Lazy Kleene Algebra

Bernhard Möller

Institut für Informatik, Universität Augsburg
Universitätsstr. 14, D-86135 Augsburg, Germany
moeller@informatik.uni-augsburg.de

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. Finally, it is shown that predicate transformers form lazy Kleene algebras again, the disjunctive and conjunctive ones even lazy Kleene algebras with an omega operation.

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 coincides 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 $\bot$ 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 lazy computation systems in which e.g. infinite sequences of states may occur. 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 [15, 16] or R. Dijkstra's computation calculus [8, 9]. 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 [10]. In addition, we integrate the theory with Cohen's ω-algebra [4] and von Wright's demonic refinement algebra [21, 22].

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 isotonicity 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 [11].

2 Left Semirings

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

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

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

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 $a \leq b \stackrel{\text{def}}{\Leftrightarrow} a + b = b$.

Note that left-isotonicity of $\cdot$ follows from its left-distributivity. Moreover, 0 is the least element w.r.t. the natural order. The left semiring structure without the requirement of right-isotonicity is also at the core of process algebra frameworks (see e.g. [3]) where δ (inaction) plays the rôle of 0. Since, however, we will make essential use of right-isotonicity, only few of our results will carry over to that setting.

By isotonicity, $\cdot$ is universally superdisjunctive and universally subconjunctive in both arguments; we state these properties for the right argument:

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

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*

$$b + c \leq d \;\Rightarrow\; a \cdot b + a \cdot c \leq a \cdot d \;. \tag{1}$$

Proof. By isotonicity 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 1. 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.
2. An IL-semiring $(K, +, 0, \cdot, 1)$ is *bounded* if K has a greatest element $\top$ w.r.t. the natural order. It is *complete* if the semilattice $(K, \leq)$ is a complete lattice and $\cdot$ is universally left-disjunctive.
3. 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 look at the composition from the other end.

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 $x \breve{\cdot} y = y \cdot x$. 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 *complete* 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*. The notions of a *complete* and *Boolean* (I-)semiring are defined analogously. A complete I-semiring is also called a *standard Kleene algebra* [5] or a *quantale* [19].

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 our two main models of the notion of IL-semiring. Both of them 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. Then, 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 $A^\infty \stackrel{\text{def}}{=} A^* \cup A^\omega$. The length of word s is denoted by $|s|$. By $\bullet$ we denote concatenation, where $s \bullet t \stackrel{\text{def}}{=} s$ 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

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

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

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

Note that in general $S \bullet T \neq \{s \bullet t : s \in S \wedge t \in T\}$; using the set on the right hand side as the definition of $S \bullet T$ one would obtain a right-strict operation. With the definition given, we have $S \bullet \emptyset = \mathsf{inf}\, S$ and hence $S \bullet \emptyset = \emptyset$ iff $\mathsf{inf}\, S = \emptyset$. It is straightforward to show that WOR is an IL-semiring. The algebra is well-known from the classical theory of ω-languages (see e.g. [20] for a recent 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 For words $s, t \in A^\infty$ we define their *join* or *fusion product* $s \bowtie t$ as a language-valued operation:

$$s \bowtie t \stackrel{\text{def}}{=} \begin{cases} s & \text{if } |s| = \infty \ , \\ \mathit{init}(s) \bullet (\mathit{last}(s) \cap \mathit{head}(t)) \bullet \mathit{tail}(t) & \text{otherwise} \ , \end{cases}$$

where $\mathit{head}(\varepsilon) \stackrel{\text{def}}{=} \mathit{tail}(\varepsilon) \stackrel{\text{def}}{=} \mathit{init}(\varepsilon) \stackrel{\text{def}}{=} \mathit{last}(\varepsilon) \stackrel{\text{def}}{=} \varepsilon$, viewed as a singleton language.

The definition entails $\varepsilon \bowtie \varepsilon = \varepsilon$ and $s \bowtie t = \emptyset$ when $\mathit{last}(s) \neq \mathit{head}(t)$, i.e., 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 model based on this composition operation STR.

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

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

Analogously to 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 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 [15, 16] and Dijkstra [8, 9].

Both WOR and STR are even Boolean IL-semirings. 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 which does not make any progress and hence may also be viewed as never terminating.

As we are interested in treating finite and infinite computations uniformly, we need to characterize these notions algebraically. 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. We write temporal succession from left to right, i.e., $a \cdot b$ means "first perform computation a and then b". Therefore we give the following

Definition 4.1 Consider an IL-semiring $(K, +, 0, \cdot, 1)$. An element $a \in K$ is called *non-terminating* or *infinite* if it is a left zero w.r.t. composition, i.e., if

$$\forall\, b \in K : a \cdot b = a\ .$$

The set of all non-terminating elements is denoted by N.

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

Lemma 4.2 $a \in \mathsf{N} \Leftrightarrow a \cdot 0 = a$.

Proof. ($\Rightarrow$) Choose $b = 0$ in the definition of N.
($\Leftarrow$) Using the assumption, associativity, left strictness and the assumption again, we calculate $a \cdot b = a \cdot 0 \cdot b = a \cdot 0 = a$. □

By this characterization 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.*

1. *An arbitrary computation followed by a non-terminating one is non-terminating, i.e., $K \cdot \mathsf{N} \subseteq \mathsf{N}$ (and hence $K \cdot \mathsf{N} = \mathsf{N}$).*
2. *If $\cdot$ is universally left-disjunctive then N is closed under $\sqcup$.*

Proof. 1. 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 $1 \in K$.
2. Consider $L \subseteq \mathsf{N}$ such that $\sqcup L$ exists. Then, by the assumptions, $(\sqcup L) \cdot 0 = \sqcup (L \cdot 0) = \sqcup L$. □

So the supremum in N coincides with the one in the overall algebra K.

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

Lemma 4.4 *The following properties are equivalent:*

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

Proof. $(1 \Rightarrow 2)$ It follows that $\mathsf{N} = \{0\}$.
$(2 \Rightarrow 3)$ Since $0 \in \mathsf{N}$ and $\top \cdot 0 \in \mathsf{N}$ we get $\top \cdot 0 = 0$.
$(3 \Rightarrow 1)$ For arbitrary $a \in K$ we have, by isotonicity, $a \cdot 0 \leq \top \cdot 0 = 0$. □

Next we show

Lemma 4.5 *1.* $\mathsf{N} = \{a \cdot 0 : a \in K\}$.

2. $b \cdot 0$ *is the greatest element of* $\mathsf{N}(b) \stackrel{\text{def}}{=} \{a \in \mathsf{N} : a \leq b\}$.
3. *If K is bounded then* $\top \cdot 0$ *is the greatest element of* N. *In particular,* $\top \cdot 0 = \bigsqcup \mathsf{N}$.
4. *If* N *is downward closed and* $\top \in \mathsf{N}$ *then* $1 = 0$ *and hence* $|K| = 1$.

Proof. 1. $(\subseteq)$ Immediate from the definition of N.
$(\supseteq)$ Assume $z = a \cdot 0$. Then $z \cdot 0 = a \cdot 0 \cdot 0 = a \cdot 0 = z$.

2. First, assume $a \in \mathsf{N} \wedge a \leq b$. Then by right-isotonicity 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 1. we have $b \cdot 0 \in \mathsf{N}$. By right-neutrality of 1 and isotonicity we get $b \cdot 0 \leq b \cdot 1 = b$, i.e., $b \cdot 0 \in \mathsf{N}(b)$, which shows the claim.
3. Immediate from 2.
4. By downward closure, $1 \in \mathsf{N}$, hence $1 = 1 \cdot 0 = 0$ by neutrality of 1. □

Property 3 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 [8, 9], where $\top \cdot 0$ is called the eternal part of K. 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 3 we may call $b \cdot 0$ the *non-terminating* or *infinite part* of b. This leads to the following

Definition 4.6 We call an element a *finite* if its infinite part is trivial, i.e., if $a \cdot 0 = 0$. The set of all finite elements is denoted by F. By this definition $0 \in \mathsf{F}$. To mirror our operational understanding we call an element a *terminating* if a is finite and $a \neq 0$. We set $\mathsf{T} \stackrel{\text{def}}{=} \mathsf{F} - \{0\}$.

A number of properties of F and T are collected in

Lemma 4.7 *1.* F *is downward closed.*

2. $1 \in \mathsf{F}$. *If* $1 \neq 0$ *then* $1 \in \mathsf{T}$ *(*skip *is terminating).*
3. *For non-empty* $S \subseteq K$ *we have* $S \subseteq \mathsf{F} \Leftrightarrow S \cdot \{0\} = \{0\}$.
4. $K \cdot \mathsf{F} = K = \mathsf{F} \cdot K$.

5. $\mathsf{F} + \mathsf{F} \subseteq \mathsf{F}$ *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 joins and* T *under non-empty ones.*
6. $\mathsf{F} \cdot \mathsf{F} \subseteq \mathsf{F}$ *(finite computations are closed under composition). By neutrality of* 1 *we have even equality.* T *need not be closed under composition.*

Proof. 1. Immediate from isotonicity.
2. Immediate from left-neutrality of 1.
3. Immediate from the definition of F.
4. 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.
5. Immediate from distributivity/disjunctivity.
6. By 2. we have $\mathsf{F} \cdot \mathsf{F} \cdot \{0\} = \mathsf{F} \cdot \{0\} = \{0\}$, and 2. again shows the claim. □

Notation. Although we do not assume a general meet operation $\sqcap$, we will sometimes use the formula $y \sqcap z = 0$; it is an abbreviation for $\forall\, u\,.\; u \leq y \wedge u \leq z \Rightarrow u = 0$.

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

Lemma 4.8 *1.* $\mathsf{N} \cap \mathsf{F} = \{0\}$.
2. *If* N *is downward closed, then for* $x \in \mathsf{N}$ *and* $y \in \mathsf{F}$ *we have* $x \sqcap y = 0$.
3. *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. 1. If $x \in \mathsf{N} \cap \mathsf{F}$ then $x = x \cdot 0 = 0$.
2. Suppose $z \leq x \wedge z \leq y$ for some $z \in K$. Then the assumption and Lemma 4.7.1 imply $z \in \mathsf{N} \cap \mathsf{F}$, hence $z = 0$ by 1.
3. 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 nonterminating elements have led to quite a number of useful properties, we are not fully satisfied, since the axiomatization 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 axiomatization either. We list the desiderata:

- While $\mathsf{inf}\, a \stackrel{\text{def}}{=} a \cdot 0$ gives us the nonterminating part of a, we have no corresponding operator fin that yields the finite part 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 nonterminating elements. However, since $a \leq b$ means that a has at most as many choices as b, one would expect a to be nonterminating if b is: removing choices between infinite computations should not produce finite computations. Then, except for 0, the finite and nonterminating elements would lie completely separately.
- Every element should be decomposable into its finite and nonterminating part.

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 that will be useful both for partitioning functions and in connection with tests in the next 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 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.*

1. $f(x) = \sqcup \{y \in f(K) : y \leq x\}$.
2. *If K has a least element 0 then* $f(0) = 0$.
3. *If K is an upper semilattice with join operation $+$ then* $f(f(x) + f(y)) = f(x) + f(y)$, *i.e., $f(K)$ is closed under $+$.*

Proof. 1. By isotonicity and the above fixpoint property, $f(x)$ is an upper bound of $S \stackrel{\text{def}}{=} \{y \in f(K) : y \leq x\}$. But $f(x) \in S$, since $f(x) \leq x$, and so $f(x)$ is the supremum of S.
2. Immediate from contractivity of f.
3. ($\leq$) follows by contractivity of f.
($\geq$) By isotonicity 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:*

1. *$f(K)$ is downward closed.*
2. *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 2. implies the second one. Assume $f(a \sqcap b) = f(a) \sqcap b$ for all a, b such that $a \sqcap b$ exists. Then by idempotence of f we get, using this assumption twice,

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

(1. $\Rightarrow$ 2.) By isotonicity and contractivity of f we have $f(a \sqcap b) \leq f(b) \leq b$ and $f(a \sqcap b) \leq f(a)$. Consider now an arbitrary lower bound c for $f(a)$ and b. Then 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 isotonicity of f.

(2. $\Rightarrow$ 1.) 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.*

1. *If $a, b \in K$ with $b \leq a$ then $f(b) = f(a) \sqcap b$.*
2. *If K is bounded then $f(a) = a \sqcap f(\top)$ for all $a \in K$.*

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 join operation $+$ and a least element 0.

Definition 5.6 Consider a pair of isotone functions $f_1, f_2 : K \to K$. 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 $\tilde{\tilde{f}} = f$. The pair is said to *weakly partition* K if for all $a \in K$ we have

$$f(a) + \tilde{f}(a) = a \ , \qquad \text{(WP1)} \qquad\qquad \tilde{f}(f(a)) = 0 \ . \qquad \text{(WP2)}$$

Of course, the concept could easily be generalized to systems consisting of more than two functions. Let us prove a few useful consequences of this definition. Note that by our notational convention also $f(\tilde{f}(a)) = 0$.

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

1. *f is a kernel operation.*
2. *$x \in f(K) \Leftrightarrow x = f(x) \Leftrightarrow \tilde{f}(x) = 0$.*
3. *The image set $f(K)$ is downward closed.*

4. $f(K) \cap \tilde{f}(K) = \{0\}$.
5. *For $y \in f(K)$ and $z \in \tilde{f}(K)$ we have $y \sqcap z = 0$. In particular, $f(x) \sqcap \tilde{f}(x) = 0$ for all $x \in K$.*

Proof. 1. By assumption f is isotone. Moreover, by (WP1) we have $f(x) \leq x$. Idempotence is shown, using (WP1) and (WP2), by

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

2. The first equivalence holds, since by 1. f is a kernel operation. For the second one we calculate, using (WP1) and (WP2),

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

3. Assume $z \leq f(y)$ for some $y \in K$. By isotonicity of $\tilde{f}$ then $\tilde{f}(z) \leq \tilde{f}(f(y)) = 0$ and hence, again by 2., also $z \in f(K)$.
4. Assume $x \in f(K) \cap \tilde{f}(K)$. By 2. then $x = f(x)$ and $f(x) = 0$ which shows the claim.
5. For a lower bound z of $x \in f(K)$ and $y \in \tilde{f}(K)$ we get by 3. and 4. 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 additive, i.e., satisfy $f_i(a+b) = f_i(a)+f_i(b)$.

Lemma 5.9 *Let $f_1, f_2 : K \to K$ strongly partition K.*

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

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

Proof. 1. By additivity and (WP2),
$f(\tilde{f}(a) + b) = f(\tilde{f}(a)) + f(b) = 0 + f(b) = f(b)$.
2. By the assumption and 1. we get $f(a) = f(x + \tilde{f}(a)) = f(x) = x$. □

Property 2. is equivalent to additivity in this context: applying(WP1) twice, then 1. twice and then Lemma 5.3.3, 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 $\mathsf{inf}\, x \stackrel{\text{def}}{=} x \cdot 0$, 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 [10] the related notion of *quemiring* is studied, although no motivation in terms of finite and infinite elements is given. A quemiring is axiomatized as a left semiring in which each element a has a unique decomposition $a = a\P + a \cdot 0$ such that $\P$ distributes over $+$ and multiplication by an image under $\P$ is also right-distributive. So $\P$ corresponds to our fin-operator. However, the calculation

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

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 (and hence, in particular, WOR and STR) is separated. To see this, we first observe that for arbitrary $b \in K$ the functions

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

strongly partition K, as is easily checked. In particular, by Lemma 5.7 they are kernel operations and hence satisfy $f_i(x) = x \sqcap f_i(\top)$ by Corollary 5.5.2.

Choosing now $b = \top \cdot 0$ we obtain $\mathsf{inf}\, x = x \sqcap T \cdot 0$. Therefore we define $\mathsf{fin}\, x \stackrel{\text{def}}{=} x \sqcap \overline{\top \cdot 0}$. 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 [8, 9].

For Boolean K we have also

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

□

Example 5.13 Now we give an example of an IL-semiring that is *not* separable. 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) separable. □

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*

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

If K is separated then $\mathsf{fin}\, x = x \sqcap 0/0$.

Proof. By separation and Lemma 5.3.1, $\mathsf{fin}\, x = \bigsqcup \{y \in \mathsf{F} : y \leq x\}$. Therefore, by downward closure of F

$$y \leq \mathsf{fin}\, x \Leftrightarrow y \in \mathsf{F} \wedge y \leq x \Leftrightarrow y \cdot 0 \leq 0 \wedge y \leq x \Leftrightarrow y \leq 0/0 \wedge y \leq x \ .$$

Now the claim follows by the universal characterization of meet. □

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.*

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

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

2. $\mathsf{inf}\,(a \cdot b) = a \cdot b \cdot 0 = a \cdot \mathsf{inf}\, b = (\mathsf{inf}\, a + \mathsf{fin}\, a) \cdot \mathsf{inf}\, b = \mathsf{inf}\, a \cdot \mathsf{inf}\, b + \mathsf{fin}\, a \cdot \mathsf{inf}\, b = \mathsf{inf}\, a + \mathsf{fin}\, a \cdot \mathsf{inf}\, b$.

3. By 1. and isotonicity,

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

If K is right-distributive, the fourth step and hence the whole calculation can be strengthened to equalities. □

6 Iteration — Lazy Kleene algebras

The central operation that moves a semiring to a Kleene algebra (KA) [5] is the star that models arbitrary but finite iteration. Fortunately, we can re-use the conventional definition [12] for our setting of IL-semirings. In connection with laziness, the second essential operation is the infinite iteration of an element. This has been studied intensively in the theory of ω-languages [20]. A recent algebraic account is provided by Cohen's ω-algebras [4] and von Wright's demonic refinement algebra [21, 22]. However, both assume right-distributivity, Cohen even right-strictness of composition. While safety analysis of infinite computations is also possible using star only [14], omega iteration serves to describe liveness aspects (see e.g. [17]).

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 *unfold* and *induction laws*

$$1 + a \cdot a^* \leq a^* \ , \qquad (2) \qquad b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c \ . \qquad (3)$$

An LKA is *strong* if it also satisfies the symmetrical star induction law

$$b + c \cdot a \leq c \Rightarrow b \cdot a^* \leq c \ . \qquad (4)$$

Therefore, a^* is the least pre-fixpoint and the least fixpoint of the function $\lambda x \,.\, a \cdot x + b$. Star is isotone with respect to the natural ordering. Even the weak star axioms suffice to prove the following laws:

$$\begin{array}{ll} a^* \cdot a^* = a^* \ , & \text{(idempotence)} \\ (a+b)^* = a^* \cdot (a \cdot b^*)^* \ , & \text{(decomposition)} \\ a \cdot c \leq c \cdot b \Rightarrow a^* \cdot c \leq c \cdot b^* \ . & \text{(semicommutation)} \end{array}$$

In a strong LKA the star also satisfies the symmetrical star unfold axiom

$$1 + a^* \cdot a \leq a^* \qquad (5)$$

and hence is the least pre-fixpoint and least fixpoint of the function $\lambda x \,.\, x \cdot a + b$.

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

Lemma 6.2 $a \in \mathsf{F} \Rightarrow a^* \in \mathsf{F}$.

Proof. By neutrality of 0 we get $a \cdot 0 \leq 0 \Leftrightarrow a \cdot 0 + 0 \leq 0$, so that star induction (3) shows $a^* \cdot 0 \leq 0$. □

We now turn to infinite iteration.

Definition 6.3 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*

$$a^\omega = a \cdot a^\omega \ , \qquad (6)$$

$$c \leq a \cdot c + b \Rightarrow c \leq a^\omega + a^* \cdot b \ . \qquad (7)$$

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. This may seem paradoxical now. But by star induction 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 corresponds to $a^* + a^\omega$ in our setting.

Some consequences of the axioms are the following.

Lemma 6.4 *Consider an ω-LKA K and an element $a \in K$.*

1. *K has a greatest element $\top \stackrel{\text{def}}{=} 1^\omega$.*
2. *Omega is isotone with respect to the natural ordering.*
3. *$a^* \cdot a^\omega = a^\omega$.*
4. *a^ω is a right ideal, i.e., $a^\omega \cdot \top = \top$.*

Proof. 1. This follows from neutrality of 1 and omega coinduction (7).
2. Immediate from isotonicity of the fixed point operators.
3. The inequation $a^* \cdot a^\omega \leq a^\omega$ is immediate from the star induction law (3). The reverse inequation follows from $1 \leq a^*$ and isotonicity.
4. First, by the fixpoint property of a^ω we get $a^\omega \cdot \top = a \cdot a^\omega \cdot \top$. Hence $a^\omega \cdot \top \leq a^\omega$. The reverse inequation is immediate from neutrality of 1 and isotonicity. □

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 [7]. We conclude this section with some decomposition properties for star and omega.

Lemma 6.5 *Assume a separated ω-LKA K.*

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

Proof.
1. $a^* = (\mathsf{fin}\, a + \mathsf{inf}\, a)^* = (\mathsf{fin}\, a)^* \cdot (\mathsf{inf}\, a \cdot (\mathsf{fin}\, a)^*)^* =$
   $(\mathsf{fin}\, a)^* \cdot (\mathsf{inf}\, a)^* = (\mathsf{fin}\, a)^* \cdot (1 + \mathsf{inf}\, a \cdot (\mathsf{inf}\, a)^*) = (\mathsf{fin}\, a)^* \cdot (1 + \mathsf{inf}\, a)$.
2. Using 1. we get
   $a^* \cdot 0 = (\mathsf{fin}\, a)^* \cdot (1 + \mathsf{inf}\, a) \cdot 0 =$
   $(\mathsf{fin}\, a)^* \cdot (1 \cdot 0 + \mathsf{inf}\, a \cdot 0) = (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a$.
3. $a \cdot (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a = (\mathsf{fin}\, a + \mathsf{inf}\, a) \cdot (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a =$
   $\mathsf{fin}\, a \cdot (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a + \mathsf{inf}\, a \cdot (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a = \mathsf{fin}\, a \cdot (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a + \mathsf{inf}\, a =$
   $(\mathsf{fin}\, a \cdot (\mathsf{fin}\, a)^* + 1) \cdot \mathsf{inf}\, a = (\mathsf{fin}\, a)^* \cdot \mathsf{inf}\, a$.
4. The inequation $\geq$ holds by isotonicity of omega, by 3 and omega coinduction. The reverse inequation reduces by omega unfold to
   $a^\omega \leq (\mathsf{fin}\, a) \cdot a^\omega + \mathsf{inf}\, a \Leftrightarrow a^\omega \leq (\mathsf{fin}\, a) \cdot a^\omega + (\mathsf{inf}\, a) \cdot a^\omega \Leftrightarrow$
   $a^\omega \leq (\mathsf{fin}\, a + \mathsf{inf}\, a) \cdot a^\omega \Leftrightarrow a^\omega \leq a \cdot a^\omega \Leftrightarrow$ TRUE . □

7 Tests, Domain and Codomain

Definition 7.1 1. A *left test semiring* is a two-sorted structure $(K, \mathsf{test}(K))$, where K is an IL-semiring and $\mathsf{test}(K) \subseteq K$ is a Boolean algebra embedded

into K, such that the join and meet operations of $\mathsf{test}(K)$ coincide with the restrictions of $+$ and $\cdot$ of K to $\mathsf{test}(K)$, respectively, and such that 0 and 1 are the least and greatest elements of $\mathsf{test}(K)$. In particular, $p \leq 1$ for all $p \in \mathsf{test}(K)$. But in general, $\mathsf{test}(K)$ is only a subalgebra of the subalgebra of all elements below 1 in K. The symbol $\neg$ denotes complementation in $\mathsf{test}(K)$.
2. A *lazy Kleene algebra with tests* is a left test semiring (K, B) such that K is a lazy KA.

This definition generalizes the one in [13]. We will consistently use the letters $a, b, c \ldots$ for semiring elements and $p, q, r, \ldots$ for Boolean elements. We will also use relative complement $p - q = p \cdot \neg q$ and implication $p \to q = \neg p + q$ with their standard laws. For all $p \in \mathsf{test}(K)$ we have that $p^* = 1$ and $p^\omega = p \cdot \top$.

If the overall IL-semiring K is Boolean, one can always choose $\mathsf{test}(K) = \{p \,|\, p \leq 1\}$ as the set of tests and define $\neg p \stackrel{\text{def}}{=} \overline{p} \sqcap 1$, where $\overline{a}$ is the complement of element a in the overall algebra. Note that by Lemma 4.7.1 all tests are finite.

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

1. *If $a \sqcap b$ exists then $p \cdot (a \sqcap b) = p \cdot a \sqcap b = p \cdot a \sqcap p \cdot b$.*
2. *$(p \sqcap q) \cdot a = p \cdot a \sqcap q \cdot a$.*
3. *$p \sqcap q = 0 \Rightarrow p \cdot a \sqcap q \cdot a = 0$.*
4. *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 $f_p(a) \stackrel{\text{def}}{=} p \cdot a$ is a kernel operation by $p \leq 1$, isotonicity 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 isotonicity, $\neg p \cdot b \leq \neg p \cdot p \cdot a = 0$ 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 2. follow immediately from Lemma 5.4 and Corollary 5.5. For 2. set $b = a$ and use 1 twice together with $p \sqcap q = p \cdot q$. □

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.

To show the interplay of tests with infinite iteration we prove a simple invariance property:

Lemma 7.3 *$p \cdot a = p \cdot a \cdot p \Rightarrow p \cdot a^\omega = (p \cdot a)^\omega$. This means that an invariant of a will hold throughout the infinite iteration of a.*

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 $(p \cdot a)^\omega$. □

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

Definition 7.4 A *semiring with domain* [6] (a $\ulcorner$-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 $p \in \mathsf{test}(K)$

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

If K is an LKA, we speak of an *LKA with domain*, briefly *$\ulcorner$-LKA*.

These axioms can be understood as follows. (d1), which by isotonicity 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) 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 their conjunction is equivalent to each of

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

(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

$$p \cdot \ulcorner a \leq 0 \;\Leftrightarrow\; p \cdot a \leq 0 \;.$$

Because of (llp), domain is uniquely characterized by the axioms. Moreover, if $\mathsf{test}(K)$ is complete then domain always exists. If $\mathsf{test}(K)$ is not complete, this need not be the case.

Although the axioms are the same as in [6], one has to check whether their consequences in KA can still be proved in LKA. Fortunately, this is the case. Right-distributivity was used in [6] only for the proofs of additivity and the import/export law $\ulcorner(pa) = p\ulcorner a$. But the latter follows from (d3) and stability $\ulcorner p = p$ (which, in turn, follows from (llp) and idempotence of tests). Additivity is a special case of

Lemma 7.5 *Domain is universally disjunctive. In particular,* $\ulcorner 0 = 0$.

The proof has been given in [18]; it only uses (llp) and isotonicity of domain. But the latter follows easily from (gla).

From (d1) and left strictness of composition we also get

$$\ulcorner a = 0 \Rightarrow a = 0 \ . \tag{8}$$

Two other useful properties are

Lemma 7.6 *1.* $\ulcorner(a \cdot b) \leq \ulcorner a$.
2. If K *is bounded then* $\ulcorner(a \cdot \top) = \ulcorner a$.

Proof. 1. Using (llp) we get

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

and the claim follows by indirect inequality, i.e., by

$$x \leq y \Leftrightarrow \forall\, z \,.\, y \leq z \Rightarrow x \leq z \ .$$

2. The inequation $\leq$ follows from 1., whereas $\geq$ follows from $1 \leq \top$ and isotonicity. □

Finally, the induction law $\ulcorner(ap) \leq p \Rightarrow \ulcorner(a^* p) \leq p$ can be proved as in [6] (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 isotonicity of codomain (in the form of superdisjunctivity to have a purely equational axiom).

Definition 7.7 A *left semiring with codomain* (a $^\urcorner$-semiring) is a structure $(K, ^\urcorner)$, where K is a left test semiring and the *codomain operation* $^\urcorner : K \to \mathsf{test}(K)$ satisfies, for all $a, b \in K$ and $p \in \mathsf{test}(K)$,

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

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

If K is an LKA, we speak of an *LKA with codomain*, briefly $^\urcorner$*-LKA*.

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

$$a^\urcorner \leq p \Leftrightarrow a \leq ap \ , \tag{lrp}$$

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

$$a^\urcorner \leq p \Leftrightarrow a \cdot \neg p \leq a \cdot 0 \ . \tag{wgra}$$

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

$$a = a \cdot p + a \cdot \neg p \tag{wrd}$$

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

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

The reverse inequation follows from monotonicity 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 (8) does not hold; rather we have

Lemma 7.8 $a^{\urcorner} = 0 \;\Leftrightarrow\; a \in \mathsf{N}$.

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 isotonicity and (llp), we can carry it over to codomain and obtain

Lemma 7.9 *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 7.10 *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 [6].

8 Modal LKAs

Definition 8.1 A *modal left semiring* is a left test 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.

$$|a\rangle p = {}^{\ulcorner}(a \cdot p) \;, \tag{9}$$

$$\langle a| p = (p \cdot a)^{\urcorner} \;, \tag{10}$$

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

$$|a]p = \neg|a\rangle\neg p \ , \qquad (11) \qquad\qquad [a|p = \neg\langle a|\neg p \ . \qquad (12)$$

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

$$|a\rangle p = \ulcorner a \ , \qquad (13) \qquad\qquad \langle a|p = 0 \ , \qquad (14)$$

$$|a]p = \neg\ulcorner a \ , \qquad (15) \qquad\qquad [a|p = 1 \ , \qquad (16)$$

since then also $p \cdot a \in \mathsf{N}$ by Lemma 4.3.1.

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

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

and

$$\langle a|p \leq q \ \Leftrightarrow \ (p \cdot a)^{\urcorner} \leq q \ \Leftrightarrow \ p \cdot a \cdot \neg q \leq a \cdot 0 \ .$$

So for finite a we regain the Galois connection

$$p \leq |a]q \ \Leftrightarrow \ \langle a|p \leq q \ ,$$

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

$$p \leq [a|q \ \Leftrightarrow \ |a\rangle p \leq q$$

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.

In the sequel, when the direction of diamonds and boxes does not matter, we will use the notation $\langle a\rangle$ and $[a]$. For a test p the modal operators satisfy $\langle p\rangle q = p \cdot q$ and $[p]q = p \rightarrow q$. Hence, $\langle 1\rangle = [1]$ is the identity function on tests. Moreover, $\langle 0\rangle p = 0$ and $[0]p = 1$. Finally, in an LKA with converse $^{\smile}$ we have $|a^{\smile}\rangle = \langle a|$ and $|a^{\smile}] = [a|$.

By left-distributivity, the forward modalities distribute over $+$ in the following way:

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

Hence, in a separated test semiring we obtain

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

Using the forward box we can give another characterization 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 [7].

9 Predicate Transformer Algebras

Assume a left test 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 $f \leq g \stackrel{\text{def}}{\Leftrightarrow} \forall\, p \,.\, f(p) \leq g(p)$, 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.:

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

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:

$$((\sqcup F) \circ g)(x) = (\sqcup F)(g(x)) = \sqcup F(g(x) = \sqcup (F \circ g)(x) \;.$$

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:

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

where μ is the least-fixpoint operator.

Using μ-subfusion (see below) one sees that by this definition M becomes an LKA which, however, is not strong. Only the subalgebra of universally disjunctive predicate transformers is strong.

Similarly, if $\mathsf{test}(K)$ is complete we can define the infinite iteration $f^\omega \stackrel{\text{def}}{=} \nu g \,.\, f \circ g$, where ν is the greatest-fixpoint operator. Whereas in M this does not imply the omega coinduction law, it does so in D.

Combining these two observations, we conclude that only the subalgebra of universally disjunctive predicate transformers can be made into an ω-LKA (which is even strong).

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 [21, 22].

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. [2] for further fixpoint properties). Let $F, G, H : L \to L$ be isotone functions on a complete lattice $(L, \leq)$ with least element $\bot$ and greatest element

$\top$. Suppose that G is continuous, i.e., preserves suprema of nonempty chains, and assume $G(\bot) \leq \mu H$. 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 $F(x) \stackrel{\text{def}}{=} f \circ x + g$ and $G(x) \stackrel{\text{def}}{=} x + f^* \circ g = x + \mu F$ and $H(x) \stackrel{\text{def}}{=} f \circ x$, 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

$$G(H(x)) = f \circ x + \mu F = f \circ x + F(\mu F) = f \circ x + f \circ \mu F + g = \\ f \circ (x + \mu F) + g = f \circ G(x) + g = F(G(x)) \ .$$

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 [1].

It should also be mentioned that the treatment, of course, generalizes 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 [17]; this will be the subject of further papers. But hopefully the framework will have many more applications.

Acknowledgements: I am grateful to J. Desharnais, T. Ehm, D. Kozen, D, Naumann and G. Struth for valuable discussions and support, and to Z. Esik for pointing out reference [10].

References

1. R. Back, J. von Wright: Refinement calculus — a systematic introduction. Springer 1998
2. R. C. Backhouse et al.: Fixed point calculus. *Inform. Proc. Letters*, 53:131–136, 1995.
3. J.A. Bergstra, I. Bethke, A. Ponse: Process algebra with iteration and nesting. The Computer Journal 37(4), 243–258, 1994

4. E. Cohen: Separation and reduction. In R. Backhouse and J.N. Oliveira (eds.): Mathematics of Program Construction. Lecture Notes in Computer Science **1837**. Berlin: Springer 2000, 45–59
5. J.H. Conway: Regular algebra and finite machines. London: Chapman and Hall 1971
6. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. Technical Report 2003-07, Universität Augsburg, Institut für Informatik, June 2003
7. J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. Technical Report 2004-04, Universität Augsburg, Institut für Informatik, January 2004. Revised version: Proc. IFIP World Computer Congress 2004, Toulouse, August 22–27, 2004, Subconference TCS-Logic (to appear)
8. R.M. Dijkstra: Computation calculus — bridging a formalization gap. In: J. Jeuring (ed.): Proc. MPC 1998. LNCS 1422, 151–174
9. R.M. Dijkstra: Computation calculus bridging a formalization gap. Science of Computer Programming **37**, 3-36 (2000)
10. C.C. Elgot: Matricial theories. Journal of Algebra **42**, 391–422 (1976)
11. B. von Karger, C.A.R. Hoare: *Sequential calculus*. Information Processing Letters **53**, 1995, 123–130
12. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation **110:2**, 366–390 (1994)
13. D. Kozen: Kleene algebras with tests. *ACM TOPLAS* 19:427–443, 1997.
14. D. Kozen: Kleene Algebra with Tests and the Static Analysis of Programs. Cornell University, Department of Computer Science, Technical Report TR2003-1915, 2003
15. 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. Lecture Notes in Computer Science **669**. Berlin: Springer 1993, 233–249
16. J.J. Lukkien: Operational semantics and generalized weakest preconditions. Science of Computer Programming **22**, 137–155 (1994)
17. B. Möller: Ideal stream algebra. In: B. Möller, J.V. Tucker (eds.): Prospects for hardware foundations. Lecture Notes in Computer Science **1546**. Berlin: Springer 1998, 69–116
18. B. Möller, G. Struth: Modal Kleene algebra and partial correctness. Technical Report 2003-08, Universität Augsburg, Institut für Informatik, May 2003. Revised version: Proc. AMAST 2004, Stirling, July 12–16, 2004 (to appear)
19. K.I. Rosenthal: *Quantales and their applications*. Pitman Research Notes in Mathematics Series, Vol. 234. Longman Scientific&Technical 1990.
20. L. Staiger: Omega languages. In G. Rozenberg, A. Salomaa (eds.): Handbook of formal languages, Vol. 3. Springer 1997, 339–387
21. J. von Wright: From Kleene algebra to refinement algebra. In E. Boiten, B. Möller (eds.): Mathematics of Program Construction. Lecture Notes in Computer Science **2386**. Berlin: Springer 2002, 233–262
22. J. von Wright: Towards a refinement algebra. Science of Computer Programming **51**, 23–45 (2004)