Kleene Algebra with Domain and Kleene Modules

K. Kazemian*

Department of Mathematics
Cornell University, Ithaca, USA

Contents

*Email addresses: kk983@cornell.edu

1 Kleene Algebra with Domain

We assume the definitions of a Kleene Algebra (KA), Kleene Algebra with Tests(KAT) and an idempotent semiring (i-semiring). The class of idempotent semirings is denoted by IS. Clearly, every i-semiring is a semilattice with respect to the natural ordering with least element 0 and addition as join. Thus,

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

A lattice-ordered monoid (an l-monoid) is a structure $(A, +, \wedge, ., 1)$, such that $(A, +, \wedge)$ is a lattice, $(A, ., 1)$ is a monoid and left and right multiplication are additive. An l-monoid is bounded if it has a least element 0 and a greatest element 1. A d-monoid and a b-monoid, respectively, is an l-monoid whose lattice reduct is distributive and Boolean.

1.1 Subidentities and KAT

An element a of an i-semiring A is a *subidentity* if $a \leq 1$. We denote the set of subidentities of A by $sid(A)$.

Properties. *We observe that:*

- *The set of subidentities of an i-semiring forms an i-semiring.*
- *Multiplication of subidentities in IS is a lower bound operation.*
- *Multiplication of subidentities in IS (in d-monoids) is not always idempotent.*
- *The set of multiplicatively idempotent subidentities of an i-semiring forms a bounded distributive lattice.*

we say that a test-semiring (a t-semiring) is an i-semiring A with a distinguished Boolean subalgebra $test(A)$ of $sid(A)$ with greatest element 1 and least element 0. We call $test(A)$ the test algebra of A. We denote the class of t-semirings by TS. A t-semiring is a KAT when the t-semiring is a KA.

1.1.1 tests in b-monoids

if A is a b-monoid since for each $a \in A$ a complement of a is uniquely defined, complements in $sid(A)$ can be defined as restrictions of complements in A, i.e. as $\bar{p} := 1 \wedge \bar{p}$ with abuse of notation for simplicity.

Observation. *$sid(A)$ is a Boolean subalgebra of A.*

1.2 Domain

In order to motivate our definitions, recall $REL(A)$, the relational KA over A. Let $R \subseteq A \times A$ for some set A. Then the domain of R represented as a binary relation is the set

$$\delta(R) = \{(a, a) \in A \times A | \exists b \in A \text{ s.t. } (a, b) \in R\}$$

Definition 1.1. *A Kleene algebra with domain is a structure (K, δ), where $K \in KAT$ and the domain operation $\delta : K \to test(K)$ satisfies, for all $a, b \in K$ and $p \in test(K)$,*

$$a \leq \delta(a)a \quad (1a) \qquad \delta(pa) \leq p \quad (1b) \qquad \delta(a\delta(b)) \leq \delta(ab) \quad (1c)$$

KAD denotes the class of Kleene algebras with domain. The impact of (1a) and (1b) can be motivated as follows. (1a) is equivalent to one implication in each of the statements.

$$\delta(a) \leq p \Leftrightarrow a \leq pa \qquad (2a) \qquad\qquad \delta(a) \leq p \Leftrightarrow pa \leq 0 \qquad (2b)$$

which constitute elimination laws for δ. (1b) is equivalent to the other implications. (2a) says that $\delta(a)$ is the least left preserver of a. (2b) says that $\delta(a)$ is the greatest left annihilator of a.

now we present details:

1.2.1 Preservers and Annihiliators

We say that b left-preserves a if $a \leq ba$, and that a is left-stable under b if $ba \leq a$. The concepts of right-preservation and right-stability are defined in a similar way. We say that a is a left annihilator of b if $ab = 0$, and a right annihilator if $ba = 0$. These concepts are useful in particular when $a \in sid(A)$. Note that every element of A is left- and right-invariant under 1 and that 0 is a left and right annihilator of every element of A.

Properties. *We observe the following:*

- *Let $A \in IS$. For all $a, b \in A$, the element $f(a)$ is the least left- preserver of a iff*

$$f(a) \leq b \Leftrightarrow a \leq ba$$

- *In IS,*
  (i) least left preservers are subidentities
  (ii) least left preservers are multiplicatively idempotent
  (iii) the set of least left preservers is a bounded distributive lattice with least element 0*, greatest element* 1*, addition as join and multiplication as meet operation.*

- *Let $A \in TS$. For every $a \in A$ and $p \in test(A)$, $f(a)$ is the greatest left-annihilator of a iff* (2b) *holds.*

- *Let $A \in TS$. For all $a \in A$, let $f(a)$ be the least left-preserver of a in A and let $g(a)$ be the greatest left-annihilator of a in A, Then $f(a) = g(a)'$.*

1.2.2 Predomain

Definition 1.2. *A structure (A, δ) is a t-semiring with predomain (a δ-semiring) if $A \in TS$ and the predomain operation $\delta : A \rightarrow test(A)$ satisfies* (2a)*.*

The class of t-semirings with predomain is denoted by TSP.

Theorem 1.1. *TSP is precisely the class of TS where each $A \in TSP$ is enriched by a mapping $\delta : A \rightarrow test(A)$ that satisfies, for all $a \in A$ and $p \in test(A)$, the two equations* (1a) *and* (1b)*.*

Properties. *Let $A \in TSP$. Let $a, b \in A$, $p \in test(A)$ and $q \in sid(A)$.*

(i) *δ is fully strict.* $\delta(a) \leq 0 \Leftrightarrow a \leq 0$

(ii) *δ is additive.* $\delta(a + b) = \delta(a) + \delta(b)$

(iii) *δ is monotonic.* $a \leq b \Rightarrow \delta(a) \leq \delta(b)$

(iv) *δ is an identity on tests.* $\delta(p) = p$

(v) δ *is idempotent.* $\delta(\delta(a)) = \delta(a)$

(vi) δ *yields a left invariant.* $a = \delta(a)a$

(vii) δ *satisfies an import/export law.* $\delta(pa) = p\delta(a)$

(viii) δ *satisfies a decomposition law.* $\delta(ab) \leq \delta(a\delta(b))$

(ix) δ *commutes with the complement operation on tests.* $\delta(p)' = \delta(p')$

1.2.3 Locality and Domain

Definition 1.3. *A t-semiring with domain ($\hat{\delta}$-semiring) is a δ-semiring in which the predomain operation* $\delta : A \to test(A)$ *also satisfies* (1c)*.*

In analogy to the definition of an integral domain in ring theory, we say that a semiring A is integral if it has no zero divisors, i.e. $ab \leq 0 \Rightarrow a \leq 0 \vee b \leq 0$ holds for all $a, b \in A$.

Observation. *Every integral δ-semiring is a $\hat{\delta}$-semiring.*

Theorem 1.2. (1a) *and* (1b) *are independent in TS.*

Theorem 1.3. *Domain commutes with all existing suprema in KAD.*

1.2.4 Predomain in b-monoids

predomain can now be defined in terms of the Galois connection

$$\delta(a) \leq p \Leftrightarrow a \leq p1 \tag{3}$$

For every b-monoid, (2a) and (3) are equivalent.

Remark. *There is a d-monoid in which* (2a) *holds, but not* (3)*.*

1.2.5 Codomain

The definition of codomain parallels that of domain. For a set-theoretic relation $R \subseteq A \times A$, it is defined as

$$\rho(R) = \{b \in A | \exists a \in A \text{ s.t. } (a, b) \in R\}$$

As usual in algebra, the opposite of a semiring $(A, +, ., 0, 1)$ is the structure $(A, +, ., 0, 1)$ where $a.b := b.a$ with abuse of notation for simplicity. We denote the opposite of a semiring A by A^{opp}.

Definition 1.4. *we define:*
(i) A t-semiring with precodomain (a ρ-semiring) is a structure (A, ρ) such that (A^{opp}, ρ) is a semiring with predomain.
(ii) A t-semiring with codomain (a $\hat{\rho}$-semiring) is a structure $(A, \hat{\rho})$ such that $(A^{opp}, \hat{\rho})$ is a semiring with domain.

1.2.6 Codomain via converse

In the relational semiring, it is evident that the domain of a relation is the codomain of its converse and vice versa. This coupling of domain and codomain via the concept of converse induces a second notion of symmetry or duality, besides the one based on opposition. As usual, the operation of converse in an i-semiring is required to be involutive, additive and contravariant, we will not cover this further, refer to [DMS06].

1.3 Image and Preimage

In the relational semiring, the preimage of a set $B \subseteq A$ under a relation $R \subseteq A \times A$ is defined as

$$R : B = \{x \in A | \exists y \in B \text{ s.t. } (x, y) \in R\}$$

This is equivalent to the point-free definition $R : B = \delta(RB)$. Dually, the image of B under R is defined as

$$B : R = \{y \in A | \exists x \in A \text{ s.t. } (x, y) \in R.\}$$

which is equivalent to the point-free definition by $B : R = \rho(BR)$.
We define for every $A \in TSP$, the image and the preimage operator, both denoted by : , as mappings of type $test(A) \times A \to test(A)$ and $A \times test(A) \to test(A)$ by

$$p : a = \rho(pa) \qquad \text{(4a)} \qquad\qquad a : p = \delta(ap) \qquad \text{(4b)}$$

for all $a \in A$ and $p \in test(A)$.

1.4 Domain and Kleene star

Properties. *Denote that:*

- *Let $A \in KAP$. For all $a \in A$ and $p \in test(A)$,*

$$\delta(a)^* = 1 \qquad\qquad \delta(a^*) = 1$$

- *Let $A \in KAD$. For all $a \in A$ and $p \in test(A)$,*

$$a : p \leq p \Rightarrow a^* : p \leq p$$

Corollary 1.3.1. *Let $A \in KAD$. For all $a, b, c \in A$ and $p \in test(A)$,*

$$(ac) : p + b : q \leq c : p \Rightarrow (a^* b) : q \leq c : p$$

1.5 Noethericity

Intuitively, a set-theoretic relation $R \subseteq A \times A$ is well-founded if there are no infinitely descending R-chains, that is, no infinite chains $x_0, x_1, ...$ such that $(x_{i+1}, x_i) \in R$. Moreover, R is Noetherian if there are no infinitely ascending R-chains, that is, no infinite chains $x_0, x_1, ...$ such that $(x_i, x_{i+1}) \in R$. Thus, R is not well-founded if there is a non-empty set $P \subseteq A$ (denoting the infinite chain) such that for all $x \in P$ there exists some $y \in P$ with $(y, x) \in R$. This is equivalent to saying that P is contained in the image of P under R, that is,

$$P \subseteq P : R$$

Consequently, if R is well-founded, then only the empty set may satisfy the above.
Abstracting to $A \in TSD$ we say that a is well-founded if for all $p \in test(A)$,

$$p \leq p : a \Rightarrow p \leq 0$$

Moreover, a is Noetherian if for all $p \in test(A)$,

$$p \leq a : p \Rightarrow p \leq 0$$

1.6 Propositional Hoare Logic

Soundness of PHL is a direct theorem of KAD.

2 Kleene Modules

2.1 Definition

Definition 2.1. *A Kleene left-module is a two-sorted algebra* $(K, B, :)$*, where* $K \in KA$ *and* $B \in BA$ *and where the left scalar product* $:$ *is a mapping* $K \times B \to B$ *such that for all* $a, b \in K$ *and* $p, q \in B$*,*

$$a : (p + q) = a : p + a : q \qquad (a + b) : p = a : p + b : p \qquad (ab) : p = a : (b : p)$$
$$1 : p = p \qquad 0 : p = 0 \qquad q + a : p \le p \Rightarrow a^* : q \le p$$

KM_l denotes the class of Kleene left-modules. In accordance with the relation-algebraic tradition, we call scalar products of KM_l also Peirce products.

Observation. *In KAD an image operator is an example of a Kleene left-module.*

2.2 Calculus

Properties. *Let* $(K, B, :) \in KM_l$*. For all* $a \in K$ *and* $p, q \in B$*, the scalar product has the following properties.*

(i) *It is right-strict, that is* $a : 0 = 0$*.*

(ii) *It is left- and right-monotonic.*

(iii) $p \le 0 \Rightarrow a : p \le 0$*.*

(iv) $a : (pq) \le (a : p)(a : q)$*.*

(v) $a : p - a : q \le a : (p - q)$*. Here,* $p - q = pq'$*.*

(vi) $p + a : (a^* : p) = a^* : p$*,*

(vii) $p + a^* : (a : p) = a^* : p$*.*

2.3 Extentionality

Refer to [EMS03].

2.4 Modalities and their Algebra

in [MS04] Modal Kleene algebra is defined as Kleene algebra enriched by forward and backward box and diamond operators. These operators are identically image and preimage operators defined in (4a) and (4b) with a different notation. Consequently ,they are Kleene module operators and all the properties mentioned in [MS04] follows.

References

[DMS06] Jules Desharnais, Bernhard Möller, and Georg Struth. Kleene algebra with domain. *ACM Transactions on Computational Logic (TOCL)*, 7(4):798–833, 2006.

[EMS03] Thorsten Ehm, Bernhard Möller, and Georg Struth. Kleene modules. In *International Conference on Relational Methods in Computer Science*, pages 112–123. Springer, 2003.

[MS04] Bernhard Möller and Georg Struth. Modal kleene algebra and partial correctness. In *International Conference on Algebraic Methodology and Software Technology*, pages 379–393. Springer, 2004.