Towards an Algebra of Hybrid Systems

Peter Höfner and Bernhard Möller

Institut für Informatik, Universität Augsburg

1 Introduction

Basic Definition

Hybrid systems are heterogeneous systems characterised by the interaction of discrete and continuous dynamics.

Effective tool for modelling, design and analysis of technological systems.
Fields of application:

- (air-)traffic controls
- car-locating systems
- chemical and biological processes
- automated manufacturing

2 Trajectory-Based Model

Aim: algebraic characterisation of hybrid systems

- approach by Left Semirings
- usage of trajectories as carrier set
- trajectories are pairs of a duration of a time-interval and a function
- more handy characterisation of hybrid systems
- based on Sintzoff, Henzinger, Davoren, Lynch

trajectories:

Let V be a set of values and D a set of *durations* (e.g. $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, ...)

- $(D, +, 0)$ commutative monoid
- $+$ cancellative
- linear order on D: $x \le y \overset{\text{def}}{\Leftrightarrow} \exists\, z \,.\, x + z = y$
  - 0 least element
  - 0 indivisible, e.g. $x + y = 0 \Leftrightarrow x = y = 0$
- possibility of element $\infty \in D$
  - greatest element
  - not cancellative

For $d \in D$ we define the *interval* $\mathsf{tim}\, d$ of admissible times as

$$\mathsf{tim}\, d \stackrel{\text{def}}{=} \begin{cases} [0, d] \text{ if } d \neq \infty \\ [0, d[\text{ otherwise} \end{cases}$$

Definition 2.1 A *trajectory* t is a pair (d, g), where $d \in D$ and $g : \mathsf{tim}\, d \to V$. Then d is the *duration* of the trajectory, the image of $\mathsf{tim}\, d$ under g is its *range* $\mathsf{ran}\ (d, g)$

- we write $(d, g)(0)$ for $g(0)$
- the set of all trajectories is denoted TRA

composition of trajectories:

$$(d_1, g_1)\cdot(d_2, g_2) \stackrel{\text{def}}{=} \begin{cases} (d_1 + d_2, g) & \text{if } d_1 \neq \infty \wedge g_1(d_1) = g_2(0) \\ (d_1, g_1) & \text{if } d_1 = \infty \\ \text{undefined} & \text{otherwise} \end{cases}$$

with $g(x) = g_1(x)$ for all $x \in [0, d_1]$ and $g(x + d_1) = g_2(x)$ for all $x \in \mathsf{tim}\, d_2$.

case of a zero-length trajectory

- $(0, g_1) \cdot (d_2, g_2) = (d_2, g_2)$ if $g_1(0) = g_2(0)$
  otherwise undefined
- $(d_2, g_2) \cdot (0, g_1) = (d_2, g_2)$ if $d_2 \neq \infty$ and $g_2(d_2) = g_1(0)$

Definition 2.2 A *process* is a set of trajectories.

$$\mathsf{inf}\, A \stackrel{\mathsf{def}}{=} \{(d, g) \in A \mid d = \infty\} \qquad \mathsf{fin}\, A \stackrel{\mathsf{def}}{=} A - \mathsf{inf}\, A$$

Composition is lifted

$$A \cdot B \stackrel{\mathsf{def}}{=} \mathsf{inf}\, A \cup \{a \cdot b \mid a \in \mathsf{fin}\, A, b \in B\}$$

The set I of all zero-length trajectories is the neutral element.

restricted form of composition (chop)

$$A \frown B \stackrel{\text{def}}{=} (\mathsf{fin}\, A) \cdot B \ ,$$

- yields only trajectories that actually reach the second process
- implies $A \cdot B = \mathsf{inf}\, A \cup A \frown B$

We now pass to a more abstract description.

3 Left Semirings and Modalities

Definition 3.1 *left* or *lazy semiring* $(S, +, \cdot, 0, 1)$:

- $(S, +, 0)$ commutative monoid
- $(S, \cdot, 1)$ monoid
- multiplication is left-distributive:

$$(a + b) \cdot c \;=\; a \cdot c + b \cdot c$$

- 0 is a left annihilator:

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

(a semiring without strictness and right-distributivity)

Definition 3.2 *idempotent* left semiring:

- $a + a = a$
- composition $\cdot$ is right-isotone: $b \le c \Rightarrow a \cdot b \le a \cdot c$

  where $a \le b \overset{\text{def}}{\Leftrightarrow} a + b = b$
- *bounded* if there is a greatest element $\top$

left-isotonicity of $\cdot$ follows from its left-distributivity

moreover, 0 is the least element

Definition 3.3 *left quantale (left standard Kleene algebra)*

$(S, +, \cdot, 0, 1)$:

- $(S, +, \cdot, 0, 1)$ left semiring
- S complete lattice under the natural order
- $\cdot$ is universally disjunctive in left argument

Definition 3.4 *left Boolean quantale*

- completely distributive Boolean algebra as underlying lattice examples:

- algebra of binary relations REL
- algebra of formal languages LAN
- processes PRO $\stackrel{\text{def}}{=} (\mathcal{P}(\mathrm{TRA}), \cup, \emptyset, \cdot, \mathrm{I})$

Definition 3.5 *left test semiring* $(S, \mathsf{test}(S))$:

- S idempotent left semiring
- $\mathsf{test}(S) \subseteq [0,1]$ Boolean subalgebra of the interval $[0,1]$ of S such that $0, 1 \in \mathsf{test}(S)$
- in $\mathsf{test}(S) : p + q \;=\; p \sqcup q,\; p \cdot q \;=\; p \sqcap q$
- $\neg$ denotes complementation in $\mathsf{test}(S)$

Analogously for quantales.

Consequence: If $a \sqcap b$ exists then

$$p \cdot (a \sqcap b) \;=\; p \cdot a \;\sqcap\; b \;=\; p \cdot a \;\sqcap\; p \cdot b \;.$$

Definition 3.6 *left domain semiring* $(S, \ulcorner)$

- S left test semiring
- *domain* operation $\ulcorner\colon S \to \mathsf{test}(S)$

$$a \leq \ulcorner a \cdot a \;, \qquad \ulcorner(p \cdot a) \leq p \;, \qquad \ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b) \;.$$

$(a, b \in S, p \in \mathsf{test}(S))$

same axioms as domain semirings together with their relevant consequences [Möller04].

REL, LAN, PRO can be extended to left domain semirings

in PRO:

- $test(\mathrm{PRO}) = \{(0, g) \mid g(0) = v, v \in V\}$ (zero-length processes)
- $\ulcorner A = \{(0, g(0)) \mid (d, g) \in A\}$ (starting points)
- $P \in \mathrm{test}(\mathrm{PRO}) \;\Rightarrow\; P \sqcap A \cdot B = (P \sqcap A) \cdot (P \sqcap B)$

Moreover, $\cdot$ in PRO is even right-distributive.

Definition 3.7 *left Kleene algebra* $(S, {}^*)$

- S idempotent semiring
- * operation

$$1 + a \cdot a^* \leq a^* \;, \qquad b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c \;.$$

Definition 3.8 *left ω algebra* $(S, {}^\omega)$

- S left Kleene algebra
- ${}^\omega$ operation

$$a^\omega = a \cdot a^\omega \;, \qquad c \leq a \cdot c + b \Rightarrow c \leq a^\omega + a^* \cdot b.$$

4 Temporal Operators

Generalization of the quantifier-like operators by Sintzoff of type $\mathsf{PRO} \longrightarrow (\mathsf{PRO} \longrightarrow \mathsf{test}(\mathsf{PRO}))$
(e.g. $\mathsf{E}'A\,.\,W \stackrel{\text{def}}{=} \ulcorner(A \cap W)$)

$$
\begin{array}{rcccl}
t \in \mathsf{E}A \;.\; W & = & \exists\, u \in A : t \cdot u \in W & = & W\lfloor A, \\
t \in \mathsf{A}A \;.\; W & = & \forall\, u \in A : t \cdot u \in W & = & W/A, \\
\mathsf{AE}A \;.\; W & = & (\mathsf{E}A\,.\,W) \sqcap (\mathsf{A}A\,.\,W), & &
\end{array}
$$

where $x \leq b/a \stackrel{\text{def}}{\Leftrightarrow} x \cdot a \leq b$ is the left residual and $b\lfloor a \stackrel{\text{def}}{=} \overline{\overline{b}/a}$ is the right detachment.

Lemma 4.1 In a Boolean test quantale

$$\ulcorner(\mathsf{b} \sqcap w) = w\lfloor \mathsf{b} \sqcap 1 = \mathsf{b}\lfloor w \sqcap 1 \ .$$

Lemma 4.2 Setting $\langle a \rangle b \stackrel{\text{def}}{=} \mathsf{E} a \,.\, b$ and $[a] b \stackrel{\text{def}}{=} \mathsf{A} a \,.\, b$ makes these operators into proper modal operators:

1. $\langle a \rangle$ is universally disjunctive and $[a]$ is universally conjunctive.
2. $\langle a \cdot b \rangle c = \langle a \rangle (\langle b \rangle c)$ and $[a \cdot b] c = [a]([b] c)$.
3. If $\cdot$ is positively disjunctive in its right argument, then $\langle \_ \rangle$ is positively disjunctive and $[\_]$ is positively antidisjunctive.

($\langle \_ \rangle$ and $[\_]$ describe the possible and the guaranteed reachability)

5 Range-Restriction Operators

in PRO:

- restrict the range $\mathsf{ran}\ A \stackrel{\text{def}}{=} \bigcup_{t \in A} \mathsf{ran}\ t$
- $P \in \mathsf{test}(\mathrm{PRO})$ is isomorphic to a subset $S \subseteq V$
- $\Diamond P \stackrel{\text{def}}{=} \mathsf{F} \cdot P \cdot \top$

  set of all trajectories whose range has one point in P,

  i.e., $\Diamond P = \{(d, g) \in \mathrm{TRA} \mid \exists\, x \in \mathsf{tim}\, d : \mathsf{ran}\ (0, g(x)) \subseteq P\}$
- $\Box P \stackrel{\text{def}}{=} \overline{\Diamond \neg P}$

  set of all trajectories whose range remains fully in P,

  i.e., $\Box P = \{t \in \mathrm{TRA} \mid \mathsf{ran}\ t \subseteq P\}$

where $\top \stackrel{\text{def}}{=} \mathrm{TRA}$ and $\mathsf{F} \stackrel{\text{def}}{=} \mathsf{fin}\,(\mathrm{TRA})$

Assume a Boolean left test quantale S and $\Diamond p \stackrel{\text{def}}{=} \mathsf{F} \cdot p \cdot \top$, $\Box p \stackrel{\text{def}}{=} \overline{\Diamond \neg p}$, $\mathsf{F} \stackrel{\text{def}}{=} \mathsf{fin}\, \top$.

Lemma 5.1 If S is right-distributive then for all $a, b \in S$ and $p \in \mathsf{test}(S)$,

1. $\Box p \sqcap a \cdot b = (\Box p \sqcap a) \cdot (\Box p \sqcap b)$
2. $\Diamond p \sqcap a \cdot b = (\Diamond p \sqcap a) \cdot b + \mathsf{fin}\, a \cdot (\Diamond p \sqcap b)$
3. $(\Box p) \cdot (\Box p) = \Box p$

Lemma 5.2 Assume a right-distributive left test quantale S and $p \in \mathrm{test}(S)$. The following three properties are equivalent:

1. $p \leq \Box p$
2. $\forall\ a, b \in S\ .\ p \sqcap\ a \cdot b\ =\ (p \sqcap a) \cdot (p \sqcap b)$
3. $p \leq \overline{\overline{1} \cdot \overline{1}}$

Lemma 5.3 Assume a right-distributive left test quantale S and $\mathrm{p} \in \mathsf{test}(S)$.

1. $\Box \mathrm{p} \;=\; \mathrm{p} \cdot \Box \mathrm{p}$
2. If additionally $\mathrm{p} \leq \Box \mathrm{p}$ then $\ulcorner(\Box \mathrm{p}) = \mathrm{p}$

6 Game-theoretic approach

- a *game* consists of one or more *players*
- a *move* is an action of a player
- various kinds of games

disjoint games with finite move duration

A *game round* is $(S_1 \cdot S_2 \cdots S_n)$ and

$(S_1 \cdot S_2 \cdot \cdots \cdot S_n)^*$	describes a finite game
$(S_1 \cdot S_2 \cdot \cdots \cdot S_n)^\omega$	describes an infinite game

why a game-theoretic approach?

- hybrid and reactive systems deal with interaction between dynamics
- the controlling and the controlled part are the proponent and the opponent
- in PRO sets of moves are just processes
- the controller has to counteract all possible failures, has to force the opponent into a “losing“ position

- game round w.r.t. winning position [DesharnaisMöllerStruth]

$$\langle a \rangle \cdot [b]$$

- traces of finite or infinite games

$$(\langle a \rangle \cdot [b])^* \text{ or } (\langle a \rangle \cdot [b])^\omega$$

- sets of winning / losing positions can be calculated by fixpoint iteration [Backhouse]

7 Outlook

- further aim: suitable specialisation of the general results to form new, more convenient algebraic calculi, both for safety and liveness proofs
- hope:game-theoretic approach one can obtain improved control of hybrid systems
- incorporation of hybrid(I/O) automata
- semantical models of Davoren, Lynch can be made into left domain semirings