Real-Time Systems

Lecture 05: Duration Calculus III

2014-05-20

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- DC Syntax and Semantics: 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
  - Correctness Proofs: Gas Burner

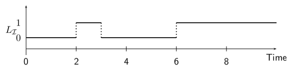
Duration Calculus Abbreviations

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



$\int \neg L = \ell \wedge \ell > 0$

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

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

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

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

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

$\mathcal{I}[\![\lceil \neg L \rceil \,;\, \lceil L \rceil]\!](\mathcal{V}, [0,3]) = tt$ ← unique chop point $m_1 = 2$

$\mathcal{I}[\![\lceil \neg L \rceil \,;\, \lceil L \rceil \,;\, \lceil \neg L \rceil]\!](\mathcal{V}, [0,6]) = tt$ $m_1 = 2, m_2 = 3$ unique

$\mathcal{I}[\![\Diamond \lceil L \rceil]\!](\mathcal{V}, [0,6]) = tt$ $m_1 = 2, m_2 = 3$ not unique, $2 \leq m_1 < m_2 \leq 3$ okay

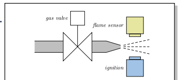
$\mathcal{I}[\![\Diamond \lceil \neg L \rceil]\!](\mathcal{V}, [0,6]) = tt$

$\mathcal{I}[\![\Diamond \lceil \neg L \rceil^2]\!](\mathcal{V}, [0,6]) = tt$ $m_1 = m_2 = 2.5$ NOT!

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

$true ; \lceil L \rceil ; true$

Duration Calculus: Looking Back



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

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

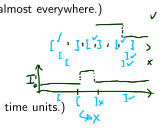
Strangest operators:

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

  (Holds in a given interval $[b, e]$ iff the gas valve is open almost everywhere.)
- **chop** — Example: $\Box((\lceil \neg I \rceil \,;\, \lceil I \rceil \,;\, \lceil \neg I \rceil) \implies \ell \geq 1)$

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

Validity vs. Satisfiability vs. Realisability

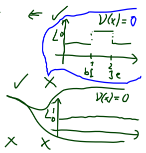
Remark 2.13. For all DC formulae F,

- 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?

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 $\qquad \forall \mathcal{V} \in \mathsf{Val} : \mathcal{I}, \mathcal{V} \models_0 F$.
- $\models_0 F$ ("F is **valid from** 0") iff $\qquad \forall$ 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.

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

Methodology: Ideal World...

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

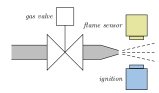
(ii) Provide the **requirement/specification** 'Spec' as a conjunction of DC formulae (over 'Obs').

(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

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

Gas Burner Revisited



(i) Choose **observables**:

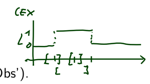
- two boolean observables G and F (i.e. Obs $= \{G, F\}$, $\mathcal{D}(G) = \mathcal{D}(F) = \{0, 1\}$)
- $G = 1$: gas valve open now (output)
- $F = 1$: have flame now (input)
- define $L := G \wedge \neg F$ (leakage)

(ii) Provide the **requirement**:

$$\text{Req} : \iff \Box(\ell \geq 60 \implies 20 \cdot \textstyle\int L \leq \ell)$$

Gas Burner Revisited

CEX



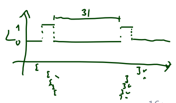
(iii) Provide a description 'Ctrl' of the **controller** in form of a DC formula (over 'Obs'). Here, firstly consider a **design**:

- Des-1 : $\iff \Box(\lceil L \rceil \implies \ell \leq 1)$ "leakage phases last at most one time unit"
- Des-2 : $\iff \Box(\lceil L \rceil \,;\, \lceil \neg L \rceil \,;\, \lceil L \rceil \implies \ell > 30)$ "non-leakage phases between two leakage phases last at least 30 time units"

(iv) Prove **correctness**:

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

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



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 : $\iff \Box(\lceil L \rceil \,;\, \lceil \neg L \rceil \,;\, \lceil L \rceil \implies \ell > 30)$

② • and we show $\models$ Des-1 ∧ Des-2 $\implies$ Req-1

(iv) Prove **correctness**:

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

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

① • We do show

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

with the simplified requirement

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

References

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