An Algebraic Semantics for Duration Calculus

Peter Höfner

Institute of Computer Science, University of Augsburg

> If you are faced by a difficulty or a controversy in science,
> an ounce of algebra is worth a ton of verbal argument.
>
> *J.B.S. Haldane*

1 Introduction

Reactive systems interact with their environment on an on-going, principally never-ending basis. A special class of reactive systems are *real-time systems*

Effective tool for modelling, design and analysis of technological systems

Fields of application:

- (air-)traffic controls / traffic management
- chemical and biological processes
- automated manufacturing
- standard example: leaking gas burner

Duration Calculus

- logic for specifying all kinds of requirements of reactive and, especially, real-time systems
- include functional requirements
- include dependability requirements as well
- support the verification and the design of reactive systems
- developed by Zhou, Hoare and Ravn in 1991
- many extensions, e.g. by He and by Zhou (Neighbourhood Logic)

2 Interval-Based Model for Duration Calculus

Example – *leaking gas burner*:

- heating or idling
- usually, no gas is flowing while it is idling
- gas can leak
  (e.g. when a flame failure appears)

safety requirement:

"For any observation interval that is shorter than 30 seconds, the accumulation of leakage must be less than 4 seconds."

$$\forall [a,b] \in \mathrm{Int}: \; b - a \leq 30 \Rightarrow \; leak([a,b]) \leq 4 \; ,$$

where

$$\begin{aligned} leak : \mathrm{Int} &\rightarrow \mathbb{R} \cup \{\infty\} \\ [a,b] &\mapsto \int_a^b \chi(t)\, dt \end{aligned}$$

Int: set of *intervals* $[a,b] \stackrel{\text{def}}{=} \{x : x \in M,\; a \leq x \leq b\}$

$\chi(t)$: characteristic function

further operations on Int and $\wp(\mathrm{Int})$

- composition of intervals

$$[a,b]\,;[c,d] \stackrel{\text{def}}{=} \begin{cases} [a,d] & \text{if } b=c \\ \text{undefined} & \text{otherwise}\ . \end{cases}$$

- composition of sets of intervals $U, V \in \wp(\mathrm{Int})$

$$U\,;V \stackrel{\text{def}}{=} \{u\,;v \;:\; u \in U,\, v \in V,\, u\,;v \text{ defined}\},$$

$$\mathrm{INT} \stackrel{\text{def}}{=} (\wp(\mathrm{Int}), \cup, \emptyset, ;, \mathbb{1}_{\mathrm{Int}})$$

where $\mathbb{1}_{\mathrm{Int}} \stackrel{\text{def}}{=} \{[a,a] \;:\; a \in M\}$ is the identity element w.r.t. ;

3 Algebraic Structures

Definition 3.1 *semiring* $(K, +, \cdot, 0, 1)$, e.g., $(\wp(\mathrm{Int}), \cup, \emptyset, ;, \mathbb{1}_{\mathrm{Int}})$:

- $(K, +, 0)$ commutative monoid
  (closed, associative, 0 neutral element)
- $(K, \cdot, 1)$ monoid
- multiplication is distributive:

$$
\begin{aligned}
(a+b)\cdot c &= a\cdot c + b\cdot c \\
a\cdot(b+c) &= a\cdot b + a\cdot c
\end{aligned}
$$

- 0 is an annihilator:

$$0\cdot a = 0 = a\cdot 0$$

a semiring is called

- *idempotent* iff $a + a = a$
- *bounded* if there is a greatest element $\top$

properties of idempotent semirings:

- *natural order*: $a \leq b \overset{\text{def}}{\Leftrightarrow} a + b = b$
- $+$ and $\cdot$ are isotone
- 0 is least element w.r.t. the natural order

Definition 3.2 *quantale* (also: *standard Kleene algebra*)

- idempotent (and bounded) semiring
- complete lattice under the natural order
- $\cdot$ universally disjunctive in both arguments

Boolean quantale iff the underlying lattice is a completely distributive Boolean algebra add finite iteration to an idempotent semiring

Definition 3.3 *Kleene algebra* $(S, {}^*)$

- idempotent semiring S
- * satisfies *unfold* and *induction* axioms
  (similar to regular algebra)

every quantale can be extended to a Kleene algebra

examples

- REL: algebra of binary relations over a set under relational composition
- LAN: algebra of formal languages under concatenation
- PAT: the algebra of path-sets of a given graph under path fusion
- INT: algebra of intervals

4 Modal Operators

aim: simplify calculations, avoid operators like $\forall, \exists$

pointwise representation in INT

- $i \in U/V \Leftrightarrow \forall v \in V : i\,;v \in U$ (provided $i\,;v$ is defined).
- $i \in U\lfloor V \Leftrightarrow \exists\, v \in V : i\,;v \in U$

Definition 4.1 *right residual* a/b and *left residual* $a\backslash b$

$$x \le a/b \stackrel{\text{def}}{\Leftrightarrow} x \cdot b \le a \quad \text{and} \quad x \le a\backslash b \stackrel{\text{def}}{\Leftrightarrow} a \cdot x \le b \;.$$

right detachment $a\lfloor b$ and *left detachment* $a\rfloor b$

$$a\lfloor b \stackrel{\text{def}}{=} \overline{\overline{a}/b} \quad \text{and} \quad a\rfloor b \stackrel{\text{def}}{=} \overline{a\backslash\overline{b}} \;.$$

- in Boolean quantales the existence guaranteed
- related to division
- usual modal properties

$a\lfloor b$ is the inverse image of a under $\cdot b$ $\Rightarrow$ forward modal operator
Equivalently, $a\rfloor b$ is a backward modal operator.

Setting modal operators by

$$\langle a \rangle b \stackrel{\text{def}}{=} a \rfloor a \lfloor b \ , \qquad [a]b \stackrel{\text{def}}{=} \overline{\langle a \rangle \overline{b}} = a \backslash b / a$$

and

$$\langle a \rangle_+ b \stackrel{\text{def}}{=} a \cdot b \cdot a \ , \qquad [a]_+ b \stackrel{\text{def}}{=} \overline{\langle a \rangle_+ \overline{b}}$$

- x contains in $\langle a \rangle b$ iff b holds for at least one extension of x in a ($\exists$)
- x contains in $[a]b$ iff b holds for all extensions of x in a ($\forall$)

5 Duration Calculus

safety requirement:

"For any observation interval that is shorter than 30 seconds, the accumulation of leakage must be less than 4 seconds."

$$\forall [a,b] \in \mathsf{Int} : \; b - a \leq 30 \; \Rightarrow \; \mathit{leak}([a,b]) \leq 4$$

using the quantale INT:

$$\texttt{gas\_req} \; = \; [\top]_{+} \overline{s}$$

where $s = \{[a,b] \; : \; b - a \leq 30, \; \mathit{leak}([a,b]) > 4\}$

possible and safe design of the gas burner problem [vonKarger00]

$$\mathtt{gas\_design} = t^*,$$

where $t = \{[a, b] \ : \ b - a = 30, \mathit{leak}([a, b]) < 2\}$

`gas_design` has the advantage over `gas_req` to include only the intervals with duration of exactly 30 seconds and can be controlled by a looping program

correctness and safety of the chosen design:

Lemma 5.1 `gas_design` is a subset of `gas_req`

the proof is by a generalisation of von Karger's engineer's induction

6 Conclusion and Outlook

- duration calculus

  logic for specifying all kinds of requirements of reactive and, especially, real-time systems
- algebraic approach
  - simple expressions, e.g., $\lceil \top \rceil_+ \overline{s}$
  - easy to handle and to calculate with
  - consider only few axioms of Kleene algebra
  - make use of all the knowledge about these algebraic structures
- infinite iteration

  Kleene algebras can be extended by an ω-operator

  ω-algebra

- infinite elements

  left semirings, *left quantales*, *left Kleene algebra* and *left ω-algebra*

  (relax axioms and abandon right-strictness $a \cdot 0 = 0$)

  [Möller04]

- trajectory-based model [HöfnerMöller05]

- ITL-extending logics

  – propositional calculus [Venema91]

  – Neighbourhood Logic [ZhouHansen98]