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: Overview

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

(i) Symbols: \(f, g, \text{true}, \text{false}, =, <, >, \leq, \geq, x, y, z, X, Y, Z, d\)

(ii) State Assertions: \(P::=0 | 1 | X = d | \neg P | 1 | P_1 \land P_2\)

(iii) Terms: \(\theta ::= x | \ell | \int P | f(\theta_1, \ldots, \theta_n)\)

(iv) Formulae: \(F ::= p(\theta_1, \ldots, \theta_n) | \neg F_1 | F_1 \land F_2 | \forall x \cdot F_1 | F_1 ; F_2\)

(v) Abbreviations: \([\quad], \lceil \quad \rceil, \lceil \quad \rceil_t, \lceil \quad \rceil_{\leq t}, \lozenge, \square\)

Formulae: Remarks

Remark 2.10.
\[
\text{[Rigid and chop-free] Let } F \text{ be a duration formula, } I \text{ an interpretation, } V \text{ a valuation, and } [b,e] \in \mathbb{Int} v.

• If } F \text{ is rigid, then } \forall [b',e'] \in \mathbb{Int} v: I/C_2 F(C_3(V, [b,e])) = I/C_2 F(C_3(V, [b',e'])).

• If } F \text{ is chop-free or } \theta \text{ is rigid, then in the calculation of the semantics of } F, \text{ every occurrence of } \theta \text{ denotes the same value.}

Substitution Lemma

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

I/C_2 F[x:=\theta](V, [b,e]) = I/C_2 F[V[x:=d], [b,e]).
\]
Abbreviations:

Duration Calculus: Overview

Symbols:

State Assertions:

Duration Calculus: Axioms

Example:

Strangest operators:

(true):=

Examples:

Duration Calculus: Axioms
Validity vs. Satisfiability vs. Realisability

For all interpretations $V$, the interval $\langle 0, L \rangle$ is realisable if and only if some valuation $V^*$ realises $I$, and DC formulae $V$ and $F$ are defined.

Validity of $I$ is not in general decidable, but not vice versa. However, if $V$ is realisable then $I$ is satisfiable, but not vice versa. If a valuation $V$ is realisable then $I$ is valid from $F$.

Initial intervals $\langle 0, \ell \rangle$ are valid from $F$ if and only if some valuation $V$ realises $I$, and DC formulae $V$ and $F$ are defined. Initial intervals $\langle 0, \ell \rangle$ are not satisfiable, but not vice versa. If a valuation $V$ is realisable then $I$ is valid from $F$.

Initial intervals $\langle 0, \ell \rangle$ are realisable if and only if some valuation $V$ realises $I$, and DC formulae $V$ and $F$ are defined. Initial intervals $\langle 0, \ell \rangle$ are satisfiable, but not vice versa. If a valuation $V$ is realisable then $I$ is valid from $F$.

Validity, Satisfiability, Realisability
\[ I \cdot e(t) = V_\ell \cdot \int_{t_0}^{t+\Delta t} I \leq P \Rightarrow \int_{t_0}^{t+\Delta t} P \leq P \int_{t_0}^{t+\Delta t} = P \cdot \int_{t_0}^{t+\Delta t} \]

\[ \text{Let } \Rightarrow \int_{t_0}^{t+\Delta t} = (ii) \]

\[ \text{For all states } \Rightarrow \int_{t_0}^{t+\Delta t} \leq 30 \]

\[ \text{Theorem 2.16} \]

\[ \text{GasBurnerRevisited: Lemma 2.17} \]

\[ (i) \text{Choose a collection of gas valves and flamesensors} \]

\[ (ii) \text{Provide a description } \text{Contral} \text{ (wrt. 'Spec') iff } \]

\[ \text{Save transitions DC formulas at hand} \]

\[ \text{Methodology: IdealWorld...} \]
GasBurnerRevisited: Lemma 2.18

Claim:

(i) \(|= \int_\mathcal{P} \leq \ell\),

(iv) \(|= \lceil\cdot\rceil = \Rightarrow \int_\mathcal{P} = 0\).

(ii) \(|= (\int_\mathcal{P} = r_1) \land (\int_\mathcal{P} = r_2) = \Rightarrow \int_\mathcal{P} = r_1 + r_2\),

(iii) \(|= \lceil\neg \mathcal{P}\rceil = \Rightarrow \int_\mathcal{P} = 0\).

Proof:

\[\square (\lceil \mathcal{L} \rceil = \Rightarrow \ell \leq 1) \land \square (\lceil \neg \mathcal{L} \rceil \land \lceil \mathcal{L} \rceil = \Rightarrow \ell > 30) = \Rightarrow \square (\ell \leq 30 = \Rightarrow \int_\mathcal{L} \leq 1)\]

References