mathcal{V},[b,e])$.

Negative example:

- $F := ((\ell = x) ; (\ell = x)) \implies (\ell = 2 \cdot x)$, $\quad \theta := \ell$

$\mathcal{I}[\![F[x:=\theta]]\!](\mathcal{V},[b,e]) = \mathcal{I}[\![\ell=\ell ; \ell=\ell \Rightarrow \ell = 2\cdot\ell]\!](\mathcal{V},[b,e]) = ff$ if $b<e$

$\mathcal{I}[\![F]\!](\mathcal{V}[x:=a],[b,e]) = tt$ (even valid)

Duration Calculus: Overview

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

(i) **Symbols:**

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

(ii) **State Assertions:**

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

(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:**

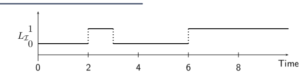
$$\lceil\rceil, \quad \lceil P \rceil, \quad \lceil P \rceil^t, \quad \lceil P \rceil^{\leq t}, \quad \Diamond F, \quad \Box F$$

Duration Calculus Abbreviations

Abbreviations

- $\lceil\rceil := \ell = 0$ **(point interval)**
- $\lceil P \rceil := \int P = \ell \wedge \ell > 0$ **(almost everywhere)**
- $\lceil P \rceil^t := \lceil P \rceil \wedge \ell = t$ **(for time t)**
- $\lceil P \rceil^{\leq t} := \lceil P \rceil \wedge \ell \leq t$ **(up to time t)**
- $\Diamond F := true \,;\, F \,;\, true$ **(for some subinterval)**
- $\Box F := \neg\Diamond\neg F$ **(for all subintervals)**

Abbreviations: Examples



$\mathcal{I}[\![\ \int L = 0\ ]\!](\mathcal{V},\ [0,2]\ ) =$

$\mathcal{I}[\![\ \int L = 1\ ]\!](\mathcal{V},\ [2,6]\ ) =$

$\mathcal{I}[\![\ \int L = 0 ; \int L = 1\ ]\!](\mathcal{V},\ [0,6]\ ) =$

$\mathcal{I}[\![\ \lceil \neg L \rceil\ ]\!](\mathcal{V},\ [0,2]\ ) =$

$\mathcal{I}[\![\ \lceil L \rceil\ ]\!](\mathcal{V},\ [2,3]\ ) =$

$\mathcal{I}[\![\ \lceil \neg L \rceil ; \lceil L \rceil\ ]\!](\mathcal{V},\ [0,3]\ ) =$

$\mathcal{I}[\![\ \lceil \neg L \rceil ; \lceil L \rceil ; \lceil \neg L \rceil\ ]\!](\mathcal{V},\ [0,6]\ ) =$

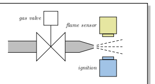
$\mathcal{I}[\![\ \Diamond \lceil L \rceil\ ]\!](\mathcal{V},\ [0,6]\ ) =$

$\mathcal{I}[\![\ \Diamond \lceil \neg L \rceil\ ]\!](\mathcal{V},\ [0,6]\ ) =$

$\mathcal{I}[\![\ \Diamond \lceil \neg L \rceil^2\ ]\!](\mathcal{V},\ [0,6]\ ) =$

$\mathcal{I}[\![\ \Diamond \lceil \neg L \rceil^2 ; \lceil \neg L \rceil^1 ; \lceil \neg L \rceil^3\ ]\!](\mathcal{V},\ [0,6]\ ) =$

Duration Calculus: Preview



- $G, F, I, H : \{0, 1\}$
- Define $L : \{0, 1\}$ as $G \wedge \neg F$.

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

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.)

DC Validity, Satisfiability, Realisability

Validity, Satisfiability, Realisability

Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, $[b, e]$ an interval, and F a DC formula.

- $\mathcal{I}, \mathcal{V}, [b, e] \models F$ ("F **holds** in $\mathcal{I}$, $\mathcal{V}$, $[b, e]$") iff $\mathcal{I}[\![F]\!](\mathcal{V}, [b, e]) = \mathrm{tt}$.

Validity, Satisfiability, Realisability

Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, $[b, e]$ an interval, and F a DC formula.

- $\mathcal{I}, \mathcal{V}, [b, e] \models F$ ("F **holds** in $\mathcal{I}$, $\mathcal{V}$, $[b, e]$") iff $\mathcal{I}[\![F]\!](\mathcal{V}, [b, e]) = \mathrm{tt}$.
- F is called **satisfiable** iff it holds in some $\mathcal{I}$, $\mathcal{V}$, $[b, e]$.

Validity, Satisfiability, Realisability

Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, $[b, e]$ an interval, and F a DC formula.

- $\mathcal{I}, \mathcal{V}, [b, e] \models F$ ("F **holds** in $\mathcal{I}$, $\mathcal{V}$, $[b, e]$") iff $\mathcal{I}[\![F]\!](\mathcal{V}, [b, e]) = \mathrm{tt}$.
- F is called **satisfiable** iff it holds in some $\mathcal{I}$, $\mathcal{V}$, $[b, e]$.

- $\mathcal{I}, \mathcal{V} \models F$ ("$\mathcal{I}$ and $\mathcal{V}$ **realise** F") iff $\forall [b, e] \in \mathsf{Intv} : \mathcal{I}, \mathcal{V}, [b, e] \models F$.

Validity, Satisfiability, Realisability

Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, $[b, e]$ an interval, and F a DC formula.

- $\mathcal{I}, \mathcal{V}, [b, e] \models F$ ("F **holds** in $\mathcal{I}$, $\mathcal{V}$, $[b, e]$") iff $\mathcal{I}[\![F]\!](\mathcal{V}, [b, e]) = \mathrm{tt}$.
- F is called **satisfiable** iff it holds in some $\mathcal{I}$, $\mathcal{V}$, $[b, e]$.

- $\mathcal{I}, \mathcal{V} \models F$ ("$\mathcal{I}$ and $\mathcal{V}$ **realise** F") iff $\forall [b, e] \in \mathsf{Intv} : \mathcal{I}, \mathcal{V}, [b, e] \models F$.
- F is called **realisable** iff some $\mathcal{I}$ and $\mathcal{V}$ realise F.

Validity, Satisfiability, Realisability

Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, $[b,e]$ an interval, and F a DC formula.

- $\mathcal{I}, \mathcal{V}, [b,e] \models F$ ("F **holds** in $\mathcal{I}$, $\mathcal{V}$, $[b,e]$") iff $\quad \mathcal{I}[\![F]\!](\mathcal{V},[b,e]) = \mathrm{tt}$.
- F is called **satisfiable** iff it holds in some $\mathcal{I}$, $\mathcal{V}$, $[b,e]$.
- $\mathcal{I}, \mathcal{V} \models F$ ("$\mathcal{I}$ and $\mathcal{V}$ **realise** F") iff $\quad \forall [b,e] \in \mathsf{Intv} : \mathcal{I}, \mathcal{V}, [b,e] \models F$.
- F is called **realisable** iff some $\mathcal{I}$ and $\mathcal{V}$ realise F.
- $\mathcal{I} \models F$ ("$\mathcal{I}$ **realises** F") iff $\quad \forall \mathcal{V} \in \mathsf{Val} : \mathcal{I}, \mathcal{V} \models F$.

Validity, Satisfiability, Realisability

Let $\mathcal{I}$ be an interpretation, $\mathcal{V}$ a valuation, $[b,e]$ an interval, and F a DC formula.

- $\mathcal{I}, \mathcal{V}, [b,e] \models F$ ("F **holds** in $\mathcal{I}$, $\mathcal{V}$, $[b,e]$") iff $\quad \mathcal{I}[\![F]\!](\mathcal{V},[b,e]) = \mathrm{tt}$.
- F is called **satisfiable** iff it holds in some $\mathcal{I}$, $\mathcal{V}$, $[b,e]$.
- $\mathcal{I}, \mathcal{V} \models F$ ("$\mathcal{I}$ and $\mathcal{V}$ **realise** F") iff $\quad \forall [b,e] \in \mathsf{Intv} : \mathcal{I}, \mathcal{V}, [b,e] \models F$.
- F is called **realisable** iff some $\mathcal{I}$ and $\mathcal{V}$ realise F.
- $\mathcal{I} \models F$ ("$\mathcal{I}$ **realises** F") iff $\quad \forall \mathcal{V} \in \mathsf{Val} : \mathcal{I}, \mathcal{V} \models F$.
- $\models F$ ("F is **valid**") iff $\quad \forall$ interpretation $\mathcal{I} : \mathcal{I} \models F$.

Validity vs. Satisfiability vs. Realisability

Remark 2.13. For all DC formulae F,

- F is satisfiable iff $\neg F$ is not valid,
  F is valid iff $\neg F$ is not satisfiable.
- If F is valid then F is realisable, but not vice versa.
- If F is realisable then F is satisfiable, but not vice versa.

Examples: Valid? Realisable? Satisfiable?

- $\ell \geq 0$
- $\ell = \int 1$
- $\ell = 30 \iff \ell = 10 \,;\, \ell = 20$
- $((F\,;G)\,;H) \iff (F\,;(G\,;H))$
- $\int L \leq x$
- $\ell = 2$

Initial Values

- $\mathcal{I}, \mathcal{V} \models_0 F$ ("$\mathcal{I}$ and $\mathcal{V}$ **realise** F **from** 0") iff

  $$\forall t \in \mathsf{Time} : \mathcal{I}, \mathcal{V}, [0,t] \models F.$$

- F is called **realisable from** 0 iff some $\mathcal{I}$ and $\mathcal{V}$ realise F from 0.
- Intervals of the form $[0,t]$ are called **initial intervals**.
- $\mathcal{I} \models_0 F$ ("$\mathcal{I}$ **realises** F **from** 0") iff $\quad \forall \mathcal{V} \in \mathsf{Val} : \mathcal{I}, \mathcal{V} \models_0 F$.
- $\models_0 F$ ("F is **valid from** 0") iff $\quad \forall$ interpretation $\mathcal{I} : \mathcal{I} \models_0 F$.

Initial or not Initial...

For all interpretations $\mathcal{I}$, valuations $\mathcal{V}$, and DC formulae F,

(i) $\mathcal{I}, \mathcal{V} \models F$ implies $\mathcal{I}, \mathcal{V} \models_0 F$,

(ii) if F is realisable then F is realisable from 0, but not vice versa,

(iii) F is valid iff F is valid from 0.

References

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