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

(ii) State Assertions: $P ::= 0 | 1 | X = d | \neg P | 1 | P \land P | 2$

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

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

(v) Abbreviations: $\lceil \cdot \rceil,$ $\lceil P \rceil,$ $\lceil P \rceil \leq t,$ $\Box F,$ $\Diamond F$

Formulae: Remarks

Remark 2.10.

[rigid and chop-free]

- Let $F$ be a duration formula, $I$ an interpretation, $V$ a valuation, and $[b,e] \in \text{Intv}$.
  - If $F$ is rigid, then $\forall [b',e'] \in \text{Intv}$: $I/\llbracket F \rrbracket(V,[b,e]) = I/\llbracket F \rrbracket(V,[b',e'])$.  
  - If $F$ is chop-free or $\theta$ is rigid, then in the calculation of the semantics of $F$, every occurrence of $\theta$ denotes the same value.

Substitution Lemma

Lemma 2.11.

[Substitution]

Consider a formula $F$, a global variable $x$, and a term $\theta$ such that $F$ is chop-free or $\theta$ is rigid.

Then for all interpretations $I$, valuations $V$, and intervals $[b,e]$, $I/\llbracket F[x:=\theta] \rrbracket(V,[b,e]) = I/\llbracket F \rrbracket(V[x:=d],[b,e])$, where $d = I/\llbracket \theta \rrbracket(V,[b,e])$. 

$\ell = x \Rightarrow \ell = 2 \cdot x$, $\theta := \ell$.
Speciation and Convergence-Based Compatibility of Real-Time Systems with DC

Remark 2.13. Validity, Satisfiability, Realisability

Validity vs. Satisfiability vs. Realisability

Examples: Valid? Realisable? Satisfiable?
Methodology: IdealWorld

(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 inform of a DC formula (over 'Obs').

(iv) We say 'Ctrl' is correct (wrt. 'Spec') if \(|\nabla = 0\) \(\Rightarrow\) 'Spec'.

GasBurnerRevisited

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

(ii) Provide the requirement: \(\text{Req} := \square (\lceil L \rceil \geq 60 \Rightarrow 20 \cdot \int L \leq \ell)\)

(iii) Provide a description 'Ctrl' of the controller inform of a DC formula (over 'Obs').
Here, firstly consider a design:
- \(\text{Des-1} := \square (\lceil L \rceil = \Rightarrow \ell \leq 1)\)
- \(\text{Des-2} := \square (\lceil L \rceil; \lceil \neg L \rceil; \lceil L \rceil = \Rightarrow \ell > 30)\)

(iv) Prove correctness:
- We want (ordowewant \(|\nabla = 0\)...?): \(|\nabla = (\text{Des-1} \land \text{Des-2}) = \Rightarrow \text{Req}\) (Thm. 2.16)
- We show \(|\nabla = \text{Req-1} = \Rightarrow \text{Req}\) (Lem. 2.17) with the simplified requirement \(\text{Req-1} := \square (\ell \leq 30 = \Rightarrow \int L \leq 1)\),
- and we show \(|\nabla = (\text{Des-1} \land \text{Des-2}) = \Rightarrow \text{Req-1}\) (Lem. 2.19).

References