Kleene getting lazy

Bernhard Möller

Angaben zur Veröffentlichung / Publication details:

Möller, Bernhard. 2007. “Kleene getting lazy.” *Science of Computer Programming* 65 (2): 195–214. https://doi.org/10.1016/j.scico.2006.01.010.

Kleene Getting Lazy

Bernhard Möller,

Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany

Abstract

We propose a relaxation of Kleene algebra by giving up strictness and right-distributivity of composition. This allows the subsumption of Dijkstra's computation calculus, Cohen's omega algebra and von Wright's demonic refinement algebra. Moreover, by adding domain and codomain operators we can also incorporate modal operators. We show that predicate transformers form lazy Kleene algebras, the disjunctive and conjunctive ones even lazy omega Kleene algebras. We also briefly sketch two further applications: a modal lazy Kleene algebra of commands modelling total correctness and another one that abstractly characterizes sets of trajectories as used in the description of reactive and hybrid systems.

Key words: algebraic semantics, lazy evaluation, Kleene algebra, omega algebra, modal operators, predicate transformers

1 Introduction

Kleene algebra (KA) provides a convenient and powerful algebraic axiomatization of the basic control constructs composition, choice and iteration. In its standard version, composition is required to distribute over choice in both arguments; also, 0 is required to be both a left and right annihilator. Algebraically this is captured by the notion of an idempotent semiring or briefly *I-semiring.*

Models include formal languages under concatenation, relations under standard composition and sets of graph paths under path concatenation.

The idempotent semiring addition induces a partial order that can be thought of as the approximation order or as (angelic) refinement. Addition then coin-

Email address: Bernhard.Moeller@informatik.uni-augsburg.de (Bernhard Möller).

cides with the binary supremum operator, i.e., every semiring is also an upper semilattice. Moreover, 0 is the least element and thus plays the rôle of $\perp$ in denotational semantics.

If the semilattice is even a complete lattice, the least and greatest fixpoint operators allow definitions of the finite and infinite iteration operators * and $^\omega$, resp. However, to be less restrictive, we do *not* assume completeness and rather add, as is customary, * and $^\omega$ as operators of their own with particular axioms.

The requirement that 0 be an annihilator on both sides of composition makes the algebra *strict*. This prohibits a natural treatment of systems in which infinite computation sequences are left annihilators w.r.t. sequential composition. Therefore we study a "one-sided" variant of KAs in which composition is strict in one argument only. This treatment fits well with systems such as the calculus of finite and infinite streams which is also used in J. Lukkien's operational semantics for the guarded command language [22,23] or R. Dijkstra's computation calculus [11,12]. Inspired by the latter papers, we obtain a very handy algebraic characterization of finite and infinite elements that also appears already in early work on so-called quemirings by Elgot [13]. In addition, we integrate the theory with Cohen's ω-algebra [7] and von Wright's demonic refinement algebra [36,37].

There is some choice in what to postulate for the right argument of composition. Whereas the above-mentioned authors stipulate binary or even general positive disjunctivity, we investigate how far one gets if only isotony is required. This allows general isotone predicate transformers as models.

Fortunately, our lazy KAs are still powerful enough to admit the incorporation of domain and codomain operators and hence an algebraic treatment of modal logic. Of course, the possibility of nontrivial infinite computations leads to additional terms in the corresponding assertion logic; these terms disappear when only finite elements are considered.

Altogether, we obtain a quite lean framework that unites assertion logic with algebraic reasoning while admitting infinite computations. The axiomatization is simpler and more general than that of von Karger's sequential calculus [18].

We also briefly sketch two applications: a modal lazy Kleene algebra of commands modelling a total correctness view of imperative programs and another one that abstractly characterizes sets of trajectories as used in the description of reactive and hybrid systems.

2 Left Semirings

The essential control constructs in almost all systems are choice and sequential composition. This is captured as follows.

Definition 2.1 A *left (or lazy) semiring*, briefly an *L-semiring*, is a quintuple $(K, +, 0, \cdot, 1)$ with the following properties:

(a) $(K, +, 0)$ is a commutative monoid.
(b) $(K, \cdot, 1)$ is a monoid.
(c) The $\cdot$ operation distributes over $+$ in its left argument and is *left-strict*:

$$(a + b) \cdot c \;=\; a \cdot c + b \cdot c \ , \qquad 0 \cdot a \;=\; 0 \ .$$

In many contexts the left semiring operations can be interpreted as follows:

$$\begin{array}{lcl} + & \leftrightarrow & \text{choice,} \\ \cdot & \leftrightarrow & \text{sequential composition,} \\ 0 & \leftrightarrow & \text{abortion,} \\ 1 & \leftrightarrow & \text{identity,} \\ \leq & \leftrightarrow & \text{increase in information or in choices.} \end{array}$$

We write temporal succession from left to right, i.e., $a \cdot b$ means "first perform computation a and then b".

Definition 2.2 An *idempotent* left semiring, or briefly *IL-semiring* is an L-semiring $(K, +, 0, \cdot, 1)$ with idempotent addition in which $\cdot$ is right-isotone:

$$a + a \;=\; a \ \wedge \ (b \leq c \Rightarrow a \cdot b \leq a \cdot c) \ ,$$

where the *natural order* $\leq$ on K is given by $a \leq b \overset{\text{def}}{\Leftrightarrow} a + b \;=\; b$.

Every IL-semiring forms an upper semilattice in which $a + b$ is the supremum of a and b with the universal characterisation

$$a + b \leq c \Leftrightarrow a \leq c \wedge b \leq c \ .$$

Moreover, 0 is the least element w.r.t. the natural order. Note that left-isotony of $\cdot$ follows from its left-distributivity.

A left semiring structure is also at the core of process algebra frameworks (see e.g. [4,5]). One model of an IL-semiring is the set of equivalence classes of processes under simulation equivalence. The associated natural order is the relation of simulatability, i.e., the union of all simulation relations [30,35]. The role of 0 is played by the deadlock or inaction element δ (also called nil

or `STOP`). The neutral element 1 for multiplication is the empty process or termination constant ε (also called `SKIP`).

However, there are also some essential differences. In process algebra, 0 has at least the empty trace, since all processes p satisfy $p \xrightarrow{\varepsilon} p$, whereas in Kleene algebra 0 stands for an element with no "traces" at all, as is apparent e.g. from its relational model. Further, composition is viewed as gluing all "elements" (such as trees or traces) of the right argument to all ends of "elements" (such as tree paths or traces) in the left argument. Therefore only infinite tree paths or traces or in the left argument "survive" composition with 0 from the right. This is the basis of our algebraic characterisation of finite and infinite parts in Section 4.

By isotony, $\cdot$ is universally superdisjunctive and universally subconjunctive in both arguments; we state these properties for the right argument (where $\sqcup$ denotes the supremum and $\sqcap$ the infimum operator):

$$a \cdot (\sqcup L) \geq \sqcup \{a \cdot l : l \in L\} \qquad a \cdot (\sqcap L) \leq \sqcap \{a \cdot l : l \in L\} \ .$$

Analogous properties hold for the left argument.

From this we can conclude a weak form of right distributivity for the left hand side of inequations:

Lemma 2.3 *For $a, b, c, d \in K$ we have*

$$b + c \leq d \ \Rightarrow \ a \cdot b + a \cdot c \leq a \cdot d \ .$$

PROOF. By isotony and superdisjunctivity we get

$$b + c \leq d \ \Rightarrow \ a \cdot (b + c) \leq a \cdot d \ \Rightarrow \ a \cdot b + a \cdot c \leq a \cdot d \ .$$

□

Definition 2.4 (a) A function between partial orders is called *universally disjunctive* if it preserves all existing suprema. A binary operation is called *universally left-(right-)disjunctive* if it is universally disjunctive in its left (right) argument.

(b) An IL-semiring $(K, +, 0, \cdot, 1)$ is *bounded* if K has a greatest element $\top$ w.r.t. the natural order. It is a *left quantale* if the semilattice $(K, \leq)$ is a complete lattice and $\cdot$ is universally left-disjunctive.

(c) Finally, K is *Boolean* if $(K, \leq)$ is a *Boolean algebra*, i.e., a complemented distributive lattice. Every Boolean IL-semiring is bounded.

Now we introduce symmetric notions w.r.t. the right argument of composition.

Definition 2.5 For a binary operation $\cdot : K \times K \to K$ we define its *mirror operation* $\breve{\cdot} : K \times K \to K$ by $x \mathbin{\breve{\cdot}} y = y \cdot x$. We call $(K, +, 0, \cdot, 1)$ an *(idempotent) right semiring* (briefly *(I)R-semiring*) if $(K, +, 0, \breve{\cdot}, 1)$ is an (I)L-semiring. The notions of a *right quantale* and *Boolean* (I)R-semiring are defined analogously. If K is both an (I)L-semiring and an (I)R-semiring it is called an *(I-)semiring.* Analogously, K is a *Boolean* (I-)semiring (a *quantale* [31]) if is both a left and right Boolean (I-)semiring (quantale). A quantale is also called a *standard Kleene algebra* [8].

Note, however, that in (I-)semirings composition is also right-strict; hence these structures are not very interesting if one wants to model lazy computation systems. Prominent I-semirings are the algebra of binary relations under relational composition and the algebra of formal languages under concatenation or join (fusion product).

3 Particular IL-Semirings

We now introduce two important non-strict IL-semirings. Both are based on finite and infinite strings over an alphabet A. Next to their classical interpretation as characters, the elements of A may e.g. be thought of as states in a computation system, or, in connection with graph algorithms, as graph nodes. As usual, A^* is the set of all finite words over A; the empty word is denoted by ε. Moreover, A^ω is the set of all infinite words over A. We set $A^\infty \overset{\text{def}}{=} A^* \cup A^\omega$. The length of word s is denoted by $|s|$. As usual, concatenation is denoted by juxtaposition, where $st \overset{\text{def}}{=} s$ if $|s| = \infty$. A *language* over A is a subset of A^∞. As usual, we identify a singleton language with its only element. For language $S \subseteq A^\infty$ we define its infinite and finite parts by

$$\begin{aligned} \mathsf{inf}\, S &\overset{\text{def}}{=} \{s \in S : |s| = \infty\} \ , \\ \mathsf{fin}\, S &\overset{\text{def}}{=} S - \mathsf{inf}\, S \ . \end{aligned}$$

Definition 3.1 The algebra $\mathrm{WOR}(A) = (\mathcal{P}(A^\infty), \cup, \emptyset, \ , \varepsilon)$ is obtained by extending concatenation to languages in the following way:

$$S\,T \overset{\text{def}}{=} \mathsf{inf}\, S \cup \{st : s \in \mathsf{fin}\, S \wedge t \in T\} \ .$$

Note that in general $S\,T \neq \{st : s \in S \wedge t \in T\}$; using the set on the right hand side as the definition of $S\,T$ one would obtain a right-strict operation. With the above definition, $S\,\emptyset = \mathsf{inf}\, S$ and hence $S\,\emptyset = \emptyset$ iff $\mathsf{inf}\, S = \emptyset$. It is straightforward to show that $\mathrm{WOR}(A)$ is an IL-semiring. The algebra is well-known from the classical theory of ω-languages (see e.g. [33] for a survey).

Next to this model we will use a second one that has a more refined view of composition and hence allows more interesting modal operators.

Definition 3.2 We define the *join* or *fusion product* $\bowtie$ of words as a language-valued operation. For $s \in A^*$, $t \in A^\infty$ and $x, y \in A$,

$$\begin{array}{lll} \varepsilon \bowtie \varepsilon \stackrel{\mathrm{def}}{=} \varepsilon & \varepsilon \bowtie s \stackrel{\mathrm{def}}{=} s \bowtie \varepsilon \stackrel{\mathrm{def}}{=} \emptyset & \text{if } s \neq \varepsilon \ , \\ sx \bowtie xt \stackrel{\mathrm{def}}{=} sxt \ , & sx \bowtie yt \stackrel{\mathrm{def}}{=} \emptyset & \text{if } x \neq y \ . \end{array}$$

Finally, $s \bowtie t \stackrel{\mathrm{def}}{=} s$ if $|s| = \infty$.

Informally, a non-empty finite word s can be joined with a non-empty word t iff the last letter of s coincides with the first one of t; only one copy of that letter is kept in the joined word.

Since we view the infinite words as streams of computations, we call the algebra based on this composition operation STR(A).

Definition 3.3 The algebra STR(A) $\stackrel{\mathrm{def}}{=}$ $(\mathcal{P}(A^\infty), \cup, \emptyset, \bowtie, A \cup \varepsilon)$ is given by extending $\bowtie$ to languages in the following way:

$$S \bowtie T \stackrel{\mathrm{def}}{=} \mathsf{inf}\, S \ \cup \ \{s \bowtie t : s \in \mathsf{fin}\, S \ \wedge \ t \in T\} \ .$$

As above, we have $S \bowtie \emptyset = \mathsf{inf}\, S$ and hence $S \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, S = \emptyset$. It is straightforward to show that STR(A) is an IL-semiring. Its subalgebra $(\mathcal{P}(A^\infty - \varepsilon), \cup, \emptyset, \bowtie, A)$ of nonempty words is at the heart of the papers by Lukkien [22,23] and Dijkstra [11,12].

Both WOR(A) and STR(A) are even Boolean left quantales. Further IL-semirings are provided by predicate transformer algebras (see below).

4 Terminating and Non-Terminating Elements

As stated, we want to model computation systems in such a way that the operator $\cdot$ represents sequential composition and 0 stands for the totally useless system abort that has no computation at all.

We now head for an algebraic characterisation of finite and infinite computations. This will be achieved using the above properties of the finite and infinite parts of a language.

Operationally, an infinite, non-terminating computation a cannot be followed by any further computation. Algebraically this means that composing a with any other element on the "infinite side" has no effect, i.e., just a again results. This convention motivates the following

Definition 4.1 In an IL-semiring $(K, +, 0, \cdot, 1)$, the set N of *non-terminating* or *infinite* elements is the set of all left zeros w.r.t. composition, i.e.,

$$\mathsf{N} \overset{\text{def}}{=} \{a \in K \mid \forall\, b \in K : a \cdot b \;=\; a\} \;.$$

Calling a non-terminating element a also infinite emphasises that all computations of a (if any) are infinite.

From left-strictness of $\cdot$ we immediately get $0 \in \mathsf{N}$. Moreover, we have the following characterisation of non-terminating elements:

Lemma 4.2 (a) $a \in \mathsf{N} \Leftrightarrow a \cdot 0 = a$.
(b) $\mathsf{N} = \{a \cdot 0 : a \in K\}$.

PROOF.

(a) $(\Rightarrow)$ Choose $b = 0$ in the definition of N.
$(\Leftarrow)$ Using the assumption, associativity, left strictness and the assumption again, we calculate $a \cdot b = a \cdot 0 \cdot b = a \cdot 0 = a$.
(b) $(\subseteq)$ Immediate from the definition of N.
$(\supseteq)$ Assume $z = a \cdot 0$. Then $z \cdot 0 = a \cdot 0 \cdot 0 = a \cdot 0 = z$. □

By (a) N coincides with the set of fixpoints of the isotone function $\lambda z \,.\, z \cdot 0$. Hence, if K is even a complete lattice, by Tarski's fixpoint theorem N is a complete lattice again.

Next we state two closure properties of N.

Lemma 4.3 *Denote by $\cdot$ also the pointwise extension of $\cdot$ to subsets of K.*

(a) *An arbitrary computation followed by a non-terminating one is non-terminating, i.e., $K \cdot \mathsf{N} \subseteq \mathsf{N}$ (and hence $K \cdot \mathsf{N} = \mathsf{N}$).*
(b) *N is closed under all existing suprema.*

PROOF.

(a) Consider $a \in K$ and $b \in \mathsf{N}$. Then $(a \cdot b) \cdot 0 \;=\; a \cdot (b \cdot 0) \;=\; a \cdot b$. The inclusion $N \subseteq K \cdot N$ follows by $1 \in K$.

(b) Consider $L \subseteq \mathsf{N}$ such that $\sqcup L$ exists. By superdisjunctivity we get $(\sqcup L) \cdot 0 \geq \sqcup (L \cdot 0) = \sqcup L$. The reverse inequality follows by $0 \leq 1$ and right-isotony of $\cdot$. □

Now we relate the notions of right-strictness and termination.

Lemma 4.4 *The following properties are equivalent:*

(a) *The $\cdot$ operation is right-strict.*
(b) $|\mathsf{N}| = 1$.
(c) $\top \cdot 0 = 0$ *(provided K is bounded).*

PROOF. ((a) ⇒ (b)) It follows that $\mathsf{N} = \{0\}$.
((b) ⇒ (c)) Since $0 \in \mathsf{N}$ and $\top \cdot 0 \in \mathsf{N}$ we get $\top \cdot 0 = 0$.
((c) ⇒ (a)) For arbitrary $a \in K$ we have, by isotony, $a \cdot 0 \leq \top \cdot 0 = 0$. □

Next we show

Lemma 4.5 (a) *$b \cdot 0$ is the greatest element of* $\mathsf{N}(b) \overset{\text{def}}{=} \{a \in \mathsf{N} : a \leq b\}$.
(b) *If K is bounded then $\top \cdot 0$ is the greatest element of N. In particular,* $\top \cdot 0 = \sqcup \mathsf{N}$.
(c) *If N is downward closed and $\top \in \mathsf{N}$ then $1 = 0$ and hence $|K| = 1$.*

PROOF.

(a) First, assume $a \in \mathsf{N} \wedge a \leq b$. Then by right-isotony of $\cdot$ we have $a = a \cdot 0 \leq b \cdot 0$. So $b \cdot 0$ is an upper bound of $\mathsf{N}(b)$.
Second, by Lemma 4.2.(b) we have $b \cdot 0 \in \mathsf{N}$. By right-neutrality of 1 and isotony we get $b \cdot 0 \leq b \cdot 1 = b$, i.e., $b \cdot 0 \in \mathsf{N}(b)$, which shows the claim.
(b) Immediate from (b).
(c) By downward closure, $1 \in \mathsf{N}$, hence $1 = 1 \cdot 0 = 0$ by neutrality of 1. □

Property (b) of this lemma says that $\top \cdot 0$ is an adequate algebraic representation of the collection of all non-terminating elements of a bounded IL-semiring. This is used extensively in [11,12], where $\top \cdot 0$ is called the eternal part of K. A similar definition appears in [27]. However, we want to manage without the assumption of completeness or boundedness and therefore prefer to work with the set N rather than with its greatest element.

By Property (b), and as motivated in Section 2 in connection with the relation between our approach and process algebra, we may call $b \cdot 0$ the *non-terminating* or *infinite part* of b. This leads to the following

Definition 4.6 In an IL-semiring K the set F of *finite* elements is

$$\mathsf{F} \stackrel{\text{def}}{=} \{a \in K \mid a \cdot 0 = 0\} .$$

So $a \in \mathsf{F}$ iff the infinite part of a is trivial. The set of *terminating* elements is

$$\mathsf{T} \stackrel{\text{def}}{=} \mathsf{F} - \{0\} .$$

The terminating elements can be thought of as processes p that have only finite tree paths or traces. Under $\cdot$ they can be continued by another process q only if q actually offer computations. This is why composition with 0 leads to an overall result of 0 for the finite processes.

A general element may have finite and infinite computations; we will look at separating these parts in the next section.

A number of properties of F and T are collected in

Lemma 4.7 (a) F *is downward closed.*
(b) $1 \in \mathsf{F}$. *If* $1 \neq 0$ *then* $1 \in \mathsf{T}$ *(*skip *is terminating).*
(c) $K \cdot \mathsf{F} = K = \mathsf{F} \cdot K$.
(d) $\mathsf{F} + \mathsf{F} \subseteq \mathsf{F}$ *and* $\mathsf{T} + \mathsf{T} \subseteq \mathsf{T}$ *(finite and terminating computations are closed under choice). Since* $+$ *is idempotent we have even equality in both cases. If* $\cdot$ *is universally left-disjunctive then* F *is closed under arbitrary existing suprema and* T *under non-empty ones.*
(e) $\mathsf{F} \cdot \mathsf{F} \subseteq \mathsf{F}$ *(finite computations are closed under composition). By neutrality of* 1 *we have even equality.* T *need not be closed under composition.*

PROOF.

(a) Immediate from isotony.
(b) Immediate from left-neutrality of 1.
(c) By left-neutrality of 1 we get $K = 1 \cdot K \subseteq \mathsf{F} \cdot K$. Similarly, by right-neutrality $K \subseteq K \cdot \mathsf{F}$. The reverse inclusions are trivial.
(d) Immediate from distributivity/disjunctivity.
(e) By (b) we have $\mathsf{F} \cdot \mathsf{F} \cdot \{0\} = \mathsf{F} \cdot \{0\} = \{0\}$, and (b) again shows the claim. An example where T is not closed under $\cdot$ is given by STR(A) over a non-singleton A. There all finite words are terminating, but for $x, y \in A$ with $x \neq y$ we have $xy \bowtie yx = 0 \notin \mathsf{T}$. □

Notation. Although we do not assume a general infimum operation $\sqcap$, we will sometimes use the formula

$$y \sqcap z = 0 \;\stackrel{\text{def}}{\Leftrightarrow}\; \forall\, u \,.\, u \leq y \wedge u \leq z \Rightarrow u = 0 \,.$$

With the help of this, we can describe the interaction between F and N.

Lemma 4.8 (a) *$\mathsf{N} \cap \mathsf{F} = \{0\}$.*
(b) *If N is downward closed, then for $x \in \mathsf{N}$ and $y \in \mathsf{F}$ we have $x \sqcap y = 0$.*
(c) *Assume $x \in \mathsf{N} \wedge y \in \mathsf{F}$. Then $x + y \in \mathsf{N} \Leftrightarrow y \leq x$. Hence if N is downward closed, $x + y \in \mathsf{N} \Leftrightarrow y = 0$.*

PROOF.

(a) If $x \in \mathsf{N} \cap \mathsf{F}$ then $x = x \cdot 0 = 0$.
(b) Suppose $z \leq x \wedge z \leq y$ for some $z \in K$. Then the assumption and Lemma 4.7.a imply $z \in \mathsf{N} \cap \mathsf{F}$, hence $z = 0$ by (a).
(c) First we note that, by the assumption,

$$(x+y) \cdot 0 = x \cdot 0 + y \cdot 0 = x + 0 = x \ . \quad (*)$$

($\Rightarrow$) If $(x+y) \cdot 0 = x + y$ then by $(*)$ $x = x + y$, i.e., $y \leq x$.
($\Leftarrow$) If $y \leq x$ then $x = x + y$ and hence $x + y = x = (x+y) \cdot 0$ by $(*)$. □

5 Separated IL-Semirings

5.1 Motivation

Although our definitions of finite and infinite elements have led to quite a number of useful properties, we are not fully satisfied, since the axiomatisation does not lead to full symmetry of the two notions, whereas in actual computation systems they behave much more symmetrically. Moreover, a number of other desirable properties do not follow from the current axiomatisation either. We list the desiderata:

- While $\mathsf{inf}\, a \overset{\text{def}}{=} a \cdot 0$ gives us the element that contains all the infinite computations of a, we have no corresponding operator fin that sums up the finite computations of a. Next, inf is disjunctive; by symmetry we would expect that for fin as well.
- The set F of finite elements is downward closed, whereas we cannot guarantee that for the set N of infinite elements. However, since $a \leq b$ means that a has at most as many choices as b, one would expect a to be infinite if b is: removing choices between infinite computations should not produce finite computations. Then, except for 0, the finite and infinite elements would lie completely separately.
- Every element should be decomposable into its finite and infinite parts.

The task is now to achieve this without using a too strong restriction on the semiring (such as requiring it to be a distributive or even a Boolean lattice).

5.2 Kernel Operations

To prepare the treatment, we first state a few properties of kernel operations, since taking the finite and infinite parts should both be such operations. The results will be useful for partitioning functions and in connection with tests in a later section.

Definition 5.1 A *kernel* operation is an isotone, contractive and idempotent function $f : K \to K$ from some partial order $(K, \leq)$ into itself. The latter two properties spell out to $f(x) \leq x$ and $f(f(x)) = f(x)$ for all $x \in K$.

Example 5.2 It is straightforward to see that multiplication by an idempotent element below 1 and hence, in particular inf, is a kernel operation. □

It is well-known that the image $f(K)$ of a kernel operation f consists exactly of the fixpoints of f.

Lemma 5.3 *Let $f : K \to K$ be a kernel operation.*

(a) $f(x) = \sqcup\{y \in f(K) : y \leq x\}$*. For the particular case of* inf *this was already shown in Lemma 4.5.(a).*
(b) *If K has a least element* 0 *then* $f(0) = 0$.
(c) *If K is an upper semilattice with supremum operation $+$ then $f(f(x) + f(y)) = f(x) + f(y)$, i.e., $f(K)$ is closed under $+$.*

PROOF.

(a) By the above fixpoint characterisation of $f(K)$ and isotony, $f(x)$ is an upper bound of $S \overset{\text{def}}{=} \{y \in f(K) : y \leq x\}$. But $f(x) \in S$, since $f(x) \leq x$, and so $f(x)$ is the supremum of S.
(b) Immediate from contractivity of f.
(c) $(\leq)$ follows by contractivity of f.
$(\geq)$ By isotony and idempotence of f,

$$f(f(x) + f(y)) \geq f(f(x)) + f(f(y)) = f(x) + f(y) \ .$$

□

Lemma 5.4 *For a kernel operation $f : K \to K$ the following two statements are equivalent:*

(a) *$f(K)$ is downward closed.*

(b) *For all $a, b \in K$ such that $a \sqcap b$ exists, also $f(a) \sqcap b$ and $f(a) \sqcap f(b)$ exist and $f(a \sqcap b) = f(a) \sqcap b = f(a) \sqcap f(b)$.*

PROOF. First we show that the first equation in (b) implies the second one. Assume $f(a \sqcap b) = f(a) \sqcap b$ for all a, b such that $a \sqcap b$ exists. By idempotence of f we get, using this assumption twice,

$$f(a \sqcap b) = f(f(a \sqcap b)) = f(f(a) \sqcap b) = f(a) \sqcap f(b) .$$

($(a) \Rightarrow (b)$) By isotony and contractivity of f we have $f(a \sqcap b) \leq f(b) \leq b$ and $f(a \sqcap b) \leq f(a)$, so that $f(a \sqcap b)$ is a lower bound of $f(a)$ and b. Consider now an arbitrary lower bound c of $f(a)$ and b. By downward closure of $f(K)$ also $c \in f(K)$, i.e., $c = f(c)$. Moreover, $c \leq f(a) \leq a$ by contractivity of f. Therefore $c \leq a \sqcap b$ and hence $c = f(c) \leq f(a \sqcap b)$ by isotony of f, so that $f(a \sqcap b)$ is indeed the greatest lower bound of $f(a)$ and b.

($(b) \Rightarrow (a)$) Consider an $a \in f(K)$ and $b \leq a$, i.e., $b = a \sqcap b$. Then by assumption $f(b) = f(a \sqcap b) = f(a) \sqcap b = a \sqcap b = b$ and hence $b \in f(K)$ as well. □

Corollary 5.5 *Suppose that $f : K \to K$ is a kernel operation and $f(K)$ is downward closed.*

(a) *If $a, b \in K$ with $b \leq a$ then $f(b) = f(a) \sqcap b$.*

(b) *If $f(K)$ has a greatest element z then for all $a \in K$ we have $f(a) = z \sqcap a$.*

(c) *If K is bounded then $f(a) = f(\top) \sqcap a$ for all $a \in K$.*

PROOF.

(a) Immediate from Lemma 5.4.(b).

(b) By contractivity, $f(a) \leq a$. Moreover, $f(a) \leq z$ by $f(a) \in f(K)$. Consider now an arbitrary lower bound c of a and z. By downward closure of $f(K)$ also $c \in f(K)$ and hence $c = f(c)$. But $f(c) \leq f(a)$ by isotony, so that $f(a)$ is indeed the greatest lower bound of a and z.

(c) Immediate from (b), since by isotony $f(\top)$ is the greatest element of $f(K)$. □

5.3 Partitions

We now study the decomposition of elements into well-separated parts. For this, we assume a partial order $(K, \leq)$ that is an upper semilattice with supremum operation $+$ and has a least element 0.

Definition 5.6 A pair of isotone functions $f_1, f_2 : K \to K$ is said to *weakly partition* K if for all $a \in K$ we have

$$f_1(a) + f_2(a) = a \ , \tag{WP1}$$

$$f_1(f_2(a)) = 0 = f_2(f_1(a)) \ . \tag{WP2}$$

Of course, the concept could easily be generalised to systems consisting of more than two functions. Let us prove a few useful consequences of this definition. To ease notation, let f range over f_1, f_2 and set $\tilde{f_1} \stackrel{\text{def}}{=} f_2, \tilde{f_2} \stackrel{\text{def}}{=} f_1$. Note that $\tilde{\tilde{f}} = f$.

Lemma 5.7 *Let f and $\tilde{f}$ weakly partition K.*

(a) *f is a kernel operation.*
(b) *$x \in f(K) \Leftrightarrow x = f(x) \Leftrightarrow \tilde{f}(x) = 0$.*
(c) *The image set $f(K)$ is downward closed.*
(d) *$f(K) \cap \tilde{f}(K) = \{0\}$.*
(e) *For $y \in f(K)$ and $z \in \tilde{f}(K)$ we have $y \sqcap z = 0$. In particular,*

$$\forall\, x \in K \,.\, f(x) \sqcap \tilde{f}(x) = 0 \ .$$

PROOF.

(a) By assumption f is isotone. Moreover, by (WP1) we have $f(x) \leq x$. Idempotence is shown, using (WP1) and (WP2), by

$$f(x) = f(f(x)) + \tilde{f}(f(x)) = f(f(x)) + 0 = f(f(x)) \ .$$

(b) The first equivalence holds, since by (a) f is a kernel operation. For the second one we calculate, using (WP1) and (WP2),

$$x = f(x) \ \Rightarrow\ \tilde{f}(x) = \tilde{f}(f(x)) = 0 \ \Rightarrow\ x = f(x) + \tilde{f}(x) = f(x) \ .$$

(c) Assume $z \leq f(y)$ for some $y \in K$. By isotony of $\tilde{f}$ then $\tilde{f}(z) \leq \tilde{f}(f(y)) = 0$ and hence, again by (b), also $z \in f(K)$.
(d) Assume $x \in f(K) \cap \tilde{f}(K)$. By (b) then $x = f(x)$ and $f(x) = 0$ which shows the claim.
(e) For a lower bound z of $x \in f(K)$ and $y \in \tilde{f}(K)$ we get by (c) and (d) that $z \in f(K) \cap \tilde{f}(K) = \{0\}$. □

The last property means that the f_i decompose every element into two parts that have only a trivial overlap; in other words $f_1(a)$ and $f_2(a)$ have to be relative pseudocomplements of each other.

Although weak partitions already enjoy quite a number of useful properties, they do not guarantee uniqueness of the decomposition. Hence we need the following stronger notion.

Definition 5.8 A pair of functions $f_1, f_2 : K \to K$ is said to *strongly partition K* if they weakly partition K and are disjunctive, i.e., satisfy $f_i(a+b) = f_i(a) + f_i(b)$.

For the next lemma we use again the notational conventions of Lemma 5.7.

Lemma 5.9 *Let $f, \tilde{f} : K \to K$ strongly partition K.*

(a) *$f(\tilde{f}(a) + b) = f(b)$, i.e., $\tilde{f}$-parts of elements are ignored by f.*
(b) *f is uniquely determined by $\tilde{f}$, i.e.*

$$a = \tilde{f}(a) + x \wedge x \in f(K) \Rightarrow x = f(a) \ .$$

PROOF.

(a) By additivity and (WP2),
$f(\tilde{f}(a) + b) = f(\tilde{f}(a)) + f(b) = 0 + f(b) = f(b)$.
(b) By the assumption and (a) we get $f(a) = f(\tilde{f}(a) + x) = f(x) = x$. □

Property (b) is equivalent to additivity in this context: applying(WP1) twice, then (a) twice and then Lemma 5.3.c, we obtain

$$f(a+b) = f(f(a) + \tilde{f}(a) + f(b) + \tilde{f}(b)) = f(f(a) + f(b)) = f(a) + f(b) \ .$$

5.4 Separating Finite and Infinite Elements

Definition 5.10 An IL-semiring K is called *separated* if, in addition to the function $\mathsf{inf} : K \to K$ defined by $\mathsf{inf}\, x \overset{\text{def}}{=} x \cdot 0$, there is a function $\mathsf{fin} : K \to K$ that together with inf strongly partitions K and satisfies $\mathsf{fin}\, K = \mathsf{F}$.

Example 5.11 In [13] the related notion of a *quemiring* is studied, although no motivation in terms of finite and infinite elements is given. A quemiring is axiomatised as a left semiring in which each element a has a unique decomposition $a = a¶ + a \cdot 0$ such that ¶ distributes over + and multiplication by an image under ¶ is also right-distributive. So ¶ corresponds to our fin-operator.

However, the calculation

$$\begin{aligned} a \cdot (b + c) &= (a\P + a \cdot 0) \cdot (b + c) \;=\; a\P \cdot (b + c) + a \cdot 0 \cdot (b + c) \\ &= a\P \cdot b + a\P \cdot c + a \cdot 0 \;=\; a\P \cdot b + a\P \cdot c + a \cdot 0 \cdot b + a \cdot 0 \cdot c \\ &= (a\P + a \cdot 0) \cdot b + (a\P + a \cdot 0) \cdot c \;=\; a \cdot b + a \cdot c \end{aligned}$$

both shows that a quemiring actually is a semiring and hence not too interesting from the perspective of the present paper. □

Example 5.12 Every Boolean IL-semiring K (in particular, WOR(A) and STR(A)) is separated. To see this, we first observe that for arbitrary $b \in K$ the functions

$$f_1(x) \overset{\text{def}}{=} x \sqcap b \;, \qquad f_2(x) \overset{\text{def}}{=} x \sqcap \bar{b} \;,$$

strongly partition K, as is easily checked. In particular, by Lemma 5.7 they are kernel operations and hence satisfy $f_i(x) = f_i(\top) \sqcap x$ by Corollary 5.5.(b).

Choosing now $b = \top \cdot 0$ we obtain $\mathsf{inf}\, x = \top \cdot 0 \sqcap x$. Therefore we define

$$\mathsf{fin}\, x \overset{\text{def}}{=} \overline{\top \cdot 0} \sqcap x \;.$$

Then $\mathsf{fin}\, K = \mathsf{F}$ follows from Lemma 5.7 and $x \in \mathsf{F} \Leftrightarrow \mathsf{inf}\, x = 0$.

It follows that for Boolean K we have

$$x \in \mathsf{N} \Leftrightarrow x \leq \top \cdot 0 \;, \qquad x \in \mathsf{F} \Leftrightarrow x \leq \overline{\top \cdot 0} \;.$$

This was used extensively in [11,12].

For Boolean K we have also

$$\mathsf{inf}\, \top = \mathsf{inf}\, (1 + \bar{1}) = \mathsf{inf}\, 1 + \mathsf{inf}\, \bar{1} = \mathsf{inf}\, \bar{1} \;.$$

□

Example 5.13 Now we give an example of an IL-semiring that is *not* separated. The carrier set is $K = \{0, 1, 2\}$ with natural ordering $0 \leq 1 \leq 2$. Composition is given by the equations

$$0 \cdot x = 0 \;, \qquad 1 \cdot x = x \;, \qquad 2 \cdot x = 2 \;.$$

Then $\mathsf{N} = \{0, 2\}$ and $\mathsf{F} = \{0, 1\}$, so that N is not downward closed as it would need to be by Lemma 5.7 if K were (weakly) separated. □

If K is separated and a complete lattice then, by Tarski's fixpoint theorem, N and F are complete lattices again. By Lemma 4.3.2 and downward closure of

F and N in this case, suprema and hence infima in N and F coincide with the ones in K.

In the presence of a left residual we can give a closed definition of fin.

Lemma 5.14 *Assume an IL-semiring K with a left residuation operation / satisfying the Galois connection*

$$y \leq x/z \Leftrightarrow y \cdot z \leq x \ .$$

(a) $y \in \mathsf{F} \Leftrightarrow y \leq 0/0$. *In particular,* F *has the greatest element* $0/0$.
(b) *If K is separated then* $\mathsf{fin}\, x = x \sqcap 0/0$.

PROOF.

(a) By the definitions, $y \in \mathsf{F} \Leftrightarrow y \cdot 0 \leq 0 \Leftrightarrow y \leq 0/0$.
(b) Immediate from Corollary 5.5.(b). □

We conclude this section by listing a few properties concerning the behaviour of inf and fin w.r.t. composition.

Lemma 5.15 *Assume a separated IL-semiring K.*

(a) $a \cdot b \ = \ \mathsf{inf}\, a + \mathsf{fin}\, a \cdot b$.
(b) $\mathsf{inf}\,(a \cdot b) \ = \ \mathsf{inf}\, a + \mathsf{fin}\, a \cdot \mathsf{inf}\, b$.
(c) $\mathsf{fin}\,(a \cdot b) \ = \ \mathsf{fin}\,(\mathsf{fin}\, a \cdot b) \geq \mathsf{fin}\, a \cdot \mathsf{fin}\, b$. *If K is right-distributive, the latter inequation can be strengthened to an equality.*

PROOF.

(a) $a \cdot b \ = \ (\mathsf{inf}\, a + \mathsf{fin}\, a) \cdot b \ = \ \mathsf{inf}\, a \cdot b + \mathsf{fin}\, a \cdot b \ = \ \mathsf{inf}\, a + \mathsf{fin}\, a \cdot b$.
(b) $\mathsf{inf}\,(a{\cdot}b) \ = \ a{\cdot}b{\cdot}0 \ = \ a{\cdot}\mathsf{inf}\, b \ = \ (\mathsf{inf}\, a{+}\mathsf{fin}\, a){\cdot}\mathsf{inf}\, b \ = \ \mathsf{inf}\, a{\cdot}\mathsf{inf}\, b{+}\mathsf{fin}\, a{\cdot}\mathsf{inf}\, b \ = \ \mathsf{inf}\, a + \mathsf{fin}\, a \cdot \mathsf{inf}\, b$.
(c) By (a), separatedness, Lemma 4.3, Lemma 4.7 and isotony,

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

If K is right-distributive, step four strengthens to an equality. □

6 Iteration — Lazy Kleene and Omega Algebras

The central operation that moves a semiring to a Kleene algebra (KA) [8] is the star that models arbitrary but finite iteration. Fortunately, we can re-use the conventional definition [19] for our setting of IL-semirings. In connection with laziness, the second essential operation is the infinite iteration of an element. While finite iteration suffices for safety analysis of infinite computations [21], infinite iteration is useful for describing liveness aspects (see e.g. [24]). It has been studied intensively in the theory of ω-languages [33]. A recent algebraic account is provided by Cohen's ω-algebras [7] and von Wright's demonic refinement algebra [36,37]. However, both assume right-distributivity, Cohen even right-strictness of composition.

In axiomatising iteration we deal only with iteration "on the left side", since for infinite computations the "right side" is never reached. For infinite iteration this is customary, but it seems only consequent to apply this to finite iteration as well. This is reflected in the following definition.

Definition 6.1 A *left* or *lazy Kleene algebra (LKA)* is a structure $(K, {}^*)$ such that K is an IL-semiring and the *star* * satisfies, for $a, b, c \in K$, the *left unfold* and *left induction laws*

$$1 + a \cdot a^* \;\leq\; a^* \;, \tag{1}$$

$$b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c \;. \tag{2}$$

Hence a^* is the least pre-fixpoint and the least fixpoint of the function $\lambda x \,.\, a \cdot x + b$. Therefore star is isotone with respect to the natural ordering. Even with the left star axioms only we can already show many of the standard laws.

Lemma 6.2 *The following laws hold in an LKA.*

(a) $a \leq a^*$.
(b) $(a^*)^* = a^*$. (Idempotence I)
(c) $a^* \cdot a^* \;=\; a^*$. (Idempotence II)
(d) $(a + b)^* \;=\; a^* \cdot (b \cdot a^*)^*$. (Decomposition)
(e) $a \cdot c \leq c \cdot b \;\Rightarrow\; a^* \cdot c \leq c \cdot b^*$. (Semicommutation)
(f) $a^* \cdot a \leq a \cdot a^*$. (Semi-Selfcommutation I)
(g) $a \cdot (b \cdot a)^* \leq (a \cdot b)^* \cdot a$. (Semi-Sliding I)

PROOF.

(a) By neutrality, isotony and (1), $a = a \cdot 1 \leq a \cdot a^* \leq a^*$.
(b) ($\geq$) follows by (a), while ($\leq$) by (2) reduces to (1).

(c) ($\geq$) follows by $1 \leq a^*$ and isotony. ($\leq$) reduces by (2) to $a^* + a \cdot a^* \leq a^*$, which holds by lattice algebra and (1).

(d) By (c), (b), (1) and isotony we get

$$(a+b)^* \;=\; (a+b)^* \cdot ((a+b)^*)^* \geq a^* \cdot ((a+b) \cdot (a+b)^*)^* \geq a^* \cdot (b \cdot a^*)^* \;.$$

The reverse inequality reduces by (2) to $1+(a+b)\cdot a^* \cdot (b \cdot a^*)^* \leq a^* \cdot (b \cdot a^*)^*$. By (1) and left distributivity of $\cdot$ we are left to show

$$a \cdot a^* \cdot (b \cdot a^*)^* \leq a^* \cdot (b \cdot a^*)^* \;\wedge\; b \cdot a^* \cdot (b \cdot a^*)^* \leq a^* \cdot (b \cdot a^*)^* \;.$$

The first conjunct follows by $a \cdot a^* \leq a \cdot a^*$ and isotony, the second one by $b \cdot a^* \cdot (b \cdot a^*)^* \leq (b \cdot a^*)^*$ as well as $1 \leq a^*$ and isotony.

(e) By (2) the claim reduces to $c + a \cdot c \cdot b^* \leq c \cdot b^*$ and by $1 \leq b^*$ to $a \cdot c \cdot b^* \leq c \cdot b^*$. By the assumption this is implied by $c \cdot b \cdot b^* \leq c \cdot b^*$, which holds by (1) and isotony.

(f) Immediate from (e) by setting $b = c = a$.

(g) By (2) the claim reduces to $a + a \cdot b \cdot a \cdot (b \cdot a)^* \leq a \cdot (b \cdot a)^*$. But this is implied by $1 + b \cdot a \cdot (b \cdot a)^* \leq (b \cdot a)^*$ and isotony. □

The following definition enforces a more symmetric behaviour.

Definition 6.3 An LKA is *strong* if it also satisfies the *right star induction* axiom

$$b + c \cdot a \leq c \;\Rightarrow\; b \cdot a^* \leq c \;. \tag{3}$$

For this we can show

Lemma 6.4 *In a strong LKA we have the following additional laws.*

(a) $a \cdot a^* \leq a^* \cdot a$. (Semi-Selfcommutation II)

(b) $1 + a^* \cdot a \leq a^*$. (Right Star Unfold)
Hence a^* is also the least pre-fixpoint and least fixpoint of the function $\lambda x \,.\, x \cdot a + b$.

(c) $a \cdot (b \cdot a)^* \leq (a \cdot b)^* \cdot a$. (Semi-Sliding II)

PROOF.

(a) By (3) the claim reduces to $a + a^* \cdot a \cdot a \leq a^* \cdot a$ and by $1 \leq a^*$ and isotony further to $a^* \cdot a \leq a^*$. Now we can use Lemma 6.2(f) to reduce this to $a \cdot a^* \leq a^*$ which holds by (1).

(b) This is immediate from (1), since the two semi-selfcommutation laws show $a^* \cdot a = a \cdot a^*$.

(c) Since we have now (b) available, the proof is completely symmetric to that of Lemma 6.2(g). □

Next we note the behaviour of finite elements under the star:

Lemma 6.5 $a \in \mathsf{F} \Leftrightarrow a^* \in \mathsf{F}$.

PROOF. ($\Rightarrow$) By neutrality of 0 we get $a \cdot 0 \leq 0 \Leftrightarrow 0 + a \cdot 0 \leq 0$, so that star induction (2) shows $a^* \cdot 0 \leq 0$.
($\Leftarrow$) This follows by Lemma 6.2(a) and downward closure of F. □

We now turn to infinite iteration.

Definition 6.6 A *lazy omega algebra*, briefly an *ω-LKA*, is a structure $(K, {}^\omega)$ consisting of an LKA K and a unary *omega* operation ${}^\omega$ that satisfies, for $a, b, c \in K$, the *unfold* and *coinduction laws*

$$a^\omega = a \cdot a^\omega \ , \tag{4}$$

$$c \leq b + a \cdot c \Rightarrow c \leq a^\omega + a^* \cdot b \ . \tag{5}$$

One may wonder why we did not formulate omega unfold as $a^\omega \leq a \cdot a^\omega$. The reason is that in absence of right-strictness we cannot show the reverse inequation. By the coinduction law, the greatest (post-)fixpoint of $\lambda x \,.\, a \cdot x$ is $a^\omega + a^* \cdot 0$ and $a^* \cdot 0$ need not vanish in the non-strict setting. But by star induction and (4) we can easily show $a^* \cdot 0 \leq a^\omega$ using $a \cdot a^\omega \leq a^\omega$, so that indeed a^ω coincides with the greatest (post-)fixpoint of $\lambda x \,.\, a \cdot x$. The inequation $a^* \cdot 0 \leq a^\omega$ seems natural, since by an easy induction one can show $a^i \cdot 0 \leq a^\omega$ for all $i \in \mathbb{N}$ anyway.

For ease of comparison we note that von Wright's a^ω [36,37] corresponds to $a^* + a^\omega$ in our setting (see [17] for a formal proof).

Some consequences of the axioms are the following.

Lemma 6.7 *Consider an ω-LKA K and an element $a \in K$.*

(a) *K has a greatest element $\top \overset{\text{def}}{=} 1^\omega$.*
(b) *Omega is isotone with respect to the natural ordering.*
(c) $a^* \cdot a^\omega = a^\omega$.
(d) *a^ω is a right ideal, i.e., $a^\omega = a^\omega \cdot \top$.*

PROOF.

(a) This follows from neutrality of 1 and omega coinduction (5).
(b) Immediate from isotony of the fixed point operators.

(c) The inequation $a^* \cdot a^\omega \le a^\omega$ is immediate from the star induction law (2). The reverse inequation follows from $1 \le a^*$ and isotony.

(d) First, by the fixpoint property of a^ω we get $a^\omega \cdot \top = a \cdot a^\omega \cdot \top$. Hence $a^\omega \cdot \top \le a^\omega$. The reverse inequation is immediate from neutrality of 1 and isotony. □

We note that in a separated ω-LKA the set F has the greatest element $\mathsf{fin}\,\top$; this element is sometimes termed "havoc", since it represents the most nondeterministic but always terminating program.

Further laws together with applications to termination analysis can be found in [10]. We conclude this section with some decomposition properties for star and omega.

Lemma 6.8 *Assume a separated ω-LKA K.*

(a) $a^* = (\mathsf{fin}\,a)^* \cdot (1 + \mathsf{inf}\,a)$.

(b) $\mathsf{inf}\,a^* = (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a$.

(c) $a \cdot (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a = (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a$.

(d) $a^\omega = (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a + (\mathsf{fin}\,a)^\omega$.

(e) $\mathsf{fin}\,a = 0 \Rightarrow a^\omega = a$.

PROOF.

(a) $a^* = (\mathsf{fin}\,a + \mathsf{inf}\,a)^* = (\mathsf{fin}\,a)^* \cdot (\mathsf{inf}\,a \cdot (\mathsf{fin}\,a)^*)^* =$

$(\mathsf{fin}\,a)^* \cdot (\mathsf{inf}\,a)^* = (\mathsf{fin}\,a)^* \cdot (1 + \mathsf{inf}\,a \cdot (\mathsf{inf}\,a)^*) = (\mathsf{fin}\,a)^* \cdot (1 + \mathsf{inf}\,a)$.

(b) Using (a) we get

$$a^* \cdot 0 = (\mathsf{fin}\,a)^* \cdot (1 + \mathsf{inf}\,a) \cdot 0 =$$

$$(\mathsf{fin}\,a)^* \cdot (1 \cdot 0 + \mathsf{inf}\,a \cdot 0) = (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a\ .$$

(c) $a \cdot (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a = (\mathsf{fin}\,a + \mathsf{inf}\,a) \cdot (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a =$

$\mathsf{fin}\,a \cdot (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a + \mathsf{inf}\,a \cdot (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a = \mathsf{fin}\,a \cdot (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a + \mathsf{inf}\,a =$

$(\mathsf{fin}\,a \cdot (\mathsf{fin}\,a)^* + 1) \cdot \mathsf{inf}\,a = (\mathsf{fin}\,a)^* \cdot \mathsf{inf}\,a$.

(d) The inequation $\ge$ holds by isotony of omega, by 3 and omega coinduction. The reverse inequation reduces by omega unfold to

$$a^\omega \le (\mathsf{fin}\,a) \cdot a^\omega + \mathsf{inf}\,a \Leftrightarrow a^\omega \le (\mathsf{fin}\,a) \cdot a^\omega + (\mathsf{inf}\,a) \cdot a^\omega \Leftrightarrow$$

$$a^\omega \le (\mathsf{fin}\,a + \mathsf{inf}\,a) \cdot a^\omega \Leftrightarrow a^\omega \le a \cdot a^\omega \Leftrightarrow \text{TRUE}\ .$$

(e) Immediate from (d). □

7 Tests, Domain and Codomain

Tests are the algebraic representation of assertions in programs. Since a statement $\mathsf{assert}\ p$ acts as the identity on all program states that satisfy p and abortion-like on all others, it seems reasonable to model tests by certain elements below 1.

Definition 7.1 A *test* in a left semiring is an element $p \leq 1$ that has a complement q relative to 1, i.e., $p + q = 1$ and $p \cdot q = 0 = q \cdot p$. The set of all tests of a left semiring K is denoted by $\mathsf{test}(K)$. It is not hard to show that $\mathsf{test}(K)$ is closed under $+$ and $\cdot$ and has 0 and 1 as its least and greatest elements. Moreover, the complement $\neg p$ of a test p is uniquely determined by the definition. Hence $\mathsf{test}(K)$ forms a Boolean algebra. If K itself is Boolean then $\mathsf{test}(K)$ coincides with the set of all elements below 1. We will consistently write $a, b, c \ldots$ for arbitrary semiring elements and $p, q, r, \ldots$ for tests. We will also use relative complement $p - q = p \cdot \neg q$ and implication $p \to q = \neg p + q$ with their standard laws.

With the above definition of tests we deviate slightly from [20], in that we do not allow an arbitrary Boolean algebra of subidentities as $\mathsf{test}(K)$ but only the maximal complemented one. The reason is that the axiomatisation of domain to be presented below forces this maximality anyway (see [9]).

In a Kleene/omega algebra, we have for all $p \in \mathsf{test}(K)$ that $p^* = 1$ and $p^\omega = p \cdot \top$.

If the overall IL-semiring K is Boolean, one has $\neg p \overset{\text{def}}{=} \overline{p} \sqcap 1$, where $\overline{a}$ is the complement of a in K. Note that by Lemma 4.7.1 all tests are finite.

Lemma 7.2 *Assume a left semiring K. Then for all $a, b, c \in K$ and all $p, q \in \mathsf{test}(K)$ the following properties hold .*

(a) *If $a \sqcap b$ exists then $p \cdot (a \sqcap b) \ = \ p \cdot a \ \sqcap \ b \ = \ p \cdot a \ \sqcap \ p \cdot b$.*
(b) *$(p \sqcap q) \cdot a \ = \ p \cdot a \ \sqcap \ q \cdot a$.*
(c) *$p \sqcap q \ = \ 0 \ \Rightarrow \ p \cdot a \ \sqcap \ q \cdot a \ = \ 0$.*
(d) *If $b \leq a$ then $p \cdot b \ = \ b \ \sqcap \ p \cdot a$.*
In particular, if K is bounded then $p \cdot b \ = \ b \ \sqcap \ p \cdot \top$.

PROOF. We first note that for any test $p \in \mathsf{test}(K)$ the function $f_p(a) \overset{\text{def}}{=} p{\cdot}a$ is a kernel operation by $p \leq 1$, isotony of $\cdot$ in both arguments and multiplicative idempotence of tests. Next we want to show that $f_p(K)$ is downward closed. Suppose $b \leq p \cdot a$. Then by isotony, $\neg p \cdot b \leq \neg p \cdot p \cdot a = 0$ and hence

$$b = 1 \cdot b = (p + \neg p) \cdot b = p \cdot b + \neg p \cdot b = p \cdot b \ ,$$

i.e., $b = f_p(b) \in f_p(K)$, too.

Now the claims other than (b) follow immediately from Lemma 5.4 and Corollary 5.5. For (b) set $b = a$ and use 1 twice together with $p \sqcap q \;=\; p \cdot q$. $\square$

Let now semiring element a describe an action or abstract program and a test p a proposition or assertion on its states. Then $p \cdot a$ describes a restricted program that acts like a when the initial state satisfies p and aborts otherwise. Symmetrically, $a \cdot p$ describes a restriction of a in its possible final states. By this, p is an *invariant* of a if $p \cdot a = p \cdot a \cdot p$. To exemplify the interplay of tests with infinite iteration we show that an invariant of a will hold throughout the infinite iteration of a if it holds initially:

Lemma 7.3 $p \cdot a = p \cdot a \cdot p \;\Rightarrow\; p \cdot a^\omega \;=\; (p \cdot a)^\omega$.

PROOF. ($\geq$) We do not even need the assumption:

$$(p \cdot a)^\omega = p \cdot a \cdot (p \cdot a)^\omega = p \cdot p \cdot a \cdot (p \cdot a)^\omega = p \cdot (p \cdot a)^\omega \leq p \cdot a^\omega \;.$$

($\leq$) By the fixpoint property of omega and the assumption,

$$p \cdot a^\omega \;=\; p \cdot a \cdot a^\omega \;=\; p \cdot a \cdot p \cdot a^\omega \;,$$

which means that $p \cdot a^\omega$ is a fixpoint of $\lambda x \,.\, p \cdot a \cdot x$ and hence below its greatest fixpoint $(p \cdot a)^\omega$. $\square$

We now introduce an abstract domain operator $\ulcorner$ that assigns to an element the test that describes precisely its possible starting states.

Definition 7.4 A *left semiring with domain* [9] (a left $\ulcorner$-semiring) is a structure $(K, \ulcorner)$, where K is an idempotent semiring and the *domain operation* $\ulcorner\colon K \to \mathsf{test}(K)$ satisfies for all $a, b \in K$ and $p \in \mathsf{test}(K)$

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

If K is an (ω-)LKA, we speak of an *(ω-)LKA with domain.*

These axioms can be understood as follows. (d1), which by isotony can be strengthened to an equality, means that restriction to all *all* starting states is no actual restriction, whereas (d2) means that after restriction the remaining starting states should satisfy the restricting test. (d3), which again can be strengthened to an equality, states that the domain of $a \cdot b$ is not determined by the inner structure or the final states of b; information about ${\ulcorner}b$ in interaction with a suffices.

To further explain (d1) and (d2) we note that, as shown in [9], their conjunction is equivalent to each of

$$\ulcorner a \le p \Leftrightarrow a \le p \cdot a\ , \qquad \text{(llp)} \qquad \ulcorner a \le p \Leftrightarrow \neg p \cdot a \le 0\ . \qquad \text{(gla)}$$

(llp) says that $\ulcorner a$ is the least left preserver of a. (gla) says that $\neg\ulcorner a$ is the greatest left annihilator of a. By Boolean algebra (gla) is equivalent to

$$p \cdot \ulcorner a \le 0 \Leftrightarrow p \cdot a \le 0\ .$$

Because of (llp), domain is uniquely characterised by the axioms.

Although the axioms are the same as in [9], one has to check whether their consequences in KA can still be proved in LKA. Fortunately, this is the case.

Lemma 7.5 *Let K be a left domain semiring. The following laws hold for $a, b \in K$ and $p \in \mathsf{test}(K)$.*

(a) *Domain is isotone.*
(b) *Domain preserves arbitrary existing suprema. In particular, $\ulcorner 0 = 0$ and $\ulcorner(a+b) = \ulcorner a + \ulcorner a$.*
(c) $\ulcorner a \le 0 \Leftrightarrow a \le 0$. (Full Strictness)
(d) $\ulcorner p = p$. (Stability)
(e) $\ulcorner(p \cdot a) = p \cdot \ulcorner(a)$. (Import/Export)
(f) $\ulcorner(a \cdot b) \le \ulcorner a$.
(g) *If K is bounded then $\ulcorner(a \cdot \top) = \ulcorner a$.*
(h) $\ulcorner(a \cdot p) \le p \Rightarrow \ulcorner(a^* \cdot p) \le p$. (Induction)

PROOF. We use the proof principles of indirect (in)equality:

$$x \le y \;\Leftrightarrow\; \forall\, z\,.\, y \le z \Rightarrow x \le z\ ,$$
$$x = y \;\Leftrightarrow\; \forall\, z\,.\, y \le z \Leftrightarrow x \le z\ .$$

(a) Suppose $a \le b$. Then by (gla) and isotony we have for all $q \in \mathsf{test}(K)$

$$\ulcorner b \le q \Leftrightarrow \neg q \cdot b \le 0 \Rightarrow \neg q \cdot a \le 0 \Leftrightarrow \ulcorner a \le q\ .$$

(b) The proof has been given in [25]; it only uses (llp) and isotony of domain, which has been shown in (a).
(c) ($\Leftarrow$) is part of (b).
($\Rightarrow$) By (d1), $a \le \ulcorner a \cdot a = 0 \cdot a = 0$.
(d) for all $q \in \mathsf{test}(K)$ we have by (llp) and the properties of infimum (which coincides with $\cdot$ on tests) that

$$\ulcorner p \le q \Leftrightarrow p \le p \cdot q \Leftrightarrow p \le q\ ,$$

so that indirect equality shows the claim.

(e) By (d3) and (d),

$$\ulcorner(p \cdot a) = \ulcorner(p \cdot \ulcorner a) = p \cdot \ulcorner a \ .$$

(f) Using (llp) and isotony we get

$$\ulcorner a \le p \ \Leftrightarrow\ a \le p \cdot a \ \Rightarrow\ a \cdot b \le p \cdot a \cdot b \ \Leftrightarrow\ \ulcorner(a \cdot b) \le p \ ,$$

and the claim follows by indirect inequality.

(g) The inequation $\le$ follows from (f), whereas $\ge$ follows from $1 \le \top$ and isotony.

(h) This can be proved as in [9] (the LKA does not even need to be strong). □

We now turn to the dual case of the codomain operation. In the KA case where we have also right-distributivity, a codomain operation $^{\urcorner}$ can easily be defined as a domain operation in the opposite semiring where, as usual in algebra, opposition just swaps the order of composition. But by lack of right distributivity this does not work in the LKA setting; we additionally have to postulate isotony of codomain (in the form of superdisjunctivity to have a purely equational axiom).

Definition 7.6 A *left semiring with codomain* (a $^{\urcorner}$-semiring) is a structure $(K, {}^{\urcorner})$, where K is a left semiring and the *codomain operation* $^{\urcorner} : K \to \mathsf{test}(K)$ satisfies, for all $a, b \in K$ and $p \in \mathsf{test}(K)$,

$$a \le a \cdot a^{\urcorner} \ , \qquad \text{(cd1)} \qquad\qquad (a \cdot p)^{\urcorner} \le p \ , \qquad \text{(cd2)}$$

$$(a^{\urcorner} \cdot b)^{\urcorner} \le (ab)^{\urcorner} \ , \qquad \text{(cd3)} \qquad\qquad (a + b)^{\urcorner} \ge a^{\urcorner} + b^{\urcorner} \ . \qquad \text{(cd4)}$$

If K is an LKA, we speak of an *LKA with codomain.*

As for domain, the conjunction of (cd1) and (cd2) is equivalent to

$$a^{\urcorner} \le p \ \Leftrightarrow\ a \le ap \ , \qquad \text{(lrp)}$$

i.e., $a^{\urcorner}$ is the least right preserver of a. However, by lack of right-strictness, $\neg(a^{\urcorner})$ need not be the greatest right annihilator of a; (lrp) only *implies*

$$a^{\urcorner} \le p \ \Leftrightarrow\ a \cdot \neg p \le a \cdot 0 \ . \qquad \text{(wgra)}$$

The reverse implication (wgra) $\Rightarrow$ (lrp) holds in presence of *weak right-distributivity*

$$a = a \cdot p + a \cdot \neg p \qquad \text{(wrd)}$$

and provided a is finite. Note that (wrd) holds automatically for all $a \in \mathsf{N}$. Moreover, (wrd) is equivalent to full right-distributivity over sums of tests:

assuming (wrd), we calculate

$$\begin{aligned} a \cdot (p+q) &= a \cdot (p+q) \cdot p + a \cdot (p+q) \cdot \neg p \\ &= a \cdot (p \cdot p + q \cdot p) + a \cdot (p \cdot \neg p + q \cdot \neg p) \\ &= a \cdot p + a \cdot q \cdot \neg p \;\leq\; a \cdot p + a \cdot q \ . \end{aligned}$$

The reverse inequation follows from isotony and superdisjunctivity. We will not assume (wrd) in the sequel, though.

In an LKA, the symmetry between domain and codomain is broken also in other respects. The analogue of Lemma 7.5(c) does not hold; rather we have

Lemma 7.7 $a^{\urcorner} = 0 \Leftrightarrow a \in \mathsf{N}$.

PROOF. Recall that $a \in \mathsf{N} \Leftrightarrow a = a \cdot 0$. Now, by (cd1), $a^{\urcorner} = 0$ implies $a = a \cdot 0$, whereas the reverse implication is shown by (cd2). □

However, since for domain the proof of preservation of suprema only involves isotony and (llp), we can carry it over to codomain and obtain

Lemma 7.8 *Codomain is universally disjunctive and hence, in particular, additive and strict.*

Also, the proof of stability of domain uses only (llp) and hence is also valid for the codomain case, so that $p^{\urcorner} = p$ for all $p \in \mathsf{test}(K)$. The import/export law $(a \cdot p)^{\urcorner} = a^{\urcorner} \cdot p$ follows from (cd3) and stability. Finally,

Lemma 7.9 *In a domain/codomain LKA,* $a^{\urcorner} \cdot {}^{\ulcorner}b = 0 \;\Rightarrow\; a \cdot b = a \cdot 0$.

Further properties of domain and codomain can be found in [9].

8 Modal LKAs

Definition 8.1 A *modal left semiring* is a left semiring K with domain and codomain. If K in addition is an LKA, we call it a *modal LKA*.

Let K be a modal left semiring. We introduce forward and backward diamond operators via abstract preimage and image.

$$|a\rangle p = {}^{\ulcorner}(a \cdot p) \ , \qquad (6) \qquad\qquad \langle a| p = (p \cdot a)^{\urcorner} \ , \qquad (7)$$

for all $a \in K$ and $p \in \mathsf{test}(K)$. The box operators are, as usual, the de Morgan duals of the diamonds:

$$|a]p = \neg|a\rangle\neg p \;, \tag{8}$$

$$[a|p = \neg\langle a|\neg p \;. \tag{9}$$

If $a \in \mathsf{N}$ then these definitions specialise to

$$|a\rangle p = \ulcorner a \;, \tag{10}$$

$$\langle a|p = 0 \;, \tag{11}$$

$$|a]p = \neg\ulcorner a \;, \tag{12}$$

$$[a|p = 1 \;, \tag{13}$$

since then also $p \cdot a \in \mathsf{N}$ by Lemma 4.3.(a)

In the KA case, diamonds and boxes satisfy an *exchange law*. Let us work out the meaning of the two formulas involved in that law. Using the definitions, Boolean algebra and (gla)/(wgra), we obtain

$$p \le |a]q \;\Leftrightarrow\; p \le \neg\ulcorner(a \cdot \neg q) \;\Leftrightarrow\; \ulcorner(a \cdot \neg q) \le \neg p \;\Leftrightarrow\; p \cdot a \cdot \neg q \le 0$$

and

$$\langle a|p \le q \;\Leftrightarrow\; (p \cdot a)\urcorner \le q \;\Leftrightarrow\; p \cdot a \cdot \neg q \le a \cdot 0 \;.$$

So for finite a we regain the Galois connection

$$p \le |a]q \;\Leftrightarrow\; \langle a|p \le q \;,$$

which, however, does not hold for $a \in \mathsf{N}$. By an analogous argument one can show that also

$$p \le [a|q \;\Leftrightarrow\; |a\rangle p \le q$$

holds when $a \in \mathsf{F}$.

The Galois connections have interesting consequences. In particular diamonds (boxes) of finite elements commute with all existing suprema (infima) of the test algebra.

Since for tests p the forward and backward modalities coincide, we will use the notation $\langle p\rangle$ and $[p]$ for these. Then

$$\langle p\rangle q = p \cdot q \;, \qquad [p]q = p \to q \;.$$

Hence, $\langle 1\rangle = [1]$ is the identity function on tests. Moreover, $\langle 0\rangle p = 0$ and $[0]p = 1$.

By left-distributivity, the forward modalities distribute over $+$ as follows:

$$|a+b\rangle p \;=\; |a\rangle p + |b\rangle p \;, \qquad |a+b]p \;=\; (|a]p) \cdot (|b]p) \;.$$

Hence, in a separated semiring we obtain

$$|a\rangle p = |\mathsf{fin}\,a\rangle p + \ulcorner(\mathsf{inf}\,a) \;, \qquad |a]p = |\mathsf{fin}\,a]p - \ulcorner(\mathsf{inf}\,a) \;.$$

Using the forward box we can give another characterisation of finite elements:

Lemma 8.2 $a \in \mathsf{F} \Leftrightarrow |a]1 = 1$.

PROOF. By the definitions, $|a]1 = \neg\ulcorner(a \cdot 0)$. Now
$a \in \mathsf{F} \Leftrightarrow a \cdot 0 = 0 \Leftrightarrow \ulcorner(a \cdot 0) = 0 \Leftrightarrow \neg\ulcorner(a \cdot 0) = 1 \Leftrightarrow |a]1 = 1$. □

Further applications of modal operators, notably for expressing Noethericity and performing termination analysis, can be found in [10].

9 Predicate Transformer Algebras

Assume a left semiring $(K, +, \cdot, 0, 1)$. By a *predicate transformer* we mean a function $f : \mathsf{test}(K) \to \mathsf{test}(K)$. It is *disjunctive* if $f(p + q) = f(p) + f(q)$ and *conjunctive* if $f(p \cdot q) = f(p) \cdot f(q)$. It is *strict* if $f(0) = 0$. Finally, *id* is the identity transformer and $\circ$ denotes function composition.

Let P be the set of *all* predicate transformers, M the set of isotone and D the set of strict and disjunctive ones. Under the pointwise ordering $f \leq g \overset{\text{def}}{\Leftrightarrow} \forall\, p \,.\, f(p) \leq g(p)$, P forms a lattice where the supremum $f + g$ and infimum $f \sqcap g$ of f and g are the pointwise liftings of $+$ and $\cdot$, resp.:

$$(f + g)(p) \overset{\text{def}}{=} f(p) + g(p) \ , \qquad (f \sqcap g)(p) \overset{\text{def}}{=} f(p) \cdot g(p) \ .$$

The least element of P (and M and D) is the constant 0-valued function $\mathbf{0}$. The substructure $(M, +, \mathbf{0}, \circ, id)$ is an IL-semiring. In fact, $\circ$ is even universally left-disjunctive and preserves all existing infima, as the following calculation and a dual one for infima show:

$$((\bigsqcup F) \circ g)(x) = (\bigsqcup F)(g(x)) = \bigsqcup F(g(x) = \bigsqcup (F \circ g)(x) \ .$$

The modal operator $|\_\rangle$ provides a left semiring homomorphism from K into M.

The substructure $(D, +, \mathbf{0}, \circ, id)$ is even an idempotent semiring.

If $\mathsf{test}(K)$ is a complete Boolean algebra then P is a complete lattice with M and D as complete sublattices. Hence we can extend M and D by a star operation via a least fixpoint definition:

$$f^* \overset{\text{def}}{=} \mu g \,.\, id + f \circ g \ ,$$

where μ is the least-fixpoint operator.

Using μ-subfusion (see below) one sees that by this definition M becomes an LKA which is even strong.

Similarly, if $\mathsf{test}(K)$ is complete we can define the infinite iteration as

$$f^\omega \stackrel{\text{def}}{=} \nu g \,.\, f \circ g \ ,$$

where ν is the greatest-fixpoint operator. Whereas in M this does not imply the omega coinduction law, it does so in D.

By passing to the mirror ordering, we see that also the subalgebra of universally conjunctive predicate transformers can be made into a strong ω-LKA; this is essentially the approach taken in [36,37].

As a sample proof we show that the omega coinduction law holds for disjunctive predicate transformers. First we briefly repeat the fixpoint fusion laws (see e.g. [3] for further fixpoint properties). Let $F, G, H : L \to L$ be isotone functions on a complete lattice $(L, \leq)$ with least element $\perp$ and greatest element $\top$. Suppose that G is continuous, i.e., preserves suprema of nonempty chains, and assume $G(\perp) \leq \mu H$. Then

$$G \circ H \leq F \circ G \Rightarrow G(\mu H) \leq \mu F \ . \qquad (\mu\text{-subfusion})$$

Suppose now dually that G is cocontinuous, i.e., preserves infima of nonempty chains, and assume $G(\top) \geq \mu H$. Then

$$G \circ H \geq F \circ G \Rightarrow G(\nu H) \geq \nu F \ . \qquad (\nu\text{-superfusion})$$

For the proof of omega coinduction we define

$$\begin{aligned} F(x) &\stackrel{\text{def}}{=} f \circ x + g \ , \\ G(x) &\stackrel{\text{def}}{=} x + f^* \circ g = x + \mu F \ , \\ H(x) &\stackrel{\text{def}}{=} f \circ x \ , \end{aligned}$$

where x ranges over D. Since we have assumed $\mathsf{test}(K)$ to be complete, $+$ is universally disjunctive in both arguments, so that G is continuous. The coinduction law is implied by $\nu F \leq G(\nu H)$, which by ν-superfusion reduces to $G \circ H \geq F \circ G$. This is shown by

$$\begin{aligned} G(H(x)) &= f \circ x + \mu F \ = \ f \circ x + F(\mu F) \ = \ f \circ x + f \circ \mu F + g \\ &= f \circ (x + \mu F) + g \ = \ f \circ G(x) + g \ = \ F(G(x)) \ . \end{aligned}$$

Note that this calculation uses finite, but not universal, disjunctivity of f in an essential way. For the subclass of universally disjunctive predicate transformers over a power set lattice the result is well-known, since they are isomorphic to relations [2].

It should also be mentioned that the treatment, of course, generalises to functions $f : L \to L$ over an arbitrary complete lattice L.

10 Conclusion and Outlook

We have seen that it is possible to integrate non-strictness with finite and infinite iteration as well as with modal operators. This framework allows, for instance, an abstract and more concise reworking of the stream applications treated in [24]; this will be the subject of further papers. Let us briefly sketch two other interesting applications of the theory.

The paper [26] presents an algebraic demonic semantics based on [28,29]. The basic idea is to start from a modal semiring K and to model a command as a pair (a, p) where $a \in K$ abstracts the transition relation between states and the test p characterises the set of states from which no divergence is possible.

The essential program constructors are the following:

- Demonic composition: $(a, p) \,;\, (b, q) \stackrel{\text{def}}{=} (a \cdot b,\ p \cdot (|a]q))$.
- Demonic choice: $(a, p) \bigsqcap (b, q) \stackrel{\text{def}}{=} (a + b,\ p \cdot q)$.
- Angelic choice: $(a, p) \bigsqcup (b, q) \stackrel{\text{def}}{=} (a + b,\ p + q)$.

Then ; is associative, has left annihilator $(0, 0)$, neutral element $(1, 1)$ and distributes through $\bigsqcap$. Both choices are idempotent and associative and distribute over each other. The natural order associated with $\bigsqcap$ is the refinement order

$$(a, p) \sqsupseteq (b, q) \ \stackrel{\text{def}}{\Leftrightarrow}\ (a, p) \bigsqcap (b, q) = (b, q) \ \Leftrightarrow\ a \le b \wedge p \ge q .$$

Both choice operators are isotone w.r.t. $\sqsupseteq$.

Parnas's [29] requires the pairs (a, p) to satisfy the restriction $p \le \ulcorner a$; thus the "must-termination" given by p is distinguished from the "may-termination" given by $\ulcorner a$. However, "miraculous" program behaviour is excluded, and so there is no neutral element w.r.t. $\bigsqcap$, since the obvious candidate $(0, 1)$ does not satisfy the restriction. So we do not have a full semiring structure.

In Nelson's approach [28] this restriction is dropped, allowing miraculous programs like the pair $\mathsf{fail} = (0, 1)$ that is guaranteed to terminate for all input states but at the same time never yields any output state. Now one obtains a left semiring that is even right-distributive. In fact, it can be made into a left domain semiring in which, perhaps surprisingly, the forward box coincides with the wp-operator, while the forward box in the underlying modal semiring K of course corresponds to wlp. If K is even a Kleene or omega algebra, the command semiring can be made into a left Kleene or omega algebra; this also reflects the results of the previous section. Then the do od and if fi commands receive pleasing algebraic semantics. For full details we have to refer to [26].

More recently, this approach has been extended in [14] to give an algebraic semantics of the sequential fragment of Hoare and He's Unifying Theories of Programming [15]. A second line of investigation extends von Wright's demonic refinement algebra by a domain operation analogous to ours for predicate transformers [34].

The second application, given in [16], concerns reactive and hybrid systems. While the words in $\mathrm{STR}(A)$ (see Sect. 3) can be viewed as computation sequences over discrete time, one can, as is well known, also define finite and infinite traces over continuous time and consider processes as sets of trajectories (see e.g. [32]). Defining a suitable generalisation of the fusion product, one can make this structure into another left quantale with domain and hence even into a left omega algebra. This can then be exploited to define and analyse reactive and hybrid systems as infinite iterations of interacting basic components, similarly to Back's action systems [1]. Again we have to refer to the original paper [16] for details.

These examples provide convincing evidence that the theory of lazy Kleene and omega algebras will have many other interesting and useful applications. Especially the connection to process algebras deserves extensive further investigation.

Acknowledgements: I am grateful to J. Desharnais, T. Ehm, W. Guttmann, P. Höfner, D. Kozen, D. Naumann, K. Solin, G. Struth and W. Vogler for valuable discussions and support, and to Z. Esik for pointing out reference [13]. The anonymous referee provided very helpful comments on the relation to process algebra.

References

[1] R. Back, K. Sere: Stepwise refinement of action systems. Structured Programming 12, 17–30 (1991)

[2] R. Back, J. von Wright: Refinement calculus — a systematic introduction. Springer 1998

[3] R. C. Backhouse et al.: Fixed point calculus. Inform. Proc. Letters, 53:131–136 (1995)

[4] J.A. Bergstra, I. Bethke, A. Ponse: Process algebra with iteration and nesting. The Computer Journal 37(4), 243–258 (1994)

[5] J.A. Bergstra, W. Fokkink, A. Ponse: Process algebra with recursive operations. In [6], 333–389

[6] J.A. Bergstra, S. Smolka, A. Ponse: Handbook of process algebra. North-Holland 2001

[7] E. Cohen: Separation and reduction. In R. Backhouse and J.N. Oliveira (eds.): Mathematics of Program Construction. LNCS 1837. Springer 2000, 45–59

[8] J.H. Conway: Regular algebra and finite machines. London: Chapman and Hall 1971

[9] J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM Transactions on Computational Logic (to appear)

[10] J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, and J. Mitchell, editors, Exploring new frontiers of theoretical informatics. IFIP International Federation for Information Processing Series 155. Kluwer 2004, 653–666

[11] R.M. Dijkstra: Computation calculus — bridging a formalisation gap. In: J. Jeuring (ed.): Proc. MPC 1998. LNCS 1422. Springer 1998, 151–174

[12] R.M. Dijkstra: Computation calculus bridging a formalisation gap. Science of Computer Programming 37, 3-36 (2000)

[13] C.C. Elgot: Matricial theories. Journal of Algebra 42, 391–422 (1976)

[14] W. Guttmann, B. Möller: Modal design algebra. In S. Dunne, B. Stoddart (eds.): Proc. First International Symposium on Unifying Theories of Programming. LNCS 4010. Springer 2006, 236–256

[15] C.A.R. Hoare, J. He: Unifying theories of programming. Prentice Hall 1998

[16] P. Höfner, B. Möller: Towards an algebra of hybrid systems. In W. MacCaull, M. Winter and I. Düntsch (eds.): Relational Methods in Computer Science. LNCS 3929. Springer 2006, 121–133

[17] P. Höfner, B. Möller, K. Solin: Omega algebra, demonic refinement algebra and commands. In: R. Schmidt, G. Struth (eds.): Relations and Kleene algebra in computer science. LNCS. Springer 2006 (to appear)

[18] B. von Karger, C.A.R. Hoare: Sequential calculus. Information Processing Letters 53, 123–130 (1995)

[19] D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation 110, 366–390 (1994)

[20] D. Kozen: Kleene algebras with tests. ACM TOPLAS 19, 427–443 (1997)

[21] D. Kozen: Kleene Algebra with Tests and the Static Analysis of Programs. Cornell University, Department of Computer Science, Technical Report TR2003-1915, 2003

[22] J.J. Lukkien: An operational semantics for the guarded command language. In: R.S. Bird, C.C. Morgan, J.C.P. Woodcock (eds.): Mathematics of Program Construction. LNCS 669. Springer 1993, 233–249

[23] J.J. Lukkien: Operational semantics and generalised weakest preconditions. Science of Computer Programming 22, 137–155 (1994)

[24] B. Möller: Ideal stream algebra. In: B. Möller, J.V. Tucker (eds.): Prospects for hardware foundations. LNCS 1546. Springer 1998, 69–116

[25] B. Möller, G. Struth: Modal Kleene algebra and partial correctness. In C. Rattray, S. Maharaj, C. Shankland (eds.): Algebraic methodology and software technology. LNCS 3116. Springer 2004, 379–393. Revised and extended version: B. Möller, G. Struth: Algebras of modal operators and partial correctness. Theoretical Computer Science 351, 221–239 (2006)

[26] B. Möller, G. Struth: wp is wlp. In W. MacCaull, M. Winter, I. Düntsch (eds.): Relational methods in computer Science. LNCS 3929. Springer 2006, 200-211

[27] B.C. Moszkowski: A complete axiomatisation of interval temporal logic with infinite time. Proc. 15th LICS. IEEE 2000, 241–252

[28] G. Nelson: A generalisation of Dijkstra's calculus. ACM Transactions on Programming Languages and Systems 11, 517–561 (1989)

[29] D. Parnas: A generalised control structure and its formal definition. Commun. ACM 26, 572–581 (1983)

[30] D. Park. Concurrency and automata on infinite sequences. Proc. 5th GI-Conference on Theoretical Computer Science, LNCS 104. Springer 1981, 167–183

[31] K.I. Rosenthal: Quantales and their applications. Pitman Research Notes in Mathematics Series, Vol. 234. Longman Scientific&Technical 1990

[32] M. Sintzoff: Iterative synthesis of control guards ensuring invariance and inevitability in discrete-decision games. In O. Owe, S. Krogdahl, and T. Lyche (eds.): From object-orientation to formal methods, Essays in memory of Ole-Johan Dahl. LNCS 2635. Springer 2004, 272–301

[33] L. Staiger: Omega languages. In G. Rozenberg, A. Salomaa (eds.): Handbook of formal languages, Vol. 3. Springer 1997, 339–387

[34] K. Solin and J. von Wright: Refinement algebra with operators for enabledness and termination. In T. Uustalu (ed.): Mathematics of Program Construction. LNCS 4014. Springer 2006, 397–415

[35] R. van Glabbeek: The linear time — branching time spectrum I. The semantics of concrete, sequential processes. In [6], 3–99

[36] J. von Wright: From Kleene algebra to refinement algebra. In E. Boiten, B. Möller (eds.): Mathematics of Program Construction. LNCS 2386. Springer 2002, 233–262

[37] J. von Wright: Towards a refinement algebra. Science of Computer Programming 51, 23–45 (2004)