Real-Time Systems

Lecture 05: Duration Calculus III

2012-05-15

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- DC Syntax and Semantics: Terms, Formulae

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
  - Read (and at best also write) Duration Calculus formulae – including abbreviations.
  - What is Validity/Satisfiability/Realisability for DC formulae?
  - How can we prove a design correct?
- **Content:**
  - Duration Calculus Abbreviations
  - Basic Properties
  - Validity, Satisfiability, Realisability

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:**

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

(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: Remarks

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

- 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.

rigid: $(x>0)_{[1}\ldots \vee (x>0)_{[n}\ldots$

$(\int L>0)_{[1}\ldots \vee (\int L>0)_{[n}\ldots$

Substitution Lemma

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 $[b, e]$,

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

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

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

VALID

$V(x) = 3$
$[b,e] = [5,11]$

$d = \mathcal{I}[\![\ell]\!](V, [b,e]) = 6$

$(6 = x); (6 = x) \Rightarrow 6 = 2 \cdot x$ ↯ NOT 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:**

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

(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:**

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

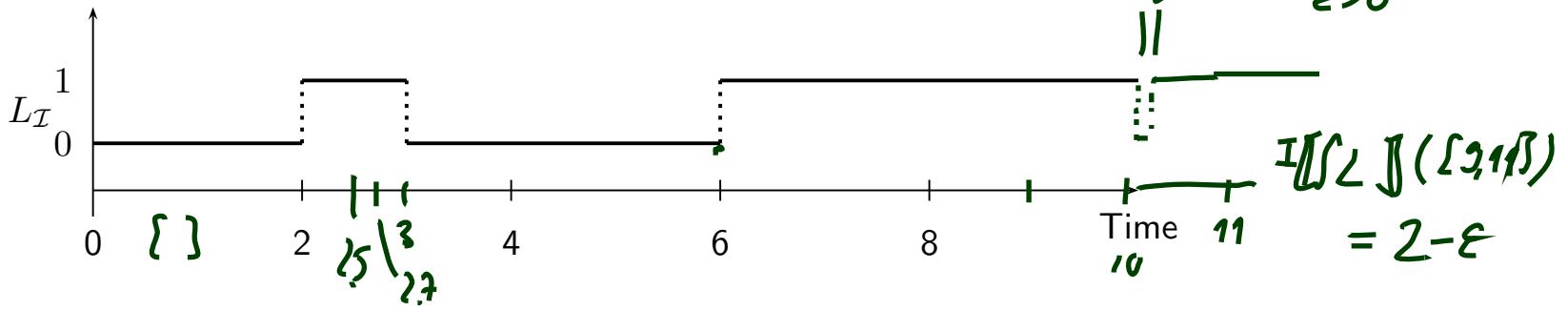
Duration Calculus Abbreviations

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)**

- $\Diamond F := \mathit{true} \,;\, F \,;\, \mathit{true}$ **(for some subinterval)**
- $\Box F := \neg \Diamond \neg F$ **(for all subintervals)**

Abbreviations: Examples



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

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

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

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

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

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

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

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

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

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

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

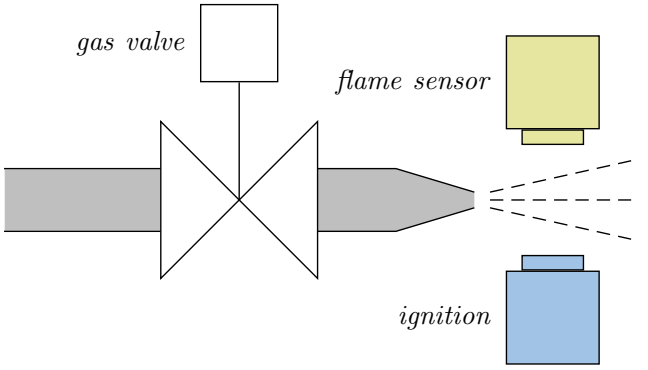
$$\mathcal{I}[\![\ \lceil \neg L \rceil^2 ; \lceil L \rceil^1 ; \lceil \neg L \rceil^3\ ]\!](\mathcal{V}, [0,6]) = tt$$

Duration Calculus: Looking back

- 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 $G \wedge \neg F$.



Strangest operators:

- **everywhere** — Example: $\lceil G \rceil$

  (Holds in a given interval $[b, e]$ iff the gas valve is open almost everywhere.)

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

  (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 $\quad \mathcal{I}[\![F]\!](\mathcal{V}, [b, e]) = \mathsf{tt}$.
- 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?

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

	Satisfiable	Realisable	Valid
$\ell \geq 0$	✓	✓	✓
$\ell = \int 1$	✓	✓	✓
$\ell = 30 \iff \ell = 10 \,;\, \ell = 20$	✓	✓	✓
$((F \,;\, G) \,;\, H) \iff (F \,;\, (G \,;\, H))$	✓	✓	✓
$\int L \leq x$	✓	✓	✗
$\ell = 2$	✓	✗	✗

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 $\mathcal{I}, \mathcal{V} \models_0 F$, but not vice versa,

(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.

Specification and Semantics-based Correctness Proofs of Real-Time Systems with DC

Methodology: Ideal World...

(i) Choose a collection of **observables** 'Obs'.

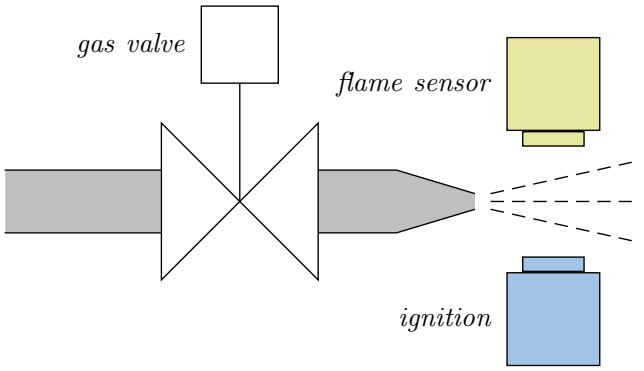
(ii) Provide the **requirement**/**specification** 'Spec' as a conjunction of DC formulae (over 'Obs').

(iii) Provide a description 'Ctrl' of the **controller** in form of a DC formula (over 'Obs').

(iv) We say 'Ctrl' is **correct** (wrt. 'Spec') iff

$$\models_0 \mathsf{Ctrl} \implies \mathsf{Spec}.$$

Gas Burner Revisited



(i) Choose **observables**:

- two boolean observables G and F
  (i.e. Obs $= \{G, F\}$, $\mathcal{D}(G) = \mathcal{D}(F) = \{0, 1\}$)
- $G = 1$: gas valve open (output)
- $F = 1$: have flame (input)
- define $L := G \wedge \neg F$ (leakage)

(ii) Provide the **requirement**:

$$\text{Req} : \Longleftrightarrow \ \square(\ell \geq 60 \implies 20 \cdot \int L \leq \ell)$$

Gas Burner Revisited

(iii) Provide a description 'Ctrl'
of the **controller** in form of a DC formula (over 'Obs').
Here, firstly consider a **design**:

- Des-1 : $\iff \Box(\lceil L \rceil \implies \ell \leq 1)$
- Des-2 : $\iff \Box(\lceil L \rceil \,;\, \lceil \neg L \rceil \,;\, \lceil L \rceil \implies \ell > 30)$

(iv) Prove **correctness**:

- We want (or do we want $\models_0$...?):

$$\models (\text{Des-1} \wedge \text{Des-2} \implies \text{Req}) \qquad \text{(Thm. 2.16)}$$

- We do show

$$\models \text{Req-1} \implies \text{Req} \qquad \text{(Lem. 2.17)}$$

with the simplified requirement

$$\text{Req-1} := \Box(\ell \leq 30 \implies \textstyle\int L \leq 1),$$

- and we show

$$\models (\text{Des-1} \wedge \text{Des-2}) \implies \text{Req-1}. \qquad \text{(Lem. 2.19)}$$

Gas Burner Revisited: Lemma 2.17

Claim:

$$\models \underbrace{\Box(\ell \leq 30 \implies \int L \leq 1)}_{\text{Req-1}} \implies \underbrace{\Box(\ell \geq 60 \implies 20 \cdot \int L \leq \ell)}_{\text{Req}}$$

Proof:

- Assume 'Req-1'.
- Let $L_{\mathcal{I}}$ be any interpretation of L, and $[b, e]$ an interval with $e - b \geq 60$.
- Show "$20 \cdot \int L \leq \ell$", i.e.

$$\mathcal{I}[\![20 \cdot \textstyle\int L \leq \ell]\!](V, [b,e]) = tt$$

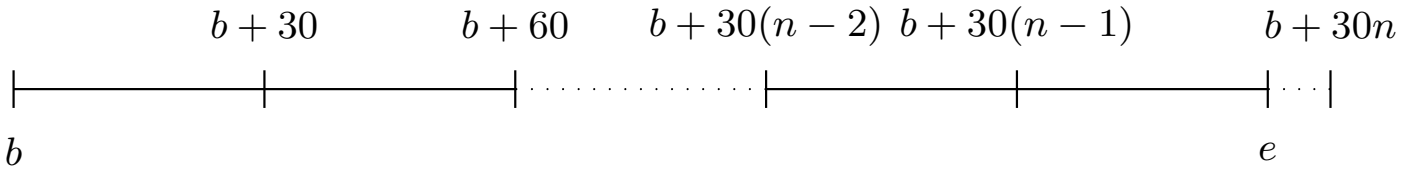
i.e.

$$20 \overset{!}{\geq} \int_b^e L_{\mathcal{I}}(t)\,dt \overset{!}{\leq} (e-b)$$

Gas Burner Revisited: Lemma 2.17

$$\models \underbrace{\square(\ell \leq 30 \implies \int L \leq 1)}_{\text{Req-1}} \implies \square(\ell \geq 60 \implies 20 \cdot \int L \leq \ell)$$

- Set $n := \lceil \frac{e-b}{30} \rceil$, i.e. $n \in \mathbb{N}$ with $n - 1 < \frac{e-b}{30} \leq n$, and split the interval



$$20 \cdot \int_b^e L_I(t)\,dt$$

$$= 20 \cdot \left(\sum_{i=0}^{n-2} \int_{b+30i}^{b+30(i+1)} L_I(t)\,dt + \int_{b+30(n-1)}^{e} L_I(t)\,dt \right)$$

$$\{\text{Req-1}\} \leq 20 \cdot \sum_{i=0}^{n-2} 1 + 20 \cdot 1$$

$$= 20 \cdot n$$

$$\{n - 1 < \tfrac{e-b}{30}\} < 20 \left(\frac{e-b}{30} + 1 \right)$$

$$= \frac{2}{3}(e-b) + 20$$

$$\{e - b \geq 60 \implies 20 \leq \tfrac{1}{3}(e-b)\} \leq e - b$$

$\{e - b \geq 60 \implies 20 \leq \frac{1}{3}(e-b)\}$

Theorem 2.18

For all state assertions P and all real numbers $r_1, r_2 \in \mathbb{R}$,

(i) $\models \int P \leq \ell$,

(ii) $\models (\int P = r_1)\,;(\int P = r_2) \implies \int P = r_1 + r_2$,

(iii) $\models \lceil \neg P \rceil \implies \int P = 0$,

(iv) $\models \lceil \rceil \implies \int P = 0$.

Gas Burner Revisited: Lemma 2.18

(i) $\models \int P \leq \ell$, (iv) $\models \lceil \rceil \implies \int P = 0$.
(ii) $\models (\int P = r_1)\,;(\int P = r_2) \implies \int P = r_1 + r_2$,
(iii) $\models \lceil \neg P \rceil \implies \int P = 0$,

Claim:

$$\models \underbrace{(\Box(\lceil L \rceil \implies \ell \leq 1)}_{\text{Des-1}} \wedge \underbrace{\Box(\lceil L \rceil\,;\lceil \neg L \rceil\,;\lceil L \rceil \implies \ell > 30))}_{\text{Des-2}} \implies \underbrace{\Box(\ell \leq 30 \implies \int L \leq 1)}_{\text{Req-1}}$$

Proof: $\ell \leq 30$

{finite variabl.} $\Rightarrow \lceil \rceil \vee \lceil L \rceil ; (\lceil \rceil \vee \lceil \neg L \rceil) \vee \lceil \neg L \rceil ; (\lceil \rceil \vee \lceil L \rceil) \vee \lceil L \rceil ; \lceil L \rceil \vee \lceil \neg L \rceil \vee \ell \leq 30 \wedge \Diamond(\lceil L \rceil ; \lceil \neg L \rceil ; \lceil L \rceil)$ } (*) } $\not\models$ Des-2

{Des-2} $\Rightarrow$ (*)

{Des-1} $\Rightarrow \lceil \rceil \vee (\ell \leq 1) ; (\lceil \rceil \vee \lceil \neg L \rceil) \vee \lceil \neg L \rceil ; (\lceil \rceil \vee \ell \leq 1) \vee \lceil \neg L \rceil ; \ell \leq 1 ; \lceil \neg L \rceil$

{(i)} $\Rightarrow \lceil \rceil \vee (\int L \leq 1) ; (\lceil \rceil \vee \lceil \neg L \rceil) \vee \lceil \neg L \rceil ; (\lceil \rceil \vee \int L \leq 1) \vee (\lceil L \rceil ; \int L \leq 1 ; \lceil \neg L \rceil$

{ii, iv} $\Rightarrow \int L = 0 \vee (\int L \leq 1) ; (\int L = 0 \vee \int L = 0) \vee (\int L = 0) ; (\int L = 0 \vee \int L \leq 1) \vee \int L \neq 0 ; \int L \leq 1 ; \int L = 0$

{iii} $\Rightarrow \int L \leq 1$ $\square$

References

References

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