Towards an Algebra of Hybrid Systems

Peter Höfner and Bernhard Möller

Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany
{hoefner,moeller}@informatik.uni-augsburg.de

Abstract. We present a trajectory-based model for describing hybrid systems. For this we use left quantales and left semirings, thus providing a new application for these algebraic structures. Furthermore, we sketch a connection between game theory and hybrid systems.

1 Introduction

Hybrid systems are heterogeneous systems characterised by the interaction of discrete and continuous dynamics. They are an effective tool for modelling, design and analysis of a large number of technical systems. Such models are used for example in (air-)traffic controls, car-locating systems, chemical and biological processes and automated manufacturing.

This paper is based on work about hybrid systems by Sintzoff [16], Davoren/Nerode [4], Henzinger [7] and Lynch et al. [13]. In the latter two cases, the authors present two different ways to encode hybrid systems in a kind of finite state machines. These descriptions are very unhandy in calculations concerning liveness and safety properties.

The paper shows how a number of concepts can be recast and thus be made more workable in the setting of (left) semirings and (lazy) Kleene algebras [5, 15] and other algebras (e.g [2, 11]), thus providing an interesting application for them. Furthermore, we show how to express and calculate properties of hybrid systems and, more generally, of Boolean left test quantales, using some temporal operators. Finally, we sketch a connection to game theory to show how to adapt results from that area (see e.g. [1]) to an algebra of hybrid systems.

2 Trajectory-Based Model

We motivate the coming definitions by an example.

Running Example (Temperature Control)
The hybrid automaton of Figure 1, adapted from [7], models a thermostat. The variable x represents the temperature. Initially, it is equal to 20 degrees and the heater is off (control mode *Off*). The temperature falls according to the flow condition $\dot{x} = -0.1x$. If the jump condition $x < 19$ is reached, the heater may start. The invariant condition $x \geq 18$ ensures that the heater will start at the latest when the temperature is equal to 18 degrees. In control mode

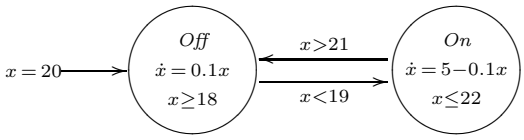

Fig. 1. Thermostat automaton

On, the temperature rises according to the flow condition $\dot{x} = 5 - 0.1x$. If the temperature reaches the second jump condition, the heater is switched off and the procedure starts again (with another initial value). □

For modelling this kind of system, we use trajectories (cf. e.g. [16]) that reflect the variation of the values of the variables over time. Let V be a set of *values* and D a set of *durations* (e.g. $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, ...). We assume a cancellative addition $+$ on D and an element $0 \in D$ such that $(D, +, 0)$ is a commutative monoid and the relation $x \leq y \stackrel{\text{def}}{\Leftrightarrow} \exists\, z \,.\, x + z = y$ is a linear order on D. Then 0 is the least element and $+$ is isotone w.r.t. $\leq$. Moreover, 0 is indivisible, i.e., $x + y = 0 \;\Leftrightarrow\; x = y = 0$. D may include the special value ∞. If so, ∞ is required to be an annihilator w.r.t. $+$ and hence the greatest element of D (and cancellativity of $+$ is restricted to elements in $D - \{\infty\}$). For $d \in D$ we define the interval $\mathsf{tim}\, d$ of admissible times as

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

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* $\mathsf{ran}\,(d, g)$. The set of all trajectories is denoted by TRA.

We define composition of trajectories (d_1, g_1) and (d_2, g_2) as

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

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

For a zero-length trajectory $(0, g_1)$ we have $(0, g_1) \cdot (d_2, g_2) = (d_2, g_2)$ if $g_1(0) = g_2(0)$; otherwise the composition is undefined. Likewise, $(d_2, g_2) \cdot (0, g_1) = (d_2, g_2)$ if $g_1(0) = g_2(d_2)$ or $d_2 = \infty$. For a value $v \in V$, let $\underline{v} \stackrel{\text{def}}{=} (0, g)$ with $g(0) = v$ be the corresponding zero-length trajectory.

A *process* is a set of trajectories, consisting of possible behaviours of a hybrid system. The finite and infinite parts of a process A are defined as

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

Composition is lifted to processes as follows:

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

The set I of all zero-length trajectories is the neutral element. A restricted form of composition, the *chop* $A^\frown B$, yields only trajectories that, after a finite trajectory of A, actually enter the second process. It is defined as $A^\frown B \stackrel{\text{def}}{=} (\mathsf{fin}\, A) \cdot B$, which implies $A \cdot B = \mathsf{inf}\, A \cup A^\frown B$.

Running Example To use trajectories, we first set $V = D = \mathbb{R}$. Now we define two processes, one for each control mode:

$$A_{\text{Off}} \stackrel{\text{def}}{=} \{(d, g) \,|\, d \in D,\, \dot{g}(t) = 0.1t\}\,,$$
$$A_{\text{On}} \stackrel{\text{def}}{=} \{(d, g) \,|\, d \in D,\, \dot{g}(t) = 5 - 0.1t\}\,.$$

A_{Off} models all possible behaviours when the heater is off, whereas A_{On} describes the thermostat when the heater is on. The initial state is $R_{20} \stackrel{\text{def}}{=} \{\underline{20}\}$ $(= \{(0, g) \,|\, g(0) = 20\})$. Hence, we can formalise the starting sequence of the thermostat described above as

$$R_{20} \cdot A_{\text{Off}} \cdot A_{\text{On}}\,.$$

Since we want to describe the whole behaviour of the thermostat, we need the possibility for iteration. Let * be an operator for finite iteration (we will show the existence of * in Section 3). Then we can describe the system as

$$R_{20} \cdot (A_{\text{Off}} \cdot A_{\text{On}})^*\,.$$

In this way, the automaton is replaced by a corresponding regular expression. In Section 4 we show how to model jump and invariant conditions by restricting the ranges of trajectories. □

3 Left Semirings and Domain

Now, let's have a closer look at the algebraic structure of the trajectory-based model.

A *left semiring* is a quintuple $(S, +, 0, \cdot, 1)$ such that $(S, +, 0)$ is a commutative monoid and $(S, \cdot, 1)$ is a monoid such that $\cdot$ is left-distributive over $+$ and *left-strict*, i.e., $0 \cdot a = 0$. The left semiring is *idempotent* if $+$ is idempotent and $\cdot$ is right-isotone, i.e., $b \leq c \Rightarrow a \cdot b \leq a \cdot c$, where the *natural order* $\leq$ on S is given by $a \leq b \stackrel{\text{def}}{\Leftrightarrow} a + b = b$. Left-isotony of $\cdot$ follows from its left-distributivity. Moreover, 0 is the $\leq$-least element. A *semiring* is a left semiring in which $\cdot$ is also right-distributive and right-strict.

A left idempotent semiring S is called a *left quantale* if S is a complete lattice under the natural order and $\cdot$ is universally disjunctive in its left argument. Following [3], one might also call a left quantale a *left standard Kleene algebra*. A left quantale is *Boolean* if its underlying lattice is a completely distributive Boolean algebra.

An important left semiring (that is even a semiring and a left quantale) is REL, the algebra of binary relations over a set under relational composition.

A *left test semiring (quantale)* is a pair $(S, \mathsf{test}(S))$, where S is an idempotent left semiring (a left quantale) and $\mathsf{test}(S) \subseteq [0,1]$ is a Boolean subalgebra of the set $[0,1]$ of S such that $0, 1 \in \mathsf{test}(S)$ and join and meet in $\mathsf{test}(S)$ coincide with $+$ and $\cdot$, respectively. This definition corresponds to the one given in [12]. We will use $a, b, c \ldots$ for arbitrary S-elements and $p, q, r, \ldots$ for tests. By $\neg$ we denote complementation in $\mathsf{test}(S)$.

An important property of left test semirings is distribution of test multiplication over meet [15]: if $a \sqcap b$ exists then

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

A *left domain semiring (quantale)* is a pair $(S, \ulcorner)$, where S is a left test semiring (quantale) and the *domain* operation $\ulcorner\colon S \to \mathsf{test}(S)$ satisfies

$$a \leq \ulcorner a \cdot a \quad \text{(d1)}, \qquad \ulcorner(p \cdot a) \leq p \quad \text{(d2)}, \qquad \ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b) \quad \text{(d3)}.$$

The axioms are the same as in [5]; their relevant consequences can still be proved over left semirings (quantales) (see [15]). In particular, $\ulcorner$ is universally disjunctive and hence $\ulcorner 0 = 0$. In contrast to arbitrary complete Boolean test semirings [14], the domain operation is guaranteed to exist in left test quantales.

Checking all the axioms for the case of processes, we get

Lemma 3.1 *1. The processes form a Boolean left domain quantale*

$$\mathrm{PRO} \stackrel{\mathrm{def}}{=} (\mathcal{P}(\mathrm{TRA}), \cup, \emptyset, \cdot, I, \ulcorner)$$

with $\mathsf{test}(\mathrm{PRO}) = \mathcal{P}(\{\underline{v} \mid v \in V\})$ *and* $\ulcorner A = \{\underline{g(0)} \mid (d, g) \in A\}$.

2. *Additionally, $\cdot$ is positively disjunctive in its right argument, and chop inherits the disjunctivity properties from $\cdot$ and is associative, too.*
3. *Since 0 is indivisible, the meet with a test distributes over composition:*

$$P \in \mathsf{test}(\mathrm{PRO}) \;\Rightarrow\; P \cap A \cdot B \;=\; (P \cap A) \cdot (P \cap B)$$

As in [15], we can extend an idempotent left semiring by finite and infinite iteration. A *left Kleene algebra* is a structure $(S, {}^*)$ consisting of an idempotent semiring S and an operation * that satisfies the left *unfold* and *induction* axioms

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

To express infinite iteration we axiomatise an ω-operator over a left Kleene algebra. A *left ω algebra* [2] is a pair $(S, {}^\omega)$ such that S is a left Kleene algebra and ${}^\omega$ satisfies the *unfold* and *coinduction* axioms

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

Lemma 3.2

1. *Every left quantale can be extended to a left Kleene algebra by defining* $a^* \stackrel{\text{def}}{=} \mu x\,.\, a \cdot x + 1$.
2. *If the left quantale is a completely distributive lattice then it can be extended to a left* ω *algebra by setting* $a^\omega \stackrel{\text{def}}{=} \nu x\,.\, a \cdot x$. *In this case,*

$$\nu x\,.\, a \cdot x + b \;=\; a^\omega + a^* \cdot b\;.$$

The proof uses fixpoint fusion.

Since by Lemma 3.1 PRO forms a left quantale, we also have finite iteration * and infinite iteration $^\omega$ with all their laws available. Moreover, being Boolean, the quantale is separated, which provides a number of useful laws about the interaction of inf and fin with the semiring and iteration operations [15].

4 Range Assertions, Safety and Liveness

Often, it is necessary to restrict the range of a process A. Here, the range $\mathsf{ran}\,A$ is defined as $\mathsf{ran}\,A \stackrel{\text{def}}{=} \bigcup_{t \in A} \mathsf{ran}\,t$.

Running Example We model the jump and invariant conditions for the transition from *Off* to *On*. First, we generally set

$$R_{[l,u]} \stackrel{\text{def}}{=} \{\underline{x} \,|\, x \in [l,u]\}\;.$$

Then the sequence "Off–jump–On" equals $A_{\mathrm{Off}} \cdot R_{[18,19]} \cdot A_{\mathrm{On}}$. As a safety condition for the thermostat of Figure 1 we want to guarantee the temperature to be between 18 and 22 degrees, i.e., we want to restrict the range of $A_{\mathrm{Off}} \cdot A_{\mathrm{On}}$ and $(A_{\mathrm{Off}} \cdot A_{\mathrm{On}})^*$. Thus we need to define a process containing all trajectories that never leave the range $[18, 22]$. □

We do this by observing that every test $P \in \mathsf{test}(\mathrm{PRO})$ is isomorphic to a subset of the value set V of the trajectories.

With $\top \stackrel{\text{def}}{=} \mathrm{TRA}$ and $\mathsf{F} \stackrel{\text{def}}{=} \mathsf{fin}\,(\mathrm{TRA})$ we define, for $P \in \mathsf{test}(\mathrm{PRO})$,

$$\Diamond P \stackrel{\text{def}}{=} \mathsf{F} \cdot P \cdot \top\,, \qquad \Box P \stackrel{\text{def}}{=} \overline{\Diamond \neg P},\,.$$

Hence, $\Box P$ describes a safety aspect, viz. the set of all trajectories whose range satisfies the "invariant" P, i.e., $\Box P = \{t \in \mathrm{TRA} \,|\, \mathsf{ran}\,t \subseteq P\}$. Thus, the requested safety condition for the thermostat can be modelled as $\Box R_{[18,22]}$. Dually, $\Diamond P$ can be used to describe liveness aspects.

We now generalise these operators to an arbitrary general Boolean left test quantale S. Let $\top$ be the greatest element of S and set $\mathsf{F} \stackrel{\text{def}}{=} \mathsf{fin}\,\top$ and $\mathsf{N} \stackrel{\text{def}}{=} \mathsf{inf}\,\top$. By general results in [15] we have $F \cdot 0 = 0$, $\mathsf{N} = \top \cdot 0 = \mathsf{N} \cdot a$ for all a and $\mathsf{F} = \overline{\mathsf{N}}$. Moreover, F is downward closed and $1 \leq \mathsf{F}$, so that also $p \leq \mathsf{F}$ for all $p \in \mathsf{test}(S)$. Finally, $\mathsf{F} \cdot \mathsf{F} \leq \mathsf{F}$. Let now, for $p \in \mathsf{test}(S)$,

$$\Diamond p \stackrel{\text{def}}{=} \mathsf{F} \cdot p \cdot \top, \qquad \Box p \stackrel{\text{def}}{=} \overline{\Diamond \neg p}.$$

Thus, $\Box p$ corresponds to the "always p" operator of von Karger [11], whence the notation. Since $\Diamond$ and $\Box$ do not yield tests as their results, they cannot be nested. This does no harm, since nested safety requirements do not seem to be useful anyway. Moreover, all other algebraic operations are available for them. Our goal is now to derive a number of useful algebraic laws for $\Diamond$ and $\Box$.

Lemma 4.1 *Assume a left test quantale in which $\cdot$ is also positively right-disjunctive. Then $\Diamond$ is universally disjunctive and $\Box$ is universally conjunctive. In particular, both operators are isotone.*

Therefore we can define a general operator $\mathsf{ran} : S \to \mathsf{test}(S)$ by the Galois connection

$$\mathsf{ran}\, a \leq p \stackrel{\text{def}}{\Leftrightarrow} a \leq \Box p \ . \tag{1}$$

Running Example Looking again at the safety requirement of the thermostat we see that by the condition $A_{\text{Off}} \cdot A_{\text{On}} \leq \Box R_{[18,22]}$ we indeed restrict the range of $A_{\text{Off}} \cdot A_{\text{On}}$ as claimed in the beginning of this section. Using the meet

$$A_{\text{Off}} \cdot A_{\text{On}} \sqcap \Box R_{[18,22]} \tag{th-rest}$$

is another way to enforce the restriction. □

By (1), ran is universally disjunctive. Moreover, we obtain

$$a \leq \Box(\mathsf{ran}\, a) \ , \qquad \mathsf{ran}\,(\Box p) \leq p \ , \qquad p \leq \Box p \Rightarrow \mathsf{ran}\, p \leq p \ .$$

For the following proofs and properties we introduce shorthands for the finite and infinite parts of boxes:

$$f_p \stackrel{\text{def}}{=} \mathsf{fin}\,(\Box p) = \mathsf{F} \sqcap \Box p \ , \qquad i_p \stackrel{\text{def}}{=} \mathsf{inf}\,(\Box p) = \mathsf{N} \sqcap \Box p \ .$$

Now we can show

Lemma 4.2 *Assume a right-distributive left test quantale S and $p \in \mathsf{test}(S)$.*

1. $\Box p = p \cdot (\Box p) = (\Box p) \cdot p$.
2. *If additionally $p \leq \Box p$ then $\ulcorner(\Box p) = p$.*

Proof. 1. We first show $\Box p = p \cdot (\Box p)$.
($\geq$) is clear by $p \leq 1$ and isotony.
($\leq$) We first show $\Box p \leq p \cdot \top$. By shunting this is equivalent to $\top \leq \overline{\Box p} + p \cdot \top$, i.e., to $\top \leq \mathsf{F} \cdot \neg p \cdot \top + p \cdot \top$, which holds by $1 \leq \mathsf{F}$, distributivity and Boolean algebra. Now we obtain $\neg p \cdot \Box p \leq 0$ and hence $\Box p = p \cdot \Box p + \neg p \cdot \Box p = p \cdot \Box p$.
Next, we show $\Box p = (\Box p) \cdot p$.
($\geq$) follows as above.
($\leq$) Splitting $\Box p$ into its finite and infinite parts and using distributivity, we get the equivalent claim $f_p + i_p \leq f_p \cdot p + i_p \cdot p = f_p \cdot p + i_p$. Since finite and

infinite elements have empty intersection, this reduces to $f_p \leq f_p \cdot p$. For this we first show $f_p \leq F \cdot p$. By shunting, this is equivalent to $\top \leq \overline{f_p} + \mathsf{F} \cdot p$, i.e., to $\top \leq \mathsf{N} + \mathsf{F} \cdot \neg p \cdot \top + \mathsf{F} \cdot p$, which holds by $1 \leq \top$, distributivity, Boolean algebra and $\top = \mathsf{N} + \mathsf{F}$. Now we obtain $f_p \cdot \neg p \leq 0$ and hence $f_p = f_p \cdot p + f_p \cdot \neg p = f_p \cdot p$.

2. Axiom (d2) and 1. imply $\lceil(\Box p) \leq p$. The reverse inequation follows from the assumption $p \leq \Box p$, isotony of domain and $\lceil p = p$. □

Some of the following properties are satisfied only in a special kind of left semirings. Since elements of the form $\Box p$ correspond to safety properties, we call a left semiring (quantale) S *safety-closed* if $(\Box p) \cdot (\Box p) \leq \Box p$. In a safety-closed left semiring, $(\Box p)^+ = \Box p$ and

$$a \leq \Box p \Leftrightarrow a^+ \leq \Box p \Leftrightarrow a^+ \leq (\Box p)^+ \ , \tag{2}$$

where $b^+ \stackrel{\text{def}}{=} b \cdot b^*$. In Section 5 we will present a sufficient condition for safety-closedness. By that result, PRO is safety-closed.

Lemma 4.3 *Suppose that S is right-distributive and safety-closed.*

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. *The box is multiplicatively idempotent, i.e.,* $(\Box p) \cdot (\Box p) = \Box p$.

Proof. 1. We show the claim first for finite a, i.e., for $a \leq \mathsf{F}$.
Let, for abbreviation, $s \stackrel{\text{def}}{=} \Box p$ and $d \stackrel{\text{def}}{=} \overline{s} = \Diamond \neg p$. By Boolean algebra and distributivity,

$$a \cdot b = (a \sqcap s) \cdot (b \sqcap s) + (a \sqcap s) \cdot (b \sqcap d) + (a \sqcap d) \cdot b$$

Now we observe that, by definition of d, we have $\mathsf{F} \cdot d \leq d$ and $d \cdot \top \leq d$, so that the last two summands are $\leq d$ by isotony. Hence,

$$a \cdot b \sqcap s = (a \sqcap s) \cdot (b \sqcap s) \sqcap s \leq (a \sqcap s) \cdot (b \sqcap s) \ .$$

The converse inequation holds by isotony and safety-closedness.
For arbitrary a we calculate, using $\mathsf{fin}/\mathsf{inf}$ decomposition, Boolean algebra and the claim for $\mathsf{fin}\, a \leq \mathsf{F}$,

$$\begin{aligned} a \cdot b \sqcap s &= (\mathsf{inf}\, a + \mathsf{fin}\, a \cdot b) \sqcap s \\ &= (\mathsf{inf}\, a \sqcap s) + ((\mathsf{fin}\, a \cdot b) \sqcap s) \\ &= \mathsf{inf}\, (a \sqcap s) + (\mathsf{fin}\, a \sqcap s) \cdot (b \sqcap s) \\ &= \mathsf{inf}\, (a \sqcap s) + \mathsf{fin}\, (a \sqcap s) \cdot (b \sqcap s) \\ &= (a \sqcap s) \cdot (b \sqcap s) \ . \end{aligned}$$

2. We show the claim for finite a; for infinite a the proof proceeds analogously to that of 1. Set $d \stackrel{\text{def}}{=} \Diamond p$ and $s \stackrel{\text{def}}{=} \overline{d} = \Box \neg p$. By Boolean algebra and distributivity,

$$d \sqcap a \cdot b = d \sqcap (d \sqcap a) \cdot b + d \sqcap (s \sqcap a) \cdot (d \sqcap b) + d \sqcap (s \sqcap a) \cdot (s \sqcap b) \ .$$

The first of these summands is below $(d \sqcap a) \cdot b$, the second one is below $a \cdot (d \sqcap b)$ and the third one is 0 by isotony, safety-closedness and $d \sqcap s = 0$. Hence, the sum is below $(d \sqcap a) \cdot b + a \cdot (d \sqcap b)$.
The converse inequation follows by $d \cdot b \leq d$, $a \leq \mathsf{F}$, $\mathsf{F} \cdot d \leq d$ and isotony.

3. This is a consequence of 1., since

$$\Box p \;=\; \Box p \sqcap \top \;=\; \Box p \sqcap \top \cdot \top \;=\; (\Box p \sqcap \top) \cdot (\Box p \sqcap \top) \;=\; \Box p \cdot \Box p \;.$$

□

Running Example Returning to requirement (th-rest), we can transform the safety requirement $R_{20} \cdot (A_{\mathrm{Off}} \cdot A_{\mathrm{On}})^* \sqcap \Box p$ into $R_{20} \cdot ((A_{\mathrm{Off}} \sqcap \Box p) \cdot (A_{\mathrm{On}} \sqcap \Box p))^*$ by (2) and Lemma 4.3.1. Hence, it suffices to guarantee the safety requirement for the two processes A_{Off} and A_{On}. □

Lemma 4.4 *Assume a right-distributive and safety-closed left test quantale S, in which $p \sqcap a \cdot b = (p \sqcap a) \cdot (p \sqcap b)$.*

1. $p \leq \Box q \;\Leftrightarrow\; p \leq q$.
2. $p \leq \Box p$.
3. $\mathsf{ran}\, p = p$.
4. $p \leq \overline{\overline{1} \cdot \overline{1}}$.

Proof. 1. $p \leq \Box q$

$\Leftrightarrow$ {⟦ definition and shunting ⟧}

$p \sqcap \mathsf{F} \cdot \neg q \cdot \top \leq 0$

$\Leftrightarrow$ {⟦ assumption twice ⟧}

$(p \sqcap \mathsf{F}) \cdot (p \sqcap \neg q) \cdot (p \sqcap \top) \leq 0$

$\Leftrightarrow$ {⟦ $p \leq \mathsf{F}$ and meet on tests ⟧}

$p \cdot p \cdot \neg q \cdot p \leq 0$

$\Leftrightarrow$ {⟦ commutativity and idempotence of tests ⟧}

$p \cdot \neg q \leq 0$

$\Leftrightarrow$ {⟦ test shunting ⟧}

$p \leq q$.

2. Set $q = p$ in 1.
3. Using the Galois connection (1) and 1., we have

$$\mathsf{ran}\, p \leq q \;\Leftrightarrow\; p \leq \Box q \;\Leftrightarrow\; p \leq q \;.$$

Now the claim follows by indirect equality.

4. We have $p \sqcap \overline{1} \cdot \overline{1} = (p \sqcap \overline{1}) \cdot (p \sqcap \overline{1}) = 0 \cdot 0 = 0$. □

By Lemma 3.1.3 properties 1. to 4. hold in PRO. In REL, however, subidentities can be decomposed into non-subidentities (unless the underlying base set

is a singleton); so these properties do not hold there. The element $\overline{\overline{1} \cdot \overline{1}}$ has been called step in von Karger's work; it represents the elements that cannot be decomposed into non-subidentities. Note that in arbitrary Boolean semirings property 4. is equivalent to $\overline{1} \cdot \overline{1} \leq \overline{1}$, which roughly says that progress in time cannot be undone.

5 A Sufficient Criterion for Safety-Closedness

For the technical developments of this section we need additional operators. In any left quantale, the *left residual* a/b exists and is characterised by the Galois connection

$$x \leq a/b \stackrel{\text{def}}{\Leftrightarrow} x \cdot b \leq a \ .$$

In PRO, this operation is characterised pointwise by $t \in V/U \ \Leftrightarrow \ \forall \ u \in U : t \cdot u \in V$ (provided $t \cdot u$ is defined). Based on the left residual, in a Boolean quantale the *right detachment* $a \lfloor b$ can be defined as

$$a \lfloor b \stackrel{\text{def}}{=} \overline{\overline{a}/b} \ .$$

The pointwise characterisation in PRO reads $t \in V \lfloor U \ \Leftrightarrow \ \exists \ u \in U : t \cdot u \in V$. By de Morgan's laws, the Galois connection for / transforms into the exchange law $a \lfloor b \leq x \ \Leftrightarrow \ \overline{x} \cdot b \leq \overline{a}$ for $\lfloor$ that generalises the Schröder rule of relational calculus. A straightforward consequence is $(\Box p) \lfloor a \leq \Box p$ (box detachment). Now we can prove

Lemma 5.1 *If S is locally linear [11], i.e., $(a \cdot b) \lfloor a \ = \ a \cdot (b \lfloor c) + a \lfloor (c \lfloor b)$, and right-distributive then S is safety-closed.*

Proof. First, by the definition of diamond, local linearity and box detachment,

$$\begin{aligned} (\Diamond \neg p) \lfloor (\Box p) \ &= \ \mathsf{F} \cdot \neg p \cdot (\top \lfloor (\Box p)) + (\mathsf{F} \cdot \neg p) \lfloor ((\Box p) \lfloor \top) \\ &\leq \ \mathsf{F} \cdot \neg p \cdot (\top \lfloor (\Box p)) + (\mathsf{F} \cdot \neg p) \lfloor (\Box p) \qquad (*) \\ &\leq \ \Diamond \neg p + (\mathsf{F} \cdot \neg p) \lfloor (\Box p) \ . \end{aligned}$$

Hence

$$\begin{array}{ll} & (\Box p) \cdot (\Box p) \leq \Box p \\ \Leftrightarrow & \quad \{\!\![\text{ exchange law }]\!\!\} \\ & (\Diamond \neg p) \lfloor (\Box p) \leq \Diamond \neg p \\ \Leftarrow & \quad \{\!\![\text{ by } (*) \ ]\!\!\} \\ & \Diamond \neg p + (\mathsf{F} \cdot \neg p) \lfloor (\Box p) \leq \Diamond \neg p \\ \Leftrightarrow & \quad \{\!\![\text{ lattice algebra }]\!\!\} \\ & (\mathsf{F} \cdot \neg p) \lfloor (\Box p) \leq \Diamond \neg p \\ \Leftrightarrow & \quad \{\!\![\text{ exchange law }]\!\!\} \\ & (\Box p) \cdot (\Box p) \leq \overline{\mathsf{F} \cdot \neg p} \end{array}$$

$\Leftrightarrow$ {⟦ Boolean algebra ⟧}
$(\Box p) \cdot (\Box p) \leq \mathsf{N} + \mathsf{F} \cdot p$
$\Leftrightarrow$ {⟦ by Lemma 4.2.1 ⟧}
$(\Box p) \cdot (\Box p) \cdot p \leq \mathsf{N} + \mathsf{F} \cdot p$
$\Leftrightarrow$ {⟦ $\Box p = f_p + i_p$ (p. 6), distributivity and $\mathsf{fin}\,/\mathsf{inf}$ laws ⟧}
$f_p \cdot f_p \cdot p \leq \mathsf{F} \cdot p$
$\Leftrightarrow$ {⟦ f_p finite and F closed under $\cdot$ ⟧}
TRUE .

□

Local linearity of PRO can be proved as in the case of the semiring of formal languages, as done in [8]; hence PRO is safety-closed. Next, we have

Lemma 5.2 *Assume a right-distributive and safety-closed left test quantale S.*

1. $a \cdot b \sqcap f_p \cdot \Box q = (a \sqcap f_p) \cdot (b \sqcap f_p \cdot \Box q) + (a \sqcap f_p \cdot \Box q) \cdot (b \sqcap \Box q)$.
2. $a \cdot b \sqcap i_p = (a \sqcap f_p) \cdot (b \sqcap i_p) + (a \sqcap i_p)$.
3. $a \cdot b \sqcap \Box p \cdot \Box q = (a \sqcap f_p) \cdot (b \sqcap \Box p \cdot \Box q) + (a \sqcap \Box p \cdot \Box q) \cdot (b \sqcap \Box q)$.

The proofs are straightforward and omitted for lack of space. An application of Lemma 5.2.1 is to combine safety requirements like $R_{[l,u]}$. Since $f_p \cdot \Box q = \Box p^\frown \Box q$, a safety requirement of this form guarantees that the process $\Box q$ is actually entered.

6 Temporal Operators

Specifications are particular processes that express desired patterns. Following Sintzoff [16], we define the following quantifier-like operators relating a specification W with a process B supposed to implement it. If one considers the values in V as states then the set $\{t(0) \mid t \in B \cap W\}$ gives all starting states of the trajectories in B admitted by W as well. However, it is more convenient to represent this set as a test in the left test semiring of processes, viz. as $\{\underline{t(0)} \mid t \in B \cap W\}$. But this compacts simply into $\ulcorner(B \cap W)$. Therefore, a first definition of Sintzoff's quantifiers reads as follows (the primes indicate that we will use a different definition later on):

$$\mathsf{E}'B \,.\, W \stackrel{\text{def}}{=} \ulcorner(B \cap W) \;, \qquad \mathsf{A}'B \,.\, W \stackrel{\text{def}}{=} \neg\mathsf{E}'B \,.\, \overline{W} = \neg\ulcorner(B \cap \overline{W}) \;,$$
$$\mathsf{AE}'B \,.\, W \stackrel{\text{def}}{=} \mathsf{A}'B \,.\, W \cap \mathsf{E}'B \,.\, W \,.$$

This definition works in general Boolean left domain semirings. However, as the resulting quantifiers are operators of type PRO $\to$ (PRO $\to$ test(PRO)), they cannot easily be composed. Therfore, Sintzoff gives a different semantics to combinations of these quantifiers. We want to avoid this by introducing new quantifiers that omit the final projection into test(PRO). Doing this, we also

allow a look into the "future" of trajectories and not only at the starting states. In other words, our new quantifiers in PRO should model formulas like

$$t \in \mathsf{E}B\,.\,W \overset{\text{def}}{\Leftrightarrow} \exists\, u \in B : t \cdot u \in W,$$
$$t \in \mathsf{A}B\,.\,W \overset{\text{def}}{\Leftrightarrow} \forall\, u \in B : t \cdot u \in W.$$

These quantifiers are operators of type PRO $\to$ PRO and their sequential composition simply is function composition. If a projection into $\mathsf{test}(\mathrm{PRO})$ is desired it can be added at the outermost level by finally applying one of the three quantifiers above. For their algebraic characterisation we use again the detachment operator.

Lemma 6.1 *In a Boolean test quantale, one has*

$$\ulcorner(b \sqcap w) \;=\; w\lfloor b \sqcap 1 \;=\; b\lfloor w \sqcap 1\ .$$

In the detachment formulas of this lemma, forming the meet with 1 performs the projection into the test algebra, and we obtain our revised operators by omitting this meet. There is a choice in which of these two formulas to use. We take the first one, since it results in a more direct translation of the universal quantifier A'. Assume a Boolean quantale S and $a, b \in S$. Then

$$\mathsf{E}b\,.\,w \overset{\text{def}}{=} w\lfloor b\ , \qquad \mathsf{A}b\,.\,w \overset{\text{def}}{=} \overline{\mathsf{E}b\,.\,\overline{w}} = w/b\ ,$$
$$\mathsf{AE}b\,.\,w \overset{\text{def}}{=} (\mathsf{A}b\,.\,w) \sqcap (\mathsf{E}b\,.\,w)\ .$$

In PRO the process $\mathsf{E}B\,.\,W$ consists of all trajectories that can be completed by a B-trajectory to yield a trajectory in W. Thus, $\mathsf{E}B\,.\,W$ is the inverse image of W under the operation $\cdot B$, while $\mathsf{A}B\,.\,W$ is the largest process whose image under $\cdot B$ is contained in W. This suggests the following modal view of these quantifiers: E is a kind of diamond, whereas A forms a box operator. Correspondingly, we have the following properties that are typical for modal operators.

Lemma 6.2

1. $\mathsf{E}a$ *is universally disjunctive and* $\mathsf{A}a$ *is universally conjunctive.*
2. $\mathsf{E}(a \cdot b)\,.\,c = \mathsf{E}a\,.\,(\mathsf{E}b\,.\,c)$ *and* $\mathsf{A}(a \cdot b)\,.\,c = \mathsf{A}a\,.\,(\mathsf{A}b\,.\,c)$.
3. *If* $\cdot$ *is positively disjunctive in its right argument then* E *is positively disjunctive and* A *is positively antidisjunctive.*

7 Linking With Game Theory

As Sintzoff [16] has shown, the theory of games helps in understanding control systems as well as hybrid and reactive ones, since it deals with interaction between dynamics. For example, a control system can be presented as a game where the *controlling* and the *controlled* components are, respectively, the proponent and the opponent [10]. As the controller has to counteract all possible failures

induced by "moves" of the controlled system, it has to force the opponent into a "losing" position where nothing can go wrong anymore. In PRO, moves correspond to process transformers of the shapes $\mathsf{E}B$ and $\mathsf{A}B$. They describe the possible and guaranteed reachabilities from a game position using B-trajectories.

Abstractly, a *game* consists of one or more *players* who interact with each other. A *move* is an action of one player. Obviously, there are various kinds of games, like games with finite or infinite duration. In the second case, one can distinguish games with finite and infinite move duration. Another possibility of classifying games are the categories of *cooperate*, *non-cooperate* and *semi-cooperate* games, depending on the methods by which the players will interact. Further, we can split all games into *disjoint* and *non-disjoint* ones. Non-disjoint games allow several moves at the same time, while in a disjoint game there is one move at a time.

In the remainder, we restrict ourselves to disjoint games with finite move duration. In a *game round*, each player, one by one, makes a move. Hence, if S_i is defined as the a move of player i, a game round is represented by $(S_1 \cdot S_2 \cdots S_n)$. In that case, we can use the * and ω operators; $(S_1 \cdot S_2 \cdot \cdots \cdot S_n)^*$ describes a finite game and $(S_1 \cdot S_2 \cdot \cdots \cdot S_n)^\omega$ a game with infinitely many game rounds. In the latter case, the game has infinite duration if the S_i have positive durations.

In a game with player X and opponent Y, represented by their respective moves $\mathsf{E}a$ and $\mathsf{A}b$, we can interpret a game round in which X has the possibility of "winning" as the product $\mathsf{E}a \circ \mathsf{A}b$ (cf. [6]), where $\circ$ is composition of process transformers. Finite or infinite games can then be described as $(\mathsf{E}a \circ \mathsf{A}b)^*$ or $(\mathsf{E}a \circ \mathsf{A}b)^\omega$ from which winning and losing "positions" can be calculated by fixpoint iteration (e.g according to *Kleene's theorem*); for details see e.g. [1, 5]. Since we have now established the connection to the modal view of games started in [1] and treated abstractly in [5], we can re-use the analysis of winning and losing positions provided in these papers. This allows us to unify several results (e.g. [16]). A more thorough analysis of the game-theoretic connection will be the subject of further papers.

8 Conclusion and Outlook

This paper provides a starting point for developing an algebraic theory of hybrid systems. The theory of *Lazy Kleene algebras* [15] finds a useful further application here, generalising some similar results for the strict setting in [11]. Although one has to take some care with the modified laws relative to standard (modal) Kleene algebra, things work out reasonably well and many results come for free.

The aim of further work in this area is to develop a suitable specialisation of the general results to form new, more convenient algebraic calculi, both for safety and liveness proofs, and to provide a connection with the algebraic view of the duration calculus started in [11, 9]. Another aim is to use the game-theoretic approach to obtain improved controllers for hybrid systems. Finally, it has to be checked in how far hybrid (I/O) automata can be treated in this style to make the theory even more useful. It seems that the semantic models used in [4, 13]

can be made into left domain quantales, too, so that our results would carry over to these frameworks.

Acknowledgements: We are grateful to M. Sintzoff for preparing the ground so well and to J. Desharnais, G. Struth and the anonymous referees for helpful discussions and remarks.

References

1. R. Backhouse, D. Michaelis: Fixed-Point Characterisation of Winning Strategies in Impartial Games. In R. Berghammer, B. Möller, G. Struth (eds.): Relational and Kleene-Algebraic Methods in Computer Science. LNCS 3051. Springer 2004, 34–47
2. E. Cohen: Separation and Reduction. In R. Backhouse, J. N. Oliveira (eds.): Mathematics of Program Construction. LNCS 1837. Springer 2000, 45–59
3. J. H. Conway: Regular Algebra and Finite Machines. Chapman & Hall, 1971
4. J. M. Davoren, A. Nerode: Logics for Hybrid Systems. Proc. IEEE 88, 985–1010 (2000)
5. J. Desharnais, B. Möller, G. Struth: Kleene Algebra with Domain. ACM Trans. Computational Logic (to appear 2006). Preliminary version: Universität Augsburg, Institut für Informatik, Report No. 2003-07, June 2003
6. J. Desharnais, B. Möller, G. Struth: Modal Kleene Algebra and Applications – A Survey. J. Relational Methods in Computer Science 1, 93–131 (2004) `http://www.cosc.brocku.ca/Faculty/Winter/JoRMiCS/`
7. T. Henzinger: The Theory of Hybrid Automata. Proc. 11th Annual IEEE Symposium on Logic in Computer Science, New Brunswick, New Jersey, 1996, 278–292
8. P. Höfner: From Sequential Algebra to Kleene Algebra: Interval Modalities and Duration Calculus. Technical Report 2005-5, Institut für Informatik, Universität Augsburg, 2005
9. P. Höfner: An Algebraic Semantics for Duration Calculus. 17th European Summer School in Logic, Language and Information (ESSLLI), Proc. 10th ESSLLI Student Session, Heriot-Watt University Edinburgh, Scotland, August 2005, 99–111
10. R. Isaacs: Differential Games. Wiley, 1965. Republished: Dover, 1999
11. B. von Karger: Temporal Algebra. Habilitation thesis, University of Kiel 1997
12. D. Kozen: Kleene Algebra with Tests. ACM Trans. Programming Languages and Systems 19, 427–443 (1997)
13. N. A. Lynch, R. Segala, F. W. Vaandrager: Hybrid I/O Automata. Information and Computation 185, 105–157 (2003)
14. B. Möller: Complete Tests do not Guarantee Domain. Technical Report 2005-6, Institut für Informatik, Universität Augsburg, 2005
15. B. Möller: Lazy Kleene Algebra. In D. Kozen (ed.): Mathematics of Program Construction. LNCS 3125. Springer 2004, 252–273
16. M. Sintzoff: Iterative Synthesis of Control Guards Ensuring Invariance and Inevitability in Discrete-Decision Games. In O. Owe, S. Krogdahl, T. Lyche (eds.): From Object-Orientation to Formal Methods — Essays in Memory of Ole-Johan Dahl. LNCS 2635. Springer 2004, 272–301