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

- \([ \bigcirc ] := \ell = 0\) (point interval)
- \([P] := \{f \mid P = \ell\} \land (\ell > 0)\) (almost everywhere)
- \([P]^t := [P] \land \ell = t\) (for time \(t\))
- \([P]^{\leq t} := [P] \land \ell \leq t\) (up to time \(t\))
- \(\bigtriangleup F := true \cdot F \cdot true\) (for some subinterval)
- \(\Box F := \neg \bigtriangleup \neg F\) (for all subintervals)
Duration Calculus: Looking Back

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

**Strangest operators:**

- **almost everywhere** — Example: \([G]\)
  (Holds in a given interval \([b, e]\) iff the gas valve is open almost everywhere.)

- **chop** — Example: \([[\neg I] ; [I] ; [\neg I]] \implies \ell \geq 1\)
  (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.)
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 \( I[F](\mathcal{V}, [b, e]) = \text{tt} \).

• \( F \) 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 \( \forall [b, e] \in \text{Intv} : \mathcal{I}, \mathcal{V}, [b, e] \models F \).

• \( F \) is called realisable iff some \( \mathcal{I} \) and \( \mathcal{V} \) realise \( F \).

• \( \mathcal{I} \models F \) ("\( \mathcal{I} \) realises \( F \)"") iff \( \forall \mathcal{V} \in \text{Val} : \mathcal{I}, \mathcal{V} \models F \).

• \( \models F \) ("\( F \) is valid"") iff \( \forall \) interpretation \( \mathcal{I} : \mathcal{I} \models F \).
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?

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

- $\ell = 2$

*\(\int\)
**Initial Values**

- \( \mathcal{I}, \mathcal{V} \models_0 F \) ("\( \mathcal{I} \) and \( \mathcal{V} \) **realise** \( F \) **from** 0") iff
  \[ \forall t \in \text{Time} : \mathcal{I}, \mathcal{V}, [0, t] \models F. \]

- \( F \) 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
  \[ \forall \mathcal{V} \in \text{Val} : \mathcal{I}, \mathcal{V} \models_0 F. \]

- \( \models_0 F \) ("\( F \) is **valid** from 0") iff
  \[ \forall \text{interpretation} \mathcal{I} : \mathcal{I} \models_0 F. \]

**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.
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

\[
\models_0 Ctrl \implies Spec.
\]
(i) Choose **observables**:
- two boolean observables \( G \) and \( F \)
  (i.e. \( \text{Obs} = \{G, F\}, D(G) = D(F) = \{0, 1\} \))
- \( G = 1 \): gas valve open
- \( F = 1 \): have flame
- define \( L := G \land \neg F \) (leakage)

(ii) Provide the **requirement**:
\[
\text{Req} : \iff \Box (\ell \geq 60 \implies 20 \cdot \int L \leq \ell)
\]

(iii) Provide a description 'Ctrl' of the **controller** in form of a DC formula (over 'Obs'). Here, firstly consider a **design**:
- \( \text{Des-1} : \iff \Box ([L] \implies \ell \leq 1) \) "leakage phases last at most one time unit"
- \( \text{Des-2} : \iff \Box ([L] ; [\neg L] ; [L] \implies \ell > 30) \) "non-leakage phases between two leakage phases last at least 30 time units"

(iv) Prove **correctness**:
- We want (or do we want \( \models_{0...} ? \)):
\[
\models (\text{Des-1} \land \text{Des-2} \implies \text{Req}) \quad \text{(Thm. 2.16)}
\]
(iii) Provide a description 'Ctrl' of the controller in form of a DC formula (over 'Obs').

Here, firstly consider a design:

- Des-1: $\square([L] \implies \ell \leq 1)$
- Des-2: $\square([L] \implies [\neg L] \implies \ell \geq 30)$

(iv) Prove correctness:

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

\[
\models (\text{Des-1} \land \text{Des-2} \implies \text{Req}) \quad (\text{Thm. 2.16})
\]

- We do show

\[
\models \text{Req-1} \implies \text{Req} \quad (\text{Lem. 2.17})
\]

with the simplified requirement

\[
\text{Req-1} := \square(\ell \leq 30 \implies \int L \leq 1)
\]