

UNIVERSITÄT AUGSBURG

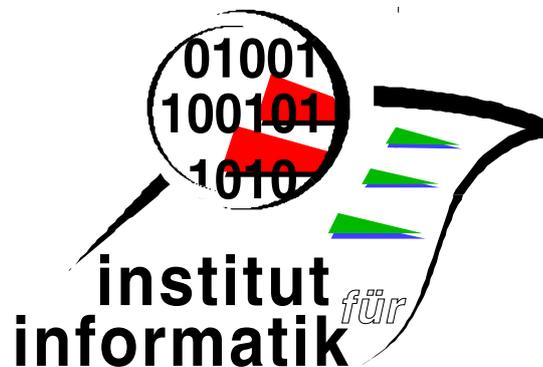


Kleene Algebra with Domain

Jules Desharnais and Bernhard Möller and Georg Struth

Report 2003-07

Mai 2003



INSTITUT FÜR INFORMATIK

D-86135 AUGSBURG

Copyright © Jules Desharnais and Bernhard Möller and Georg Struth
Institut für Informatik
Universität Augsburg
D-86135 Augsburg, Germany
<http://www.Informatik.Uni-Augsburg.DE>
— all rights reserved —

Kleene Algebra with Domain

Jules Desharnais¹ Bernhard Möller² Georg Struth²

¹ Département d'informatique, Université Laval,
Québec QC G1K 7P4 Canada
`Jules.Desharnais@ift.ulaval.ca`

² Institut für Informatik, Universität Augsburg
Universitätsstr. 14, D-86135 Augsburg, Germany
`moeller, struth@informatik.uni-augsburg.de`

Abstract We propose Kleene algebra with domain (KAD), an extension of Kleene algebra with two equational axioms for a domain and a codomain operation, respectively. KAD considerably augments the expressibility of Kleene algebra, in particular for the specification and analysis of state transition systems. We develop the basic calculus, discuss some related theories and present the most important models of KAD. We demonstrate applicability by two examples: First, an algebraic reconstruction of Noethericity and well-foundedness. Second, an algebraic reconstruction of propositional Hoare logic.

Keywords: Idempotent semiring, Kleene algebra, domain, codomain, image and preimage operation, state transition systems, program development and analysis.

1 Introduction

State transition systems are often modelled in a bipartite world in which propositions and actions coexist. Propositions express static properties of states, while actions relate states to model their dynamics. Propositions are usually organized in a Boolean algebra, whereas the sequential, non-deterministic and iterative behaviour of actions is often ruled by a Kleene algebra. Reasoning about state transition systems requires migration between the two parts of the world. This can be modelled by two mappings. One sends actions to propositions in order to express properties of actions. The other sends propositions to actions in order to model propositions as tests, measurements or observations on states, hence as state-preserving actions. This is needed in particular for programming constructs like conditionals or *while*-loops.

There are two prominent, but complementary realizations of this two-world picture: Propositional dynamic logic and its algebraic variants [18,22,33,34,36,39] (PDL) and Kleene algebra with tests (KAT) [25]. In PDL, only propositions are first-class citizens. This gives the approach a logical flavor. While equivalence of propositions is directly expressible, actions can only be observed indirectly through propositions; the algebra of actions is implicitly defined within that of

propositions. However, both mappings are present: modal operators from actions and propositions into propositions and test operators from propositions into actions. This approach is suited for an extensional world, in which actions are completely determined by their input/output behaviour, for instance, when they are modelled as set-theoretic relations. Then, the use of modal operators allows a very versatile and intuitive reasoning. In KAT, only actions are first-class citizens. This gives the approach an algebraic flavour. While equivalence of actions is directly expressible, propositions can only be observed by considering them as actions; the algebra of propositions is embedded as a subalgebra into the algebra of actions, which is a Kleene algebra. Thus only the mapping from propositions to actions is present. The overloading of syntax for propositions and actions leads to particularly economical specifications and proofs. KAT does not make any extensionality assumptions and therefore admits a rich class of models beyond the relational one¹. Using PDL or KAT, many properties of state transition systems can succinctly be expressed and analyzed. Each approach has its particular advantages and merits. Note, however, that PDL is EXPTIME-complete [18], while the equational theory of KAT is PSPACE-complete [27].

We propose Kleene algebra with domain (KAD) as an extension of KAT and as a reconciliation of KAT and PDL with equal opportunities for propositions and actions. We believe that KAD not only combines the particular advantages of both previous approaches. It also offers additional flexibility and symmetry and yields new structural insights. In particular, beyond this reconciliation, our algebraic abstraction of the domain operation yields a uniform view of hitherto separate approaches to program analysis and development: formalisms based on modal logic such as PDL, formalisms based on algebra such as KAT, set-based formalisms such as B [2] and Z [38], where domain is extensively used, and semantic approaches based on predicate transformers [13]. As in KAT, we embed propositions into actions. As in PDL, we also provide a mapping from actions to propositions: the domain operation. Adding domain to KAT is only natural. Relations are the standard model for state transition systems in KAT and PDL. Domain is probably the most natural “modal operator” for relations and KAD supports abstract algebraic reasoning with it. Domain has been already been defined algebraically in extensions of Kleene algebra like quantales and relation algebras (cf. [1,11,12,37]). But there is no straightforward transfer to KAT. Again, KAD offers several benefits. In opposition to relation algebra, it focuses entirely on the essential operations for state transition systems. Compared with quantales, our approach is entirely first-order and therefore better suited for automated reasoning.

Here, our main emphasis is on motivating the definitions, developing the basic calculational aspects and discussing the most interesting models of KAD. We also provide two examples that show its applicability. Many interesting questions, for instance concerning completeness, representability, expressiveness, complexity, the precise relation to modal algebras and a more extensive investigation of applications are postponed to further publications.

¹ Extensionality is studied under the name *separability* in the context of PDL [21].

More precisely, our main results are the following.

- We propose finite equational axiomatizations of a domain and codomain operator for certain idempotent semirings and Kleene algebras.
- We develop a basic domain calculus for KAD. Our axioms capture many natural properties of domain in the relational model and provide new structural insight into the abstract algebraic properties of domain.
- We show that KAD is well-behaved on the standard models of Kleene algebra.
- We define preimage and image operators in KAD. These are very interesting for the specification and analysis of state transition systems and programs.
- We show that Noethericity and well-foundedness are expressible in KAD. We derive properties of these notions.
- We show that KAD subsumes propositional Hoare logic; moreover, we argue that it can serve as the core of abstract axiomatic semantics for imperative programming languages.
- We derive implementation schemata for efficient reachability algorithms for directed graphs within KAD.

Besides these main results there are the following interesting contributions. We show independence of the domain and codomain axioms of KAD. We discuss show their compatibility with those for quantales and relation algebra. We provide translations from a class of KAD-expressions to KAT without domain. We introduce two notions of duality that enable a transfer between properties of domain and those of codomain. We show that KAD is not a finitely based variety, whereas all its subalgebras of propositions and all idempotent semirings with domain are.

The remainder of this text is organized as follows. Section 2 introduces idempotent semirings, Kozen’s Kleene algebra, some extensions and the standard models for these structures. Section 3 introduces idempotent semirings with tests, KAT and again the standard models. Section 4 presents an equational axiomatization of domain for idempotent semirings. We show independence of the axioms, discuss several extensions and provide some examples for the standard models. Moreover, we outline a basic domain calculus for idempotent semirings. Another important concept, locality domain and codoman, paves the way to an incorporation of propositional dynamic logic. Section 5 presents two ways of basing an equational axiomatization of codomain for idempotent semirings on that of domain. In Section 6, image and preimage operators are derived from the domain and codomain operators. In Section 7 we derive properties of domain and codomain in KAD. In connection with the Kleene star operator, they allow an abstract treatment of reachability in directed graphs and state transition systems. Section 8 contains some simple metaresults on KAD. Section 9 algebraically reconstructs Noethericity and well-foundedness in KAD. Section 10 shows that propositional Hoare logic is subsumed by KAD. Section 11 draws conclusions and points out further work.

2 Idempotent Semirings and Kleene Algebra

In this section, we introduce idempotent semirings, Kozen's variants of Kleene algebras and certain related structures such as lattice-ordered monoids and quantales. We also present some important models of Kleene algebra, such as the relational model, the language model, the path model, the $(\min, +)$ - and $(\max, +)$ -models and some of the small finite Kleene algebras of Conway.

Kleene algebras are a class of algebras that axiomatize the regular operations of addition, multiplication and Kleene star as they arise in formal languages and in the analysis of state transition systems and programs. Traditionally, there are two main approaches to Kleene algebra, one based on semirings, the other based on lattices.

2.1 Semirings

A *semiring* is a structure $(A, +, \cdot, 0, 1)$, such that $(A, +, 0)$ is a commutative monoid, $(A, \cdot, 1)$ is a monoid, multiplication is left and right distributive with respect to addition and 0 is an annihilator with respect to multiplication ($a0 = 0 = 0a$). As a convention, we always assume that 0 and 1 are elements of A . We call a semiring *trivial* if $0 = 1$, since then for all $a \in A$

$$a = a1 = a0 = 0,$$

i.e., $A = \{0\}$. Therefore, henceforth we identify semirings with non-trivial semirings. We also write ab instead of $a \cdot b$ and stipulate that multiplication binds stronger than addition.

A semiring is *idempotent* (an *i-semiring*) if addition is idempotent. The class of idempotent semirings is denoted by IS.

The relation \leq defined on an i-semiring A by

$$a \leq b \Leftrightarrow a + b = b \tag{1}$$

for all $a, b \in A$ is a partial ordering, in fact the only partial ordering on A for which $0 \leq a$ for all $a \in A$ and which is (left and right) monotonic with respect to addition and multiplication. It is therefore called the *natural ordering* on A . By (1), inequalities can be understood as abbreviations for equations. We therefore use the notion of equation freely for both kinds of expressions.

Obviously, every i-semiring is a semilattice with respect to the natural ordering with least element 0 and addition as join. Thus

$$a \leq c \wedge b \leq c \Leftrightarrow a + b \leq c. \tag{2}$$

In calculations with partial orders, we often appeal to the principles of *indirect inequality* and *indirect equality*. Instead of $a \leq b$ we show $\forall c. c \leq a \Rightarrow c \leq b$ or $\forall c. b \leq c \Rightarrow a \leq c$. Likewise, $a = b$ can be proved by showing $\forall c. c \leq a \Leftrightarrow c \leq b$ or $\forall c. b \leq c \Leftrightarrow a \leq c$.

2.2 Kozen Semirings

A *Kozen semiring* (a K-semiring) [23] is a structure $(A, +, \cdot, *, 0, 1)$, such that $(A, +, \cdot, 0, 1)$ is an i-semiring, a^*b is the least prefixed point of the function $\lambda x.b + ax$ and ba^* is the least prefixed point of $\lambda x.b + xa$. Formally, the *Kleene star* $*$ satisfies the equations

$$1 + aa^* \leq a^*, \quad (*-1)$$

$$1 + a^*a \leq a^*, \quad (*-2)$$

and the Horn rules

$$b + ac \leq c \Rightarrow a^*b \leq c, \quad (*-3)$$

$$b + ca \leq c \Rightarrow ba^* \leq c, \quad (*-4)$$

for all $a, b, c \in A$. The class of K-semirings is denoted by KA.

The expressions a^*b and ba^* are uniquely defined by (*-1) and (*-3), and (*-2) and (*-4), respectively. We now recall some further standard properties of K-semirings (cf. [23]). Most of them are also familiar from formal language theory [15].

Lemma 2.1. *Let $A \in \text{KA}$. For all $a, b \in A$,*

$$1 \leq a^*, \quad (3)$$

$$a^*a^* = a^*, \quad (4)$$

$$\forall i \in \mathbb{N}. a^i \leq a^*, \quad (5)$$

$$a^{**} = a^*, \quad (6)$$

$$(ab)^*a = a(ba)^*, \quad (7)$$

$$(a + b)^* = a^*(ba^*)^*. \quad (8)$$

For all $a, b, c \in A$,

$$a \leq 1 \Rightarrow a^* = 1, \quad (9)$$

$$a \leq b \Rightarrow a^* \leq b^*, \quad (10)$$

$$ac \leq cb \Rightarrow a^*c \leq cb^*, \quad (11)$$

$$ca \leq bc \Rightarrow ca^* \leq b^*c. \quad (12)$$

2.3 Lattice-Ordered Monoids and Quantales

A *lattice-ordered monoid* (an *l-monoid*) is a structure $(A, +, \sqcap, \cdot, 1)$, such that $(A, +, \sqcap)$ is a lattice, $(A, \cdot, 1)$ is a monoid and left and right multiplication are additive. l-monoids are extensively studied in [4]. An l-monoid is *bounded* if it has a least element 0 and a greatest element \top . It is *complete* if the underlying lattice is. A *quantale* [32] or *standard Kleene algebra* [9] is a complete l-monoid in which left and right multiplication is universally additive. Quantales have been

investigated in contexts like the logic of quantum mechanics [32] and algebraic models of certain linear logics [41]. A *d-monoid* and *ab-monoid*, respectively, is an l-monoid whose lattice reduct is distributive and Boolean, respectively. A *d-quantale* and *b-quantale*, respectively, is a quantale whose lattice reduct is distributive, and Boolean, respectively. Remember that a Boolean lattice is a complemented distributive lattice, we use the notion *Boolean algebra* as a synonym. b-monoids and b-quantales have been studied, for instance, in [11,12]. Also the sequential algebras of [19] are particular b-quantales. In quantales, the Knaster-Tarski theorem guarantees that the Kleene star, which is again defined as the least pre-fixed point of a monotonic function, always exists. This is in contrast to KA, where completeness of the underlying semilattice is not assumed.

The main results of this paper are entirely based on i-semirings and not on quantales. A first reason is that i-semirings are more general than quantales. Every quantale is an l-monoid; every K-semiring and every l-monoid is an i-semiring. K-semirings are first-order structures whereas, due to completeness, quantales are essentially higher-order. However, completeness is the key to using Galois connections as a very elegant means of defining functions on quantales, whereas this is not in general possible for i-semirings.

A second reason is that in b-modules and b-quantales there is a notion of complementation. When reasoning about programs, elements of a b-monoid represent programs as input/output relations. Hence the complement of such an element relates all states that are not in the input/output relation. IS has the advantage of avoiding an ontological commitment to this concept, which is rather unnatural in this context.

2.4 Example Structures

The classes IS and KA are quite rich. We now present some standard examples. We will later show that the domain and codomain operations are well-behaved on all these structures. In the first examples, we present some of the finite K-semirings with at most 4 elements from Conway's book (c.f. [9], p.101). We will later use them, in particular, as counterexamples.

Example 2.1.

$$\begin{array}{c} 1 \\ | \\ 0 \end{array}$$

Consider the structure $A_2 = (\{0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by the tables

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Then A_2 is an i-semiring, called the *Boolean semiring*, since $+$ and \cdot play the roles of disjunction and conjunction. A_2 can uniquely be extended to a K-semiring by setting $0^* = 1^* = 1$. □

Example 2.2.

$$\begin{array}{c} a \\ | \\ 1 \\ | \\ 0 \end{array}$$

Consider the structure $A_3^1 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by the tables

$$\begin{array}{c|ccc} + & 0 & a & 1 \\ \hline 0 & 0 & a & 1 \\ a & a & a & a \\ 1 & 1 & a & 1 \end{array} \quad \begin{array}{c|ccc} \cdot & 0 & a & 1 \\ \hline 0 & 0 & 0 & 0 \\ a & 0 & a & a \\ 1 & 0 & a & 1 \end{array}$$

Then A_3^1 is an i-semiring. It can uniquely be extended to a K-semiring by setting $0^* = 1^* = 1$ and $a^* = a$. \square

Example 2.3.

$$\begin{array}{c} 1 \\ | \\ a \\ | \\ 0 \end{array}$$

Consider the structure $A_3^2 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with natural ordering $0 < a < 1$ and addition and multiplication defined by the tables

$$\begin{array}{c|ccc} + & 0 & a & 1 \\ \hline 0 & 0 & a & 1 \\ a & a & a & 1 \\ 1 & 1 & 1 & 1 \end{array} \quad \begin{array}{c|ccc} \cdot & 0 & a & 1 \\ \hline 0 & 0 & 0 & 0 \\ a & 0 & 0 & a \\ 1 & 0 & a & 1 \end{array}$$

Then A_3^2 is an i-semiring. It can uniquely be extended to a K-semiring by setting $a^* = 0^* = 1^* = 1$. \square

Example 2.4. Consider the structure $A_3^3 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ which is like A_3^2 except for $a \cdot a = 0$:

$$\begin{array}{c|ccc} + & 0 & a & 1 \\ \hline 0 & 0 & a & 1 \\ a & a & a & 1 \\ 1 & 1 & 1 & 1 \end{array} \quad \begin{array}{c|ccc} \cdot & 0 & a & 1 \\ \hline 0 & 0 & 0 & 0 \\ a & 0 & 0 & a \\ 1 & 0 & a & 1 \end{array}$$

Then A_3^3 is an i-semiring. It can uniquely be extended to a K-semiring by setting $a^* = 0^* = 1^* = 1$. \square

Example 2.5.

$$\begin{array}{c} b \\ | \\ 1 \\ | \\ a \\ | \\ 0 \end{array}$$

Consider the structure $A_4^1 = (\{a, b, 0, 1\}, +, \cdot, 0, 1)$ with natural ordering $0 < a < 1 < b$ and addition and multiplication defined by the tables

$$\begin{array}{c|cccc} + & 0 & a & 1 & b \\ \hline 0 & 0 & a & 1 & b \\ a & a & a & 1 & b \\ 1 & 1 & 1 & 1 & b \\ b & b & b & b & b \end{array} \quad \begin{array}{c|cccc} \cdot & 0 & a & 1 & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & a & a \\ 1 & 0 & a & 1 & b \\ b & 0 & a & b & b \end{array}$$

Then A_4^1 is an i-semiring. It can be extended to a K-semiring by setting $0^* = a^* = 1^* = 1$ and $b^* = b$. \square

There are 18 four-element K-semirings, up to isomorphism.

Example 2.6. Consider a set A and the structure $\text{REL}(A) = (2^{A \times A}, \cup, \circ, \emptyset, \Delta)$, where $2^{A \times A}$ denotes the set of binary relations over A , \cup denotes set union, \circ denotes relational product, \emptyset denotes the empty relation and Δ denotes the identity relation $\{(a, a) \mid a \in A\}$.

Then $\text{REL}(A)$ is an i-semiring with set inclusion as the natural ordering. It can be extended to a K-semiring by defining R^* as the reflexive transitive closure of R for all $R \in \text{REL}(A)$, that is, $R^* = \bigcup_{i \geq 0} R^i$, where $R^0 = \Delta$ and $R^{i+1} = R \circ R^i$.

We call $\text{REL}(A)$ the *relational* i-semiring or K-semiring over A . \square

Example 2.7. Let $(A, +, \cdot, 0, 1)$ be a semiring and Q be a finite set. Then the set $A^{Q \times Q}$ can be viewed as the set of $|Q| \times |Q|$ -matrices with indices in Q and elements in A . Now consider the structure $\text{MAT}(Q, A) = (A^{Q \times Q}, +, \cdot, \mathbf{0}, \mathbf{1})$ where $+$ and \cdot are the usual operations of matrix addition and multiplication and $\mathbf{0}$ and $\mathbf{1}$ are the zero and unit matrices. Then $\text{MAT}(Q, A)$ again forms a semiring, the *matrix semiring* over Q and A . $\text{MAT}(Q, A)$ is idempotent if A is. In this case, the natural order is the componentwise order. If the underlying semiring A admits infinite sums, Q may also be infinite.

Taking A as the Boolean semiring yields another representation of $\text{REL}(A)$ as $\text{MAT}(Q, A)$ in terms of adjacency matrices.

If A is a K-semiring and Q finite then $\text{MAT}(Q, A)$ can be extended to a K-semiring (see [9]) by setting

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} f^* & f^* b d^* \\ d^* c f^* & d^* + d^* c f^* b d^* \end{pmatrix},$$

where $f = a + bd^*c$.

***hier ergaenzen...

□

Example 2.8. Let Σ^* be the set of finite words over some finite alphabet Σ and consider the structure $\text{LAN}(\Sigma) = (2^{\Sigma^*}, \cup, \cdot, \emptyset, \{\varepsilon\})$, where 2^{Σ^*} denotes the set of languages over Σ , and the \cup denotes set union, $L_1.L_2 = \{vw \mid v \in L_1, w \in L_2\}$, where vw denotes concatenation of v and w , \emptyset denotes the empty language and ε denotes the empty word.

Then $\text{LAN}(\Sigma)$ is an i-semiring with natural ordering defined by language inclusion. It can be extended to a K-semiring, defining $L^* = \{w_1w_2 \dots w_n \mid n \geq 0, w_i \in L\}$.

We call $\text{LAN}(\Sigma)$ the *language* i-semiring or K-semiring over Σ . Remember that \cup , \cdot and $*$ are often called *regular operations* and the sets that can be obtained from finite subsets of Σ^* by a finite number of regular operations are called *regular subsets* or *regular events* of Σ^* . The equational theory of the rational subsets is also called the *algebra of regular events*.

There is a natural homomorphism L from the term algebra over the signature of K-semirings generated by a set Σ onto the algebra of regular subsets of Σ^* , given by $L(a) = \{a\}$ for each $a \in \Sigma$, $L(a + b) = L(a) \cup L(b)$ and $L(a \cdot b) = L(a).L(b)$. Kozen [23] has shown that $\text{LAN}(\Sigma)$ is the free K-semiring on the generators Σ . □

Example 2.9. Consider a set Σ of vertices (or states). Then subsets of Σ^* can be viewed as sets of possible graph paths (or state sequences in a transition system). The partial operation of *join* or *fusion product* of elements of Σ^* is defined as

$$\varepsilon \bowtie \varepsilon = \varepsilon \tag{13}$$

$$\varepsilon \bowtie (y.t) \text{ is undefined,} \tag{14}$$

$$(s.x) \bowtie \varepsilon \text{ is undefined,} \tag{15}$$

$$(s.x) \bowtie (y.t) = \begin{cases} s.x.t & \text{when } x = y, \\ \text{undefined} & \text{otherwise} \end{cases} \tag{16}$$

for all $s, t \in \Sigma^*$ and $x, y \in \Sigma$. It describes the gluing of paths at a common end point. This operation is extended to subsets of Σ^* by

$$S \bowtie T = \{s \bowtie t \mid s \in S \wedge t \in T \wedge s \bowtie t \text{ defined}\}.$$

Then $\text{PAT}(\Sigma) = (2^{\Sigma^*}, \cup, \bowtie, \emptyset, \Sigma \cup \{\varepsilon\})$ is an i-semiring that we call the *path i-semiring* over Σ . □

Example 2.10. Using matrices over the language algebra we can also model labelled transition systems. Assume a set Q of states and a set Σ of labels. The matrices in $\text{MAT}(Q, \text{LAN}(\Sigma))$ can be considered as recording possible sequences of labels (traces) that connect two states; if there is no possible transition between two states, the corresponding matrix element is the empty language. □

Example 2.11. The language example can easily be generalized to an arbitrary monoid $(A, \cdot, 1)$. Then $(2^A, \cup, \circ, \emptyset, \{1\})$ is the free i-semiring over $(A, \cdot, 1)$. In particular, multiplication (and star) are defined as in Example 2.8. □

Example 2.12. Set $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$ and define the operations \min and $+$ in the obvious way. Then the structure $(\min, +) = (\mathbb{N}_\infty, \min, +, \infty, 0)$ is an i-semiring, called the *tropical semiring* [28]. Its natural ordering is the converse of the standard ordering on \mathbb{N}_∞ . Hence 0—the semiring multiplicative unit—is the largest element, so that by (9) $(\min, +)$ can uniquely be extended to a K-semiring by setting $n^* = 0$ for all $n \in \mathbb{N}_\infty$. \square

Example 2.13. Set $\mathbb{N}_{-\infty} = \mathbb{N} \cup \{-\infty\}$ and consider the structure $(\max, +) = (\mathbb{N}_{-\infty}, \max, +, -\infty, 0)$ with operations defined in the obvious way. Then $(\max, +)$ is an i-semiring, called the *max-plus semiring* [17]. Its natural ordering coincides with the standard ordering on $\mathbb{N}_{-\infty}$. Unlike the tropical semiring, the max-plus semiring cannot be extended to a K-semiring. The reason is that for $a > 0$ the set $\{a^n \mid n \in \mathbb{N}\} = \{na \mid n \in \mathbb{N}\}$ is unbounded, whereas, according to (5), it should have a^* as an upper bound. \square

3 Subidentities and Kleene Algebra with Tests

We now take the first step towards the definition of domain and codomain operations on IS. We discuss the subidentities of IS, KA and related structures. These are the elements that lie below the multiplicative unit. We also introduce idempotent semirings with tests and Kleene algebras with tests. Finally, we discuss a few important models of these structures.

As a motivation, consider the relational i-semiring from Example 2.6. Here, the domain of a relation is a set. Abstracting to arbitrary i-semirings, the domain operation should be a mapping from the i-semiring to some appropriate Boolean algebra. In the matrix representation for finite relations based on the Boolean semiring, obviously, a *characteristic matrix* can be associated with each set A . Setting $n = |A|$, the empty set is characterized by the $n \times n$ zero matrix, the set A by the $n \times n$ unit matrix and all other sets by matrices smaller than the unit matrix. Obviously, there are 2^n such matrices, which is also the number of subsets of A . Using this abstraction, we model domain and codomain in an i-semiring as an i-semiring endomorphism into the set of elements that are smaller than 1. We now take a closer look at the set of these elements.

3.1 Subidentities

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

Lemma 3.1. *The set of subidentities of an i-semiring forms an i-semiring.*

However, this subsemiring is usually too large for our purposes. In the relational i-semiring or in b-monoids, multiplication of subidentities is a meet operation; the set of subidentities is a Boolean sublattice (c.f. Section 3.3). In i-semirings, this need not be the case.

Lemma 3.2. *Multiplication of subidentities in IS is a lower bound operation.*

Proof. Let $A \in \mathbf{IS}$ and $p, q \in \text{sid}(A)$. Then $p = p1 \geq pq \leq 1q = q$. Thus pq is a lower bound of p and q . \square

Lemma 3.3. *Multiplication of subidentities in \mathbf{IS} (in d -monoids, d -quantales) is not always idempotent.*

Proof. Consider the i -semiring A_3^2 from Example 2.3. Obviously, a is a subidentity that is not multiplicatively idempotent. Since A_3^2 is a chain, it is automatically a distributive lattice, hence a d -monoid. Since it is finite, it is automatically complete, hence a d -quantale. The counterexample is minimal for all these structures. \square

Consequently, multiplication of subidentities in \mathbf{IS} is not in general a greatest lower bound operation. Additional properties are required to model sets, propositions or tests in \mathbf{IS} .

Lemma 3.4. *The set of multiplicatively idempotent subidentities of an i -semiring forms a bounded distributive lattice.*

Proof. Let $\text{isid}(A)$ be the set of multiplicatively idempotent subidentities of $A \in \mathbf{IS}$.

We first show that multiplication restricted to $\text{isid}(A)$ is meet, hence a greatest lower bound operation. It is a lower bound operation by Lemma 3.2. Let $p, q, r \in \text{isid}(A)$ with $r \leq p$ and $r \leq q$. Then $r = rr \leq pq$, whence pq is the greatest lower bound of p and q . Consequently, also

$$pq = qp \tag{17}$$

for $p, q \in \text{isid}(A)$.

We now show the closure properties of the subalgebra. $0, 1 \in \text{isid}(A)$ is obvious. Let $p, q \in \text{isid}(A)$. Then

$$\begin{aligned} (p + q)(p + q) &= pp + pq + qp + qq \\ &= p + (p \sqcap q) + (q \sqcap p) + q \\ &= p + q \end{aligned}$$

and, using (17),

$$(pq)(pq) = ppqq = pq.$$

We now show that the sublattice is distributive. The first distributivity law

$$p(q + r) = pq + pr$$

holds by the semiring laws. The second distributivity law

$$p + (qr) = (p + q)(p + r)$$

then follows from the first one by lattice algebra.

Finally, the lattice is bounded, since $0, 1 \in \text{isid}(A)$. \square

Instead of following this way (see also the discussion on page 18), we chose another one which is conceptually much simpler and which is introduced in the following subsection.

3.2 Test-Semirings and Kleene Algebra with Tests

Following Kozen's approach to Kleene algebra with tests, we say that a *test-semiring* (a *t-semiring*) is an i-semiring A with a distinguished Boolean subalgebra $\text{test}(A)$ of $\text{sid}(A)$ with greatest element 1 and least element 0. We call $\text{test}(A)$ the *test algebra* of A and say that A *has tests*. We denote the class of t-semirings by **TS**. A t-semiring is a *Kt-semiring* or *Kleene algebra with tests*, when the t-semiring is also a K-semiring [25]. The class of Kleene algebras with test is denoted by **KAT**.

We will henceforth use letters

$$a, b, c, \dots$$

for arbitrary semiring elements (actions) and the letters

$$p, q, r, \dots$$

for tests (propositions). Moreover, by p' we denote the complement of test p in $\text{test}(A)$. Also, $p \sqcap q$ denotes the meet of p and q .

Lemma 3.5. $\text{IS} \subseteq \text{TS}$.

Proof. Let $A \in \text{IS}$. If $0 = 1$ then the claim $A \in \text{TS}$ is trivially satisfied. Otherwise, let $\text{test}(A) = \{0, 1\}$ with $p \sqcup q = p + q$, $p \sqcap q = pq$ for all $p, q \in \text{test}A$ and $1' = 0$, $0' = 1$. This yields a Boolean subalgebra. \square

We call t-semirings with test algebra $\{0, 1\}$ *discrete*.

Lemma 3.6. Let $p, q \in \text{test}(A)$ for some $A \in \text{TS}$.

- (i) $pp = p$.
- (ii) $pq = p \sqcap q$.

Proof. By Lemma 3.2, $pq \leq p \sqcap q$.

(i)

$$p = p1 = p(p + p') = pp + pp' \leq pp + (p \sqcap p') = pp + 0 = pp \leq p1 = p.$$

(ii) Similar to the first part of the proof of Lemma 3.4, using idempotency of tests. \square

The following lemma collects some properties of **TS** which will be needed for computing with abstract image and preimage operations in Section 6.

Lemma 3.7. Let $A \in \text{TS}$ with $a \in A$ and $p, q \in \text{test}(A)$.

(i) The following properties are equivalent.

$$\begin{aligned} pa &\leq aq, \\ aq' &\leq p'a, \\ paq' &\leq 0, \\ pa &= paq. \end{aligned}$$

(ii) The following properties are equivalent.

$$\begin{aligned} ap &\leq qa \\ q'a &\leq ap', \\ q'ap &\leq 0, \\ ap &= qap. \end{aligned}$$

Proof. We only show (i). The proofs of (ii) are symmetric.

$$(1) pa \leq aq \Rightarrow aq' \leq p'a.$$

$$aq' = 1aq' = (p + p')aq' = paq' + p'aq' \leq aqq' + p'a = a0 + p'a = p'a.$$

$$(2) aq' \leq p'a \Rightarrow paq' \leq 0.$$

$$paq' \leq pp'a = 0a = 0.$$

$$(3) paq' \leq 0 \Rightarrow pa = paq.$$

$$pa = pa1 = pa(q + q') = paq + paq' = paq.$$

$$(4) pa = paq \Rightarrow pa \leq aq.$$

$$pa = paq \leq aq.$$

□

3.3 Tests in b-Monoids

When A is a b-monoid with uniquely defined complement \bar{a} for each $a \in A$, the situation is much simpler. Now complements in $\text{sid}(A)$ can be defined as restrictions of complements in A as $p' = 1 \sqcap \bar{p}$. The properties $1' = 0$, $0' = 1$, $p + p' = 1$, $pp' = 0$ are easily verified. Using the restricted complement we can show that all subidentities are multiplicatively idempotent, since

$$p = 1p = (p + p')p = pp + p'p = pp + 0 = pp.$$

Consequently, $pq = p \sqcap q$ and the whole set $\text{sid}(A)$ is a Boolean subalgebra of A (c.f. [11]).

The following lemma is the key to our comparison of the domain operations in t-semirings and b-monoids in Subsection 4.6.

Lemma 3.8. (i) Let A be a b-monoid. Let $a \in A$ and $p \in \text{sid}(A)$. Then

$$a \leq p\top \Leftrightarrow a \leq pa. \tag{18}$$

(ii) There is a d-monoid A such that the implication

$$a \leq p\top \Rightarrow a \leq pa$$

does not hold.

Proof. (ad i) $a \leq pa$ implies $a \leq p\top$, since $a \leq \top$.

$a \leq p\top$ implies $a \leq pa$. By lattice theory, $a \leq p\top$ iff $a = a \sqcap p\top$. We calculate

$$\begin{aligned}
a &= a \sqcap p\top \\
&= a \sqcap p(a + a') \\
&= (a \sqcap pa) + (a \sqcap pa') \\
&\leq (a \sqcap pa) + (a \sqcap 1a') \\
&\leq (a \sqcap pa) + 0 \\
&= a \sqcap pa \\
&\leq pa.
\end{aligned}$$

(ad ii) The i-semiring A_4^1 of Example 2.5 is clearly also a d-monoid with $\top = b$, since the natural ordering is a chain. It satisfies $a = ab = a\top$, but $a \not\leq 0 = aa$. \square

3.4 Example Structures

We now consider some models of TS and KAT. First, note that all examples by Conway from Section 2 (that is, Example 2.1 to Example 2.5 are discrete and therefore not very interesting.

Example 3.1. In $\text{REL}(A)$, there are $2^{|A|}$ subrelations of Δ . They form a Boolean algebra with $P \sqcap Q = P \circ Q$ and $P' = \Delta - P$. For finite relations, in particular, this can be verified in the matrix representation. \square

Example 3.2. In $\text{LAN}(\Sigma)$, the only subidentities are \emptyset and $\{\varepsilon\}$. They also form the only possible test algebra; hence $\text{LAN}(\Sigma)$ is always discrete. The example easily generalizes to arbitrary monoids. \square

Example 3.3. In the tropical semiring, all elements are subidentities. However, except for 0 and ∞ , they are not idempotent. Thus the only possible test algebra consists of the elements 0 and ∞ . \square

Example 3.4. In the max-plus semiring, the only subidentities are $-\infty$ and 0. These two elements also form the only possible test algebra. \square

Example 3.5. In the path i-semiring $\text{PAT}(\Sigma)$ over Σ (cf. Example 2.9), the subidentities $P \subseteq \Sigma \cup \{\varepsilon\}$ can be considered as modelling sets of nodes or states, where ε also serves as the only “pseudo-node” or “pseudo-state” in an empty sequence. \square

4 Domain

In this section, we introduce several equivalent axiomatizations of the domain operation on TS, among them a purely equational one. For a differentiated picture, we present two notions of different expressive power:

- A notion of *predomain* that suffices for deriving many natural properties of domain, as we will show in Section 4.4.
- A notion of *domain* that is important for more advanced applications.

We also show independence of the respective axioms, discuss extensions to b-monoids, quantales and relation algebras, and provide examples for the standard models.

4.1 Domain in the Relational i-Semiring

In order to motivate our abstract definitions, consider again the relational i-semiring of Example 2.6. Let $R \subseteq A \times A$ for some set A . Then the domain of R is given by the set

$$\{a \in A \mid \exists b \in A. (a, b) \in R\}.$$

For our abstraction to t-semirings, it should be represented as a binary relation instead, viz. as the subidentity

$$\delta(R) = \{(a, a) \in A \times A \mid \exists b \in A. (a, b) \in R\}.$$

In the following subsections, we will propose algebraic point-free characterizations of a predomain and domain operation. We leave it to the reader to show that they are consistent with the relational semiring. But first, let us replace the set-theoretic characterization of domain by two more algebraic ones.

First, $\delta(R)$ is the least solution for X of the inclusion

$$R \subseteq X \circ R.$$

Second, using Example 3.1, the complement $\delta(R)'$ of $\delta(R)$ in the Boolean lattice of subidentities of $\text{REL}(A)$ — the set of all pairs below Δ that are not in $\delta(R)$ — is the greatest solution for X of the inclusion

$$X \circ R \subseteq \emptyset$$

under the constraint $X \subseteq \Delta$. Without this restriction, the greatest solution is $\overline{V \circ R}$, where V denotes the universal relation. Interestingly, $\overline{V \circ R} \circ \delta(R) = \emptyset$, but $\delta(R) \circ \overline{V \circ R} \neq \emptyset$, except under special circumstances. So, there is an asymmetry that is compatible with the definition of domain in terms of a greatest and a least solution.

Since $\text{REL}(A)$ is a complete lattice with respect to set-inclusion, both solutions are unique and the functional notation $\delta(R)$ is justified. In particular, $\delta(R) \subseteq \Delta$ is an immediate consequence of the definition in terms of a least solution. Since, according to Example 3.1, the subidentities of $\text{REL}(A)$ form a Boolean algebra, Lemma 3.7 shows that the two definitions in terms of least and greatest solutions are indeed equivalent.

4.2 Preservers and Annihilators

As a first step of the abstraction to semirings, we introduce some auxiliary concepts. Let $A \in \mathbf{IS}$ and $a, b \in A$. We say that b *left-preserves* a if $a \leq ba$, and that a is *left-stable* under b if $ba \leq a$. If $a = ba$ we say that a is *left-invariant* under b . The concepts of *right-preservation*, *right-stability* and *right-invariance* 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 $a \in \text{sid}(A)$. 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 .

We now use these concepts for abstracting the characterizations of domain of the previous subsection from the relational semiring to arbitrary idempotent semirings and test semirings.

Lemma 4.1. *Let $A \in \mathbf{IS}$. For all $a, b \in A$, the element $f(a)$ is the least left-preserver of a iff*

$$f(a) \leq b \Leftrightarrow a \leq ba. \quad (\text{llp})$$

Proof. We show that (llp) is equivalent to

$$a \leq f(a)a, \quad (19)$$

$$a \leq ba \Rightarrow f(a) \leq b. \quad (20)$$

Equation (20) is one direction of (llp). Setting $b = f(a)$ in (llp) yields (19). Moreover, $a \leq f(a)a \leq ba$ follows immediately from (19) and $f(a) \leq b$. \square

Lemma 4.2. *In \mathbf{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.*

Proof. (ad i) Set $b = 1$ in (llp).

(ad ii) $f(a)f(a) \leq f(a)$, follows from (i).

We have already seen in the proof of Lemma 4.1 that (llp) implies $a \leq f(a)a$, hence $a \leq f(a)f(a)a$. Insertion in the right-hand side of (llp) yields $f(a) \leq f(a)f(a)$.

(ad iii) This follows from (i) and (ii) with Lemma 3.4. \square

An analogous treatment of greatest left annihilators in \mathbf{IS} is, however, not straightforward. By Lemma 3.3, subidentities are in general not multiplicatively idempotent; meets and therefore complements need not in general exist.

There are two obvious solutions:

1. Greatest left annihilators can be defined in terms of least left preservers if the distributive lattice of least left preservers can be extended to a Boolean lattice and if the search for a greatest solution is restricted to this Boolean

lattice. This extension is possible by the representation theorem for distributive lattices (cf. [4]) according to which every distributive lattice can be isomorphically embedded into some field of sets.

2. The considerations can be specialized from **IS** to **TS**. Then, least left preservers and greatest left annihilators can be defined as mappings into the set of tests.

Here, we choose the second alternative because of its simplicity, naturalness and technical convenience. Then, in particular, least left preservers and greatest left annihilators are multiplicatively idempotent subidentities by definition. Since domain elements are essentially abstractions of sets, they should possess a Boolean structure.

For the remainder, we will therefore restrict our attention to test-semirings.

Lemma 4.3. *Let $A \in \mathbf{TS}$. For every $a \in A$ and $p \in \mathbf{test}(A)$, $f(a)$ is the greatest left-annihilator of a iff*

$$p \leq f(a) \Leftrightarrow pa \leq 0. \quad (\text{gla})$$

Proof. We must show that (gla) is equivalent to

$$f(a)a \leq 0, \quad (21)$$

$$pa \leq 0 \Rightarrow p \leq f(a). \quad (22)$$

The calculations are similar to those in the proof of Lemma 4.1. \square

It follows from properties of the partial ordering, that least left-preservers and least left-annihilators are uniquely defined. Moreover, they always exist, since 1 and 0 are solutions of the respective inequalities.

The following lemma shows the relation between the least left-preserver and the greatest left-annihilator in a test-semiring.

Proposition 4.1. *Let $A \in \mathbf{TS}$. 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 $f(a) = g(a)'$.*

Proof. Using Lemma 3.7, (llp) and (gla), we calculate

$$f(a) \leq p \Leftrightarrow a \leq pa \Leftrightarrow p'a \leq 0 \Leftrightarrow p' \leq g(a) \Leftrightarrow g(a)' \leq p.$$

Thus $f(a) = g(a)'$ by the principle of indirect inequality. \square

4.3 Defining Predomain

We now define a notion of predomain for test-semirings that uses the notion of least left preserver. We will show that a characterization in terms of a greatest left annihilator is equivalent. Moreover, we provide a further equivalent characterization in terms of two simple equations. We also show independence of the equational axioms and that predomain exists and is uniquely defined for each test semiring.

Definition 4.1. A structure (A, δ) is a t-semiring with predomain (a δ -semiring) if $A \in \mathbf{TS}$ and the predomain operation $\delta : A \rightarrow \mathbf{test}(A)$ satisfies (llp), that is, for all $a \in A$ and $p \in \mathbf{test}(A)$,

$$\delta(a) \leq p \Leftrightarrow a \leq pa. \quad (\text{llp})$$

The class of t-semirings with predomain is denoted \mathbf{TSP} .

The predomain operation is always uniquely defined, since least elements in a partial order are always unique.

We distinguish between predomain and domain, since, as already noted, the weaker definition suffices for deriving many natural properties.

Proposition 4.2. \mathbf{TSP} is precisely the class of \mathbf{TS} where each $A \in \mathbf{TSP}$ is enriched by a mapping $\delta : A \rightarrow \mathbf{test}(A)$ that satisfies, for all $a \in A$ and $p \in \mathbf{test}(A)$,

$$\delta(a) \leq p \Leftrightarrow p'a \leq 0. \quad (\text{gla})$$

Proof. Immediate from Lemma 4.1. \square

We now present an equational characterization of domain.

Theorem 4.1. \mathbf{TSP} is precisely the class of \mathbf{TS} where each $A \in \mathbf{TSP}$ is enriched by a mapping $\delta : A \rightarrow \mathbf{test}(A)$ that satisfies, for all $a \in A$ and $p \in \mathbf{test}(A)$, the two equations

$$a \leq \delta(a)a, \quad (\text{d1})$$

$$\delta(pa) \leq p. \quad (\text{d2})$$

Proof. We prove a somewhat stronger statement. First, we show that (d1) is equivalent to

$$\delta(a) \leq p \Rightarrow a \leq pa, \quad (23)$$

which is one direction of (llp). Obviously, (23) implies (d1), setting $p = \delta(a)$. For the converse direction, $a \leq \delta(a)a$ and $\delta(a) \leq p$ imply $a \leq pa$ by monotonicity of multiplication.

Second, we show that (d2) is equivalent to

$$a \leq pa \Rightarrow \delta(a) \leq p, \quad (24)$$

which is the other direction of (llp). Obviously, (24) implies (d2), setting $a = pa$ and using multiplicative idempotence of p . For the converse direction, observe that $a \leq pa$ implies $a = pa$, since $p \leq 1$. Thus $\delta(a) = \delta(pa) \leq p$ by (d2).

Third, taking the previous parts together, (d1) and (d2) are equivalent to (llp). \square

Corollary 4.1. \mathbf{TSP} is a variety.

We have thus presented three equivalent axiomatizations for predomain. They are all of particular interest. The use of the equivalences (llp) and (gla) allows us to reduce certain TSP-expressions to TS-expressions that do not mention domain. Moreover, both capture the basic algebraic intuition behind this concept. The two equational axioms (d1) and (d2) are perhaps less intuitive, but very beneficial for several reasons. First, they allow us to classify t-semirings with domain in Section 8. Second, they enable us to connect δ -semirings with modal algebras and logics, which is, however, beyond the scope of this work. Third, they support a simple check, whether some given mapping in some test-semiring is a domain operation. The three axiomatizations taken together give us maximal flexibility in calculations.

We now show that the equational axiomatization is minimal:

Theorem 4.2. *(d1) and (d2) are independent in TS.*

Proof. We provide t-semirings in which precisely one of these axioms holds.

Set $\delta(0) = \delta(1) = 1$ in the Boolean semiring A_2 (Example 2.1). It is easy to verify that (d1) holds. But $\delta(01) = 1 \not\leq 0$. Thus (d2) does not hold.

Set $\delta(0) = \delta(1) = 0$ in the same (and only) Boolean semiring. It is easy to verify that (d2) holds. But $1 \not\leq 0 = 01 = \delta(1)1$. Thus (d1) does not hold. \square

We will see in the following subsection that (d1) and (d2) together imply that $\delta(a) = 0$ iff $a = 0$.

We now show that there also is always a meaningful predomain definition for an i-semiring by choosing the discrete algebra of tests.

Lemma 4.4. *A discrete t-semiring admits precisely one predomain operation.*

Proof. Let $A \in \text{TS}$. The mapping f defined by $f : 0 \mapsto 0$ and $f : a \mapsto 1$ for all $0 \neq a \in A$ satisfies (d1) and (d2).

For (d1), if $\delta(a) = 0$ then $a = 0$. Hence $\delta(a)a = \delta(0)0 = 0 = a$. Otherwise, if $a \neq 0$ then $\delta(a) = 1$. Hence $\delta(a)a = 1a = a$.

For (d2), if $\delta(pa) = 0$ then (d2) holds trivially. Otherwise, if $\delta(pa) = 1$ then $pa \neq 0$ and therefore also $p \neq 0$. Thus $p = 1$ and (d2) also holds.

Thus δ is a well-defined predomain operation for A .

Finally, uniqueness is immediate from Lemma 4.5 (i), which will be shown in the next subsection. \square

Let us conclude this section with a remark of general interest. In opposition to relational semirings, the elements of general test-semirings are intensional, that is, they are not completely determined by the elements of the associated test algebra. For a given i-semiring there may be many test algebras that can be embedded. These and the choice of the associated (pre)domain operation determine the precision of measuring properties of the Kleenean elements. Thus our definition of domain leaves the possibility of distinguishing not only between extensional and intensional behavior, but also between different degrees of intensionality.

4.4 Predomain Calculus

A look at the relational semiring shows that the domain operation has further useful and interesting algebraic properties. We will now show that many of them can already be derived from our simple definition of predomain. We will see, however, in the remaining sections that an additional equational axiom is needed for more advanced applications. The statements of this section are useful for a more intuitive understanding of domain. They also serve as the basic library of rules in a domain calculus.

Here, we list algebraic properties of domain without discussing their counterparts in the relational model. We leave this exercise to the reader or appeal to intuition.

Lemma 4.5. *Let $A \in \text{TSP}$. Let $a, b \in A$, $p \in \text{test}(A)$ and $q \in \text{sid}(A)$.*

(i) δ is fully strict.

$$\delta(a) \leq 0 \Leftrightarrow a \leq 0. \quad (25)$$

(ii) δ is additive.

$$\delta(a + b) = \delta(a) + \delta(b). \quad (26)$$

(iii) δ is monotonic.

$$a \leq b \Rightarrow \delta(a) \leq \delta(b). \quad (27)$$

(iv) δ is an identity on tests.

$$\delta(p) = p. \quad (28)$$

(v) δ is idempotent.

$$\delta(\delta(a)) = \delta(a). \quad (29)$$

(vi) δ yields a left invariant.

$$a = \delta(a)a. \quad (30)$$

(vii) δ satisfies an import/export law.

$$\delta(pa) = p\delta(a). \quad (31)$$

(viii) δ satisfies a decomposition law.

$$\delta(ab) \leq \delta(a\delta(b)). \quad (32)$$

(ix) δ commutes with the complement operation on tests.

$$\delta(p)' = \delta(p'). \quad (33)$$

Proof. (i) $\delta(a) \leq 0 \Leftrightarrow a \leq 0a \Leftrightarrow a \leq 0$ follows from (llp). (ii) Using (gla), we calculate

$$\begin{aligned} \delta(a + b) \leq p &\Leftrightarrow p'(a + b) \leq 0 \\ &\Leftrightarrow p'a + p'b \leq 0 \\ &\Leftrightarrow p'a \leq 0 \wedge p'b \leq 0 \\ &\Leftrightarrow \delta(a) \leq p \wedge \delta(b) \leq p \\ &\Leftrightarrow \delta(a) + \delta(b) \leq 0. \end{aligned}$$

The claim then follows from the principle of indirect inequality.

(iii) Using (26), this is a standard result from lattice theory.

(iv) $p \leq \delta(p)p \leq \delta(p)$ follows immediately from (d1) and $p \leq 1$. $\delta(p) = \delta(1p) \leq p$ follows immediately from (d2).

(v) $\delta(\delta(a)) \leq \delta(a) \Leftrightarrow \delta(a) \leq \delta(a)\delta(a)$ is immediate from (llp). $\delta(a) \leq \delta(a)\delta(a)$ holds, since $\delta(a)$ is a subidentity. Now use (28).

(vi) By (d1) it remains to show that $\delta(a)a \leq a$, which is evident, since $\delta(a) \in \text{test}(A)$.

(vii) By Boolean algebra and (26) we have $\delta(a) = \delta(pa) + \delta(p'a)$. Now

$$p\delta(a) = p\delta(pa) + p\delta(p'a) = \delta(pa),$$

since $\delta(pa) \leq p$ and $\delta(p'a) \leq p'$ by (d2).

(viii) By (llp) it suffices to show that $ab \leq \delta(a\delta(b))ab$. We calculate

$$ab \leq a\delta(b)b \leq \delta(a\delta(b))a\delta(b)b \leq \delta(a\delta(b))ab.$$

(ix) Immediate from (iv). □

Most of these equations are also useful for simplifying terms on t-semirings that mention domain.

4.5 Locality and Domain Definition

Our definition of domain for t-semirings is not yet complete. There is a natural property of domain — called *locality* — that holds in the relational model but which is independent of (d1) and (d2). Namely

$$\delta(RS) = \delta(R\delta(S))$$

holds for all $R, S \in A \times A$, where A is a set. We leave the verification to the reader. Intuitively, for computing the domain of a relation RS , information about the domain of S suffices; information about the inner structure or the codomain of S is not needed.

In TSP, only one half of locality is derivable, as Lemma 4.5 (viii) shows, the other half is independent.

Lemma 4.6. *There is an $A \in \text{TSP}$ in which*

$$\delta(a\delta(b)) \leq \delta(ab). \tag{\delta 1}$$

does not hold for all $a, b \in A$.

Proof. Consider again the discrete t-semiring A_3^2 of Example 2.3. Following Lemma 4.4, the mapping $f : 0 \mapsto 0$, $f : 1 \mapsto 1$, and $f : a \mapsto 1$ is a predomain operation. Then $f(af(a)) = f(a1) = 1$ and $f(aa) = f(0) = 0$. That is, $f(aa) \leq f(a(f(a)))$ holds, but not $f(aa) = f(a(f(a)))$. □

Due to independence of locality, we add $(\delta 1)$ to the predomain axioms to define the domain operation. However, we would like to distinguish between the two definitions, since in many applications, $(\delta 1)$ is not needed.

Definition 4.2. A t-semiring with domain (a $\hat{\delta}$ -semiring) is a δ -semiring in which the predomain operation $\hat{\delta} : A \rightarrow \text{test}(A)$ also satisfies

$$\hat{\delta}(a\hat{\delta}(b)) \leq \hat{\delta}(ab), \quad (\delta 1)$$

for all $a, b \in A$. We denote the class of t-semirings with domain by TSD.

We also use the notion of δ -locality to distinguish locality of domain from that of codomain.

We now impose a necessary and sufficient condition such that a discrete δ -semiring is also a $\hat{\delta}$ -semiring. 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, that is,

$$ab \leq 0 \Rightarrow a \leq 0 \vee b \leq 0. \quad (34)$$

holds for all $a, b \in A$.

Lemma 4.7. A discrete t-semiring is a $\hat{\delta}$ -semiring iff it is integral.

Proof. Let A be a discrete t-semiring. From Lemma 4.4 we know that f defined by $f : 0 \mapsto 0$ and $f : a \rightarrow 1$ for all $0 \neq a \in A$ is the unique predomain operation on A . Thus A is a δ -semiring.

Let A be integral. We must show that $f(af(b)) \leq 0$ whenever $f(ab) \leq 0$. So let $f(ab) \leq 0$. Then the construction of f implies that $ab \leq 0$, hence $a \leq 0$ or $b \leq 0$, since there are no zero divisors. In the first case,

$$f(af(b)) = f(0f(b)) = f(0) = 0,$$

by construction of f . In the second case

$$f(af(b)) = f(af(0)) = f(a0) = f(0) = 0,$$

again by construction of f .

Now assume that f satisfies $(\delta 1)$, that is, $f(af(b)) \leq f(ab)$, and let $ab \leq 0$. Thus $f(af(b)) \leq f(ab) \leq 0$ and hence $af(b) \leq 0$ by construction of f . There are two cases.

If $f(b) = 1$ then $af(b) = a1 = a$. Hence $af(b) \leq 0$ implies $a \leq 0$.

If $f(b) = 0$ then $b = 0$ by construction of f .

Thus $ab \leq 0$ implies $a \leq 0$ or $b \leq 0$, that is, A is integral. \square

We will now show that this condition can be generalized to a sufficient condition on non-discrete t-semirings.

Lemma 4.8. Every integral δ -semiring is a $\hat{\delta}$ -semiring.

Proof. Let A be integral. Thus $ab \leq 0$ implies $a \leq 0$ or $b \leq 0$. By the principle of indirect inequality, we show

$$\delta(ab) \leq p \Rightarrow \delta(a\delta(b)) \leq p.$$

Using Theorem 4.1 (iii),

$$\begin{aligned} \delta(ab) \leq p &\Leftrightarrow p'ab \leq 0 \\ &\Rightarrow p'a \leq 0 \vee b \leq 0 \\ &\Leftrightarrow \delta(a) \leq p \vee \delta(b) \leq 0. \end{aligned}$$

In the first case $\delta(a\delta(b)) \leq \delta(a) \leq p$. In the second case,

$$\delta(a\delta(b)) = \delta(a0) = \delta(0) = 0 \leq p.$$

□

4.6 Domain in b-Monoids

Definitions for predomain have originally been given for b-monoids and b-quantales. There, the situation is considerably simpler.

First, as we have pointed out in Section 3, the entire set of subidentities of a b-monoid forms a Boolean sublattice and therefore a suitable test algebra. Second, predomain can now be defined in terms of the Galois connection

$$\delta(a) \leq p \Leftrightarrow a \leq p\top, \tag{35}$$

from which the equational axioms

$$a \leq \delta(a)\top, \tag{36}$$

$$\delta(p\top) \leq p, \tag{37}$$

$$\tag{38}$$

are obtained in a generic way (cf. [11]). Note that (35) and the equations (36) and (37) are just (llp) and the equations (d1) and (d2), when \top is replaced by a .

In fact, by Lemma 3.8, in b-monoids, (36) is equivalent to (d1) and (37) is equivalent to (d1). However, (llp) does not express a Galois connection. It is therefore rather surprising, that (d1), (d2) are equivalent to (llp) in TSP. Moreover, standard Galois theory would suggest that also (27) is needed as an equational axiom. The fact that this is not the case in TSP and therefore also in b-monoids, is rather surprising.

We will now show formally that for b-monoids, the definition of predomain via least left preservers and that via the Galois connection coincide. We also show that the requirement on the monoid cannot be much relaxed. This means that our definition of pre-domain is really non-trivial.

Lemma 4.9.

- (i) For every b -monoid, (llp) and (35) are equivalent.
- (ii) There is a d -monoid in which (llp) holds, but not (35).

Proof. (i) Immediate from Lemma 3.8 (i).

(ii) Let $\delta(0) = 0$ and $\delta(a) = 1$ for all $a \neq 0$ in the discrete t -semiring A_4^1 (Example 2.5). Then clearly (llp) holds, but (35) does not hold by Lemma 3.8 (ii). □

In a b -quantale, domain is a priori well-defined by the Galois connection.

4.7 Example Structures

We now consider some models in TSP and TSD.

Example 4.1. In the Boolean semiring A_2 (Example 2.1), the test algebra coincides with A_2 . Setting $\delta(x) = 0 \Leftrightarrow x = 0$ is compatible with the definition of f in Lemma 4.4. Thus it satisfies (d1) and (d2). Since A_2 is integral, also (δ l) holds. Moreover, this definition is unique. □

Example 4.2. In A_3^2 , the test algebra is $\{0, 1\}$. Setting $\delta(0) = 0$, $\delta(a) = 1$ and $\delta(1) = 1$ is compatible with the definition of f in Lemma 4.4. Thus it satisfies (d1) and (d2). Since A_3^2 is integral, also (δ l) holds. Moreover, this definition is unique. □

Example 4.3. The only possible test algebra of the language i -semiring (Example 2.8) is $\{\emptyset, \{\varepsilon\}\}$. We set $\delta(\emptyset) = \emptyset$ and $\delta(L) = \{\varepsilon\}$ for all $\emptyset \neq L \subseteq \Sigma^*$. This is compatible with the definition of f in Lemma 4.4. Thus it satisfies (d1) and (d2). Since the language model is integral (since it is free), also (δ l) holds. Moreover, this definition is unique. The example easily generalizes to arbitrary monoids. □

Example 4.4. In the path i -semiring (Example 2.9), the test algebra is $2^{\Sigma \cup \{\varepsilon\}}$. For a subset $S \subseteq \Sigma^*$, the set $\delta(S)$ consists of all starting (pseudo-)nodes/states of sequences in S . □

Example 4.5. In the tropical semiring, the test algebra consists solely of 0 and ∞ . Taking $\delta(\infty) = \infty$ and $\delta(n) = 0$ is compatible with the definition of f in Lemma 4.4. Thus it satisfies (d1) and (d2). Since the tropical semiring is integral, also (δ l) holds. Moreover, this definition is unique. □

These examples show that our definition of domain is meaningful in all the usual models, although non-trivial only in the relational model and the path model.

5 Codomain

In this section, we introduce an equational axiomatization of codomain for idempotent semirings and two concepts of *duality*, one based on the *opposite* of a semiring, the other one based on the operation of *converse*, that allow an automatic transfer between statements about domain and those about codomain and save half of the work in proofs.

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

$$\rho(R) = \{b \in A \mid \exists a \in A. (a, b) \in R\}.$$

For a t-semiring this suggests to define a codomain operation as a least right preserver or a greatest right annihilator. Similarly to domain, there is a property of ρ -linearity that is independent from the other postulates.

5.1 Codomain Definition

As usual in algebra, the *opposite* of a semiring $(A, +, \cdot, 0, 1)$ is the structure $(A, +, \check{\cdot}, 0, 1)$ where $a \check{\cdot} b = b \cdot a$. We denote the opposite of a semiring A by A^{opp} .

Definition 5.1. (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.

Lemma 5.1. Let A be a ρ -semiring.

(i) The mapping ρ has type $A \rightarrow \mathbf{test}(A)$.
(ii) For all $a \in A$, the element $\rho(a)$ is a least right preserver of a , that is, for all $a \in A$ and $p \in \mathbf{test}(A)$,

$$\rho(a) \leq p \Leftrightarrow a \leq ap. \quad (\text{lrp})$$

(iii) For all $a \in A$, the element $\rho(a)$ is a greatest right annihilator of a , that is, for all $a \in A$ and $p \in \mathbf{test}(A)$,

$$\rho(a) \leq p \Leftrightarrow ap' \leq 0. \quad (\text{gra})$$

(iv) ρ satisfies the following two equations.

$$a \leq a\rho(a), \quad (\text{cd1})$$

$$\rho(ap) \leq p. \quad (\text{cd2})$$

(iii) A is a $\hat{\rho}$ -semiring if also the following equation holds.

$$\hat{\rho}(\hat{\rho}(a)b) \leq \hat{\rho}(ab). \quad (\rho\hat{\rho})$$

The proof is immediate from the definition and the results for predomain and domain in Section 4. More generally, all results of this section carry over to precodomain and codomain. Therefore we will only quote properties of domain even when talking about the codomain operation.

We call a t-semiring with predomain and precodomain a $\delta\rho$ -semiring and a t-semiring with domain and codomain a $\hat{\delta}\hat{\rho}$ -semiring. When we do not want to distinguish, we uniformly speak about *test semirings with domain* and denote the associated class by TSD.

Lemma 5.2. *There is a non-integral $\hat{\delta}\hat{\rho}$ -semiring.*

Proof. We have seen that (d1), (d2), (δ 1), and (cd1), (cd2), (ρ 1), respectively, hold in the relational model. However it is obvious that set-theoretic relations need not be integral. Let R relate all even numbers and S all odd numbers on \mathbb{N} . Then $R \neq \emptyset \neq S$, but $RS = \emptyset$. \square

5.2 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.

Definition 5.2. (i) *An i-semiring with pre-converse is a structure (A, \circ) such that A is an i-semiring and $\circ : A \rightarrow A$ is an operation that satisfies the following equations.*

$$a^{\circ\circ} = a, \tag{c1}$$

$$(a + b)^{\circ} = a^{\circ} + b^{\circ}, \tag{c2}$$

$$(ab)^{\circ} = b^{\circ}a^{\circ}. \tag{c3}$$

(ii) *An i-semiring with weak converse is an i-semiring with pre-converse such that all $p \leq 1$ satisfy*

$$p^{\circ} \leq p. \tag{c4}$$

(iii) *An i-semiring with converse [10] is an i-semiring with pre-converse that satisfies the equation*

$$a \leq aa^{\circ}a. \tag{c5}$$

It is easy to show that the properties

$$1^{\circ} = 1, \tag{39}$$

$$0^{\circ} = 0, \tag{40}$$

$$a \leq b \Leftrightarrow a^{\circ} \leq b^{\circ} \tag{41}$$

hold in every i-semiring with pre-converse. The equation

$$p^{\circ} = p \tag{42}$$

holds in every i-semiring with weak converse. Moreover, every i-semiring with converse is an i-semiring with weak converse.

Using the operation of converse we can express the duality between domain and codomain *within* the test-semiring rather than at the meta-level.

Proposition 5.1. *Let A be a $\delta\rho$ -semiring (or a $\hat{\delta}\hat{\rho}$ -semiring) with weak converse. Then for all $a \in A$,*

$$\delta(a^\circ) = \rho(a), \quad (43)$$

$$\rho(a^\circ) = \delta(a). \quad (44)$$

Proof. We only show (43), verifying that $\delta(a^\circ)$ satisfies Definition 5.1 of codomain.

(cd1) By (d1), $a^\circ \leq \delta(a^\circ)a^\circ$, thus

$$a = a^{\circ\circ} \leq (\delta(a^\circ)a^\circ)^\circ = a^{\circ\circ}(\delta(a^\circ))^\circ = a\delta(a^\circ).$$

(cd2) By (d2),

$$\delta((ap)^\circ) = \delta(p^\circ a^\circ) = \delta(pa^\circ) \leq p.$$

(ρ l) By (δ l),

$$\delta((ab)^\circ) = \delta(b^\circ a^\circ) = \delta(b^\circ \delta(a^\circ)) = \delta(b^\circ (\delta(a^\circ))^\circ) = \delta((\delta(a^\circ)b)^\circ).$$

The proof of (44) is dual. \square

We could therefore take (43) as definition of codomain in a t-semiring with weak converse.

Corollary 5.1. *Let A be a $\delta\rho$ -semiring with weak converse. For all $a \in A$, $p \in \text{test}(A)$,*

$$\delta(a^\circ p) = \rho(pa), \quad (45)$$

$$\rho(a^\circ p) = \delta(pa). \quad (46)$$

5.3 Equivalence of δ -Locality and ρ -Locality

It may come as a surprise that domain and codomain enjoy perfect symmetry with respect to locality of composition. We prepare the proof by an auxiliary property.

Lemma 5.3. *A $\delta\rho$ -semiring A satisfies (δ l) iff for all $a, b \in A$,*

$$ab \leq 0 \Leftrightarrow \rho(a)\delta(b) \leq 0. \quad (47)$$

Proof. We first show that (δ l) implies (47).

$$\begin{aligned} ab \leq 0 &\Leftrightarrow \delta(ab) \leq 0 \\ &\Leftrightarrow \delta(a\delta(b)) \leq 0 \\ &\Leftrightarrow a\delta(b) \leq 0 \\ &\Leftrightarrow \rho(a) \leq \delta(b)' \\ &\Leftrightarrow \rho(a)\delta(b) \leq 0. \end{aligned}$$

The first and third step of the proof use (25), the second step uses ($\delta 1$), the fourth step uses (gra) and the last step is by Boolean algebra.

Now we show that (47) implies ($\delta 1$). First, by (31) $\rho(a)\delta(b) = \rho(a\delta(b))$ and therefore, by (25)

$$ab \leq 0 \Leftrightarrow a\delta(b) \leq 0. \quad (48)$$

Using Boolean algebra, (48) thrice and Boolean algebra again, we calculate

$$\begin{aligned} \delta(ab) \leq p &\Leftrightarrow p'\delta(ab) \leq 0 \\ &\Leftrightarrow p'ab \leq 0 \\ &\Leftrightarrow p'a\delta(b) \leq 0 \\ &\Leftrightarrow p'\delta(a\delta(b)) \leq 0 \\ &\Leftrightarrow \delta(a\delta(b)) \leq p, \end{aligned}$$

whence $\delta(ab) = \delta(a\delta(b))$ by the principle of indirect inequality. \square

Since (47) is symmetric in δ and ρ , we obtain

Corollary 5.2. *A $\delta\rho$ -semiring is a $\hat{\delta}$ -semiring iff it is a $\hat{\rho}$ -semiring.*

6 Image and Preimage

In many applications, domain and codomain operations occur more specifically as *image* and *preimage* operations for some given test element. In the relational semiring, the preimage of a set $B \subseteq A$ under a relation $R \subseteq A \times A$ is defined as

$$R:B = \{x \in A \mid \exists y \in B. (x, y) \in R\}.$$

We leave it to the reader to verify that this is equivalent to the point-free definition $R:B = \delta(RB)$. Dually, the image of B under R is defined as

$$B:R = \{y \in A \mid \exists x \in A. (x, y) \in R\},$$

which is equivalent to the point-free definition by $B:R = \rho(BR)$.

As usual, we abstract this point-free definition from sets to semirings and define for every $A \in \text{TSP}$, the *image* and the *preimage operator*, both denoted by $:$, as mappings of type $\text{test}(A) \times A \rightarrow \text{test}(A)$ and $A \times \text{test}(A) \rightarrow \text{test}(A)$ by

$$p:a = \rho(pa), \quad (49)$$

$$a:p = \delta(ap). \quad (50)$$

for all $a \in A$ and $p \in \text{test}(A)$. We henceforth use this notation and avoid domain and codomain whenever this is appropriate. In particular, we often use $a:1$ and $1:a$ instead of $\delta(a)$ and $\rho(a)$. We also overload this notation to definitions with respect to $\hat{\delta}$ and $\hat{\rho}$. Since the preimage and the image operator are multiplications, we stipulate that they bind stronger than addition.

Moreover, since image and preimage are defined by codomain and domain and since codomain and domain are coupled via the concept of opposition, there is again an automatic transfer between properties of image and those of preimage. Like in previous sections, we therefore only mention properties of preimage and quote preimage properties even when talking about the image operation.

The following lemma connects preimage with least left preservation and annihilation. Like (llp) and (gla), this allows us to eliminate certain occurrences of preimage and image operators.

Lemma 6.1. *Let $A \in \text{TSP}$. For all $a \in A$ and $p \in \text{test}(A)$,*

$$a:p \leq q \Leftrightarrow ap \leq qa, \quad (51)$$

$$a:p \leq q \Leftrightarrow q'ap \leq 0. \quad (52)$$

Proof. Immediate from (llp), and Lemma 3.7, respectively. \square

From (31) we get the following import/export rule for the preimage.

Corollary 6.1. *Let $A \in \text{TSP}$. For all $a \in A$ and $p, q \in \text{test}(A)$,*

$$(p:a)q = p:(aq). \quad (53)$$

Lemma 6.1 has the following consequence, that couples preimage and image operations.

Lemma 6.2. *Let $A \in \text{TSP}$. The preimage and the image operation satisfies the following exchange law. For all $a \in A$ and $p \in \text{test}(A)$,*

$$a:p \leq q \Leftrightarrow q':a \leq p'. \quad (54)$$

Proof. Immediate from Lemma 6.1 and Lemma 3.7. \square

The equivalence (54) and its dual are weak analoga of the Schröder rules from the relational calculus. Lemma 6.2 has the following immediate consequence.

Corollary 6.2. *Let $A \in \text{TSP}$. For all $a \in A$ and $p \in \text{test}(A)$,*

$$(p:a)q \leq 0 \Leftrightarrow p(a:q) \leq 0. \quad (55)$$

Finally, locality yields the following interaction of domain with preimage and of codomain with image.

Lemma 6.3. *Let $A \in \text{TSD}$. Then for all $a, b \in A$,*

$$\hat{\delta}(ab) = a:\hat{\delta}(b), \quad (56)$$

$$\hat{\rho}(ab) = \hat{\rho}(a):b. \quad (57)$$

7 Domain, Codomain and Kleene Star

So far, we have only investigated domain and codomain operations in test-semirings, that is, in absence of the Kleene star operation. In fact, there is no need for further axioms in presence of Kleene star. Therefore, in this section, we only need to investigate the interaction of domain and codomain and that of image and preimage with the Kleene star. It turns out that only image and preimage show nontrivial behaviour. In particular we will see that when the Kleene star is adapted to occur within domain and codomain operators, a finite equational axiomatization instead of the Horn clauses (*-3) and (*-4) is possible. Moreover, one of these equational axioms can be interpreted as an efficient reachability algorithm, when interpreted over finite relations; its proof is by a formal derivation from a less efficient specification.

Henceforth K-semirings are called $K\delta$ -semirings, $K\rho$ -semirings, $K\hat{\delta}$ -semirings, $K\hat{\rho}$ -semirings, $K\delta\rho$ -semirings and $K\hat{\delta}\hat{\rho}$ -semirings, when they are extended by the respective operation(s) and defined by the respective axioms. Moreover, when we do not want to distinguish, we uniformly speak of *Kleene algebra with predomain* or *Kleene algebra with domain*. We denote the classes by KAP and KAD.

First, the properties of the Kleene star from Lemma 2.1 have some trivial consequences for domain and codomain.

Lemma 7.1. *Let $A \in \text{KAP}$. Then for all $a \in A$,*

$$\delta(a)^* = 1, \quad (58)$$

$$\delta(a^*) = 1. \quad (59)$$

The Kleene star in combination with images or preimages has a much richer and more interesting behaviour. The following three statements show that preimages in combination with star satisfy expressions analogous to (*-1) and (*-2) for K-semirings. Like their counterparts in KA, they are the working horses for many interesting derivations. We give variants for KAD, because presence of ($\delta 1$), that is, $(ab):p = a:(b:p)$, allows a more compositional treatment of images and preimages.

Lemma 7.2. *Let $A \in \text{KAP}$. For all $a \in A$ and $p \in \text{test}(A)$,*

$$p + a^*:(a:p) \geq a^*:p \leq p + a:(a^*:p), \quad (60)$$

The inequalities become equations, when $A \in \text{KAD}$.

Proof. By (*-1),

$$a^*:p = (1 + a^*a):p = (1:p) + (a^*a:p) \geq p + a^*:(a:p).$$

The last step uses (32). The second half of (60) is shown analogously. The equations follow by using ($\delta 1$) instead of (32). \square

Note the analogy to the variants $b + a^*ab = a^*b$ and $b + aa^*b = a^*b$ of (*-2) and (*-1) in KA. By (60), $a^*:p$ is a fixed point of the mapping $\lambda x.p + a:x$.

Lemma 7.3. *Let $A \in \text{KAD}$. For all $a \in A$ and $p \in \text{test}(A)$,*

$$a:p \leq p \Rightarrow a^*:p \leq p. \quad (61)$$

Proof. Using Lemma 6.1 (11), we calculate

$$a:p \leq p \Leftrightarrow ap \leq pa \Rightarrow a^*p \leq pa^* \Leftrightarrow a^*:p \leq p.$$

□

Lemma 7.3 can also be viewed as an assertion about invariants: an invariant of a is also an invariant of a^* . Moreover, it has two important consequences. First, we will use it in the following lemma to derive more efficient variants of the statements of Lemma 7.2. Second, when the Kleene star is adapted to occur only within preimages, we will show in the following lemma that there are even equivalent equational characterizations.

Lemma 7.4. *Let $A \in \text{KAD}$. Let $a \in A$ and $p, q \in \text{test}(A)$. The following properties are equivalent and hold in KAD.*

$$a:p \leq p \Rightarrow a^*:p \leq p, \quad (62)$$

$$a:p + q \leq p \Rightarrow a^*:q \leq p, \quad (63)$$

$$a^*:p \leq p + a^*:(p'(a:p)), \quad (64)$$

$$a^*:p = p + (ap')^*:(a:p). \quad (65)$$

Proof. We first show that (62), (63) and (64) are equivalent.

(62) implies (63). $a:p + q \leq p$ iff $a:p \leq p$ and $q \leq p$ and therefore $a^*:p \leq p$ by the assumption. Hence also $a^*:q \leq p$.

(63) implies (64). For $a^*:p \leq p + a^*:(p'(a:p))$ it suffices by (63) to show that

$$\begin{aligned} p &\leq p + a^*:(p'(a:p)), \\ a:(p + a^*:(p'(a:p))) &\leq p + a^*:(p'(a:p)). \end{aligned}$$

The first inequality is trivial. The second one is proved as follows.

$$\begin{aligned} a:(p + a^*:(p'(a:p))) &= (a:p) + a:(a^*:(p'(a:p))) \\ &= (p + p')(a:p) + a:(a^*:(p'(a:p))) \\ &\leq p + (p'(a:p)) + a:(a^*:(p'(a:p))) \\ &= p + a^*:(p'(a:p)). \end{aligned}$$

The third step uses $p(a:p) \leq p$; the last step uses $q = 1;q$ and (60).

(64) implies (62). Let $a^*:p \leq p + a^*:(p'(a:p))$ and assume $a:p \leq p$. Then

$$a^*:p \leq p + a^*:(p'(a:p)) \leq p + a^*:(p'p) = p + a^*:0 = p + 0 = p.$$

We now show that (63) implies (65) and that (65) implies (62). This yields simpler proofs than a direct circle.

(63) implies (65). First, $p + (ap')^*:(a:p) \leq p + a^*:(a:p) = a^*:p$ by monotonicity of the Kleene star, the fact that $p \leq 1$ and $(\delta 1)$.

For the converse direction, that is, $a^*:p \leq p + (ap')^*:(a:p)$, it suffices by (63) to show that

$$\begin{aligned} p &\leq p + (ap')^*:(a:p), \\ a:(p + (ap')^*:(a:p)) &\leq p + (ap')^*:(a:p). \end{aligned}$$

The first inequality is trivial. The second one is proved as follows.

$$\begin{aligned} a:(p + (ap')^*:(a:p)) &= (a:p) + a(p + p'):(ap')^*:(a:p) \\ &= (a:p) + (ap):(ap')^*:(a:p) + (ap'):(ap')^*:(a:p) \\ &\leq (a:p) + (ap):1 + (ap'):(ap')^*:(a:p) \\ &\leq (a:p) + ap':(ap')^*:(a:p) \\ &= (ap')^*:(a:p) \\ &\leq p + (ap')^*:(a:p). \end{aligned}$$

The first two steps use additivity of domain, the third step uses that $(ap)^*:(a:p) \leq 1$, the fourth step uses that $(ap):1 = a:p$, the fifth step uses (61).

(65) implies (62). Assume $a:p \leq p$. Then

$$\begin{aligned} a^*:p &= p + (ap')^*:(a:p) \\ &\leq p + (ap')^*:p \\ &= p + (ap')^*:(ap'):p \\ &= p + (ap')^*:0 \\ &= p. \end{aligned}$$

The third step uses (61), the fourth step uses that $(ap'):p = \delta(app') = \delta(0) = 0$, the fifth step uses (25).

Finally, it remains to show that (61), (63), (64) and (65) hold in KAD. This holds, since, by Lemma 7.3, the expression (61) holds, to which the other expressions are equivalent. \square

Note the analogy of (63) to $b + ac \leq c \Rightarrow a^*b \leq c$, that is, (*-3).

Corollary 7.1. *Let $A \in \text{KAD}$. For all $a, b, c \in A$ and $p \in \text{test}(A)$,*

$$(ac):p + b:q \leq c:p \Rightarrow (a^*b):q \leq c:p, \quad (66)$$

Proof. The expression (66) follows immediately from (63), replacing p by $c:p$, q by $b:q$ and using $(\delta 1)$. \square

Already (60) describes an unfolding step of the preimage operation. However, this is not the most efficient way of unfolding. In $a^*:p = p + a^*:(a:p)$, for instance, it is not necessary to perform a full a -iteration from $a:p$. Since all steps starting from p have already been considered, it suffices to perform the a -iteration from p' -states. This is expressed by (65).

The following example show that the mappings from test sets to test sets in a KAD again induce a K-semiring.

Example 7.1. (An algebra of predicate transformers) Let $A \in \text{KAD}$ and consider for all $a \in A$ the set F_A of mappings $f_a = \lambda x.(a:x)$. We write $f_a(p) = a:p$ and define addition and multiplication on F_A by

$$(f_a \oplus f_b)(p) = f_a(p) + f_b(p), \quad (67)$$

$$(f_a \odot f_b)(p) = f_a(f_b(p)). \quad (68)$$

for all $p \in \text{test}(A)$. Then it is easy to verify that $(F_A, \oplus, \odot, f_0, f_1)$ is a t-semiring with set of tests $\{f_p \mid p \in \text{test}(A)\}$. Moreover, setting

$$f_a^*(p) = a^*:p, \quad (69)$$

we obtain

$$f_1 \oplus (f_a \odot f_a^*) = f_a^*, \quad (70)$$

$$f_1 \oplus (f_a^* \odot f_a) = f_a^* \quad (71)$$

from the first half of (60) and

$$f_b \oplus (f_a \odot f_c) \leq f_c \Rightarrow f_a^* \oplus f_b \leq f_c \quad (72)$$

from (66). Hence $(F_A, \oplus, \odot, f_0, f_1, (\cdot)^*)$ is a “left-handed” K-semiring. \square

8 Kleene Algebras as Varieties

In this section we classify some of our results in the context of universal algebra.

We identify varieties with equational classes. A variety is *finitely based* if it can be axiomatized by a finite set of equations. The following lemma is immediate.

Lemma 8.1. *TSD is a finitely based variety.*

The next lemma is not so immediate. It has been shown in [24,35] that KA with a residuation operation is a finitely based variety. The same phenomenon might occur when adding a domain or codomain operation. The following lemma shows that this is not the case. A similar argument has been used in [20] for algebras related to PDL.

Lemma 8.2. *KAP and KAD are not finitely based varieties.*

Proof. In [9], p. 106, Conway gives an algebra A_p for showing that the algebra of regular events (c.f. Example 2.8) is not finitely based. For every finite set of equations and every prime p there is a particular valid equation parameterized by p that is not deducible and there is an algebra A_p parameterized by p that satisfies the finite set of equations, but not the given additional equation. According to Conway, every expression in the language of KA is equivalent to some sum of terms each of which is either 0 or 1 or is simultaneously 0-free, 1-free

and $+$ -free. This implies that in A_p , which is constructed from such normal form terms, $ab \leq 0$ implies that $a \leq 0$ or $b \leq 0$, thus the integral condition (34) holds.

Now in presence of domain, we consider the discrete t-semiring on A_p . Then by Lemma 4.4 and Lemma 4.7, the mapping defined by $\delta(0) = 0$ and $\delta(a) = 1$ for all $0 \neq a \in A_p$ satisfies (d1), (d2) and (δ 1). In particular $0 \neq 1$.

Thus the expansion of A_p satisfies the finite set of equations and the domain axioms, but not the given additional equation. Consequently, the given finite set of equation is not complete for KAP and KAD. \square

However, Lemma 7.4 shows that the extensional behaviour of the Kleene star can be defined equationally using only equations on the test algebra.

Lemma 8.3. *The classes of test subalgebras on KAP and KAD are finitely based varieties.*

9 Reconstructing Noethericity

In this section we demonstrate the expressive power and applicability of KAD in the field of termination analysis of programs. We show that concepts of Noethericity and well-foundedness can be algebraically reconstructed. We further show that our concepts subsume those in Cohen's ω -algebra [8], an extension of KA with infinite iteration that is defined as a greatest fixed point by expressions similar to (*-1), (*-2), (*-3) and (*-4). Moreover we show that for transitive relations our concept is also equivalent to an algebraic variant of Löb's formula from modal logic [5,6]. In particular, this last example is very interesting, since our proof uses an interaction of images and preimages that could not be modeled, for instance, in dynamic logic. Finally, we show that some simple and well-known properties of well-founded relations can be calculated in KAD in a simple and elegant way.

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, \dots 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, \dots 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,

$$P \subseteq P:R. \tag{73}$$

Consequently, if R is well-founded, then only the empty set may satisfy (73).

9.1 Noethericity: Definition and Simple Properties

Abstracting to $A \in \text{TSD}$ we say that a is *well-founded* if for all $p \in \text{test}(A)$,

$$p \leq p:a \Rightarrow p \leq 0. \tag{74}$$

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

$$p \leq a:p \Rightarrow p \leq 0. \quad (75)$$

We now calculate abstract algebraic variants of some simple and well-known properties of well-founded and Noetherian relations. Again, as in previous sections, we restrict our attention to Noethericity, which is expressed in terms of preimages. We do not explicitly mention well-foundedness properties that hold by duality in the opposite semiring.

Lemma 9.1. *Let $A \in \text{KAD}$. Let $a, b \in A$ and let $0 \neq 1$.*

- (i) 0 is *Noetherian*.
- (ii) 1 is not *Noetherian*.
- (iii) If b is *Noetherian* and $a \leq b$, then a is *Noetherian*.
- (iv) If a is *Noetherian*, then $1 \not\leq a$, that is, a is *irreflexive*.
- (v) If $a \not\leq 0$ is *Noetherian* then $a \not\leq aa$, that is, a is not *dense*.
- (vi) a is *Noetherian* iff a^+ is *Noetherian*.
- (vii) a^* is not *Noetherian*.

Proof. (i) Let $p \leq 0:p$. Then $p \leq 0$, since $0:p = 0$.

(ii) The equation $p \leq 1:p$ holds for all $p \in \text{test}(A)$, thus in particular for $p = 1$. But $1 \not\leq 0$.

(iii) Let a be *Noetherian*, that is, $p \leq p:a$ implies $p \leq 0$ and let $b \leq a$. Then

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

Thus b is *Noetherian*.

(iv) Let a be *Noetherian* and $1 \leq a$. Then, by (iii), 1 is *Noetherian*, a contradiction.

(v) Let a be *dense* and *Noetherian*. $a \leq aa$ implies $a:p \leq a:(a:p)$, by monotonicity. Thus $a:p \leq 0$ for all $p \in \text{test}(A)$. The particular case $p = 1$ yields $a \leq 0$, a contradiction.

(vi) Let a be *Noetherian* and remember that $a^+ = aa^*$. We calculate

$$\begin{aligned} p \leq a^+:p &\Rightarrow a^*:p \leq a^*:(a^+:p) \\ &\Leftrightarrow a^*:p \leq a:(a^*:p) \\ &\Rightarrow a^*:p \leq 0 \\ &\Rightarrow 1:p \leq 0 \\ &\Leftrightarrow p \leq 0. \end{aligned}$$

The second step uses $(\delta 1)$, $a^*a^* = a^*$ and $aa^* = a^*a$. The third step uses *Noethericity* of a . The fourth step uses $1 \leq a^*$. Thus a^+ is *Noetherian*.

Now let a^+ be *Noetherian*. Then, by (iii) and $a \leq a^+$, a is *Noetherian*.

(vii) By (ii), 1 is not *Noetherian*. Then $1 \leq a^*$ implies that a^* is not *Noetherian* using (iii). \square

9.2 Noethericity and ω -Algebra

We now show how our definition of Noethericity is related to the property of Noethericity as it is defined in Cohen's ω -algebra. We do not introduce the axioms for this class. Intuitively, while an expression a^* denotes finite non-deterministic iteration of a , a^ω denotes infinite iteration. As an ω -regular expression, a^ω therefore denotes a set of words of infinite length or streams. Consequently, in ω -algebra Noethericity of a means absence of infinite iteration of a ; thus $a^\omega = 0$. In our calculations we only need the following properties of a^ω .

$$a^\omega \leq aa^\omega, \quad (76)$$

$$a \leq a^\omega. \quad (77)$$

Lemma 9.2. *Let A be an ω -algebra that is also a $\hat{\delta}$ -semiring. Then for all $a \in A$, if a is Noetherian then $a^\omega = 0$.*

Proof. Let a be Noetherian. Using ($\delta 1$) we obtain

$$\delta(a^\omega) \leq \delta(aa^\omega) = \delta(a\delta(a^\omega)) = a:\delta(a^\omega).$$

Thus $\delta(a^\omega) = 0$ by definition (75) of Noethericity. By strictness of domain (Lemma 4.5 (i)), this is the case if and only if $a^\omega = 0$.

The converse implication does not hold. In the language semiring we have $a^\omega = 0$ if $1 \sqcap a = 0$, but also

$$a \neq 0 \Rightarrow \forall p. a:p = p.$$

Note that ω -algebra can only express Noethericity, whereas TSD can express both Noethericity and well-foundedness.

9.3 Noethericity and the Löb Axiom

We now investigate an alternative characterization of Noethericity for transitive relations that is even equational. Remember that an element of a semiring is transitive if $aa \leq a$.

In modal logic, Noethericity of the underlying Kripke frame is characterized by Löb's axiom

$$\Box(\Box p \rightarrow p) \rightarrow \Box p$$

(cf. [5,6]). Translating $p \rightarrow q$ as $p' + q$ and validity of p as $1 \leq p$ we calculate as follows.

$$\begin{aligned} 1 \leq \Box(\Box p \rightarrow p) \rightarrow \Box p &\Leftrightarrow 1 \leq (\Box(\Box p \rightarrow p))' + \Box p \\ &\Leftrightarrow (\Box p)' \leq (\Box(\Box p \rightarrow p))' \\ &\Leftrightarrow \Diamond p' \leq \Diamond((\Box p)' + p)' \\ &\Leftrightarrow \Diamond p' \leq \Diamond((\Box p)p') \\ &\Leftrightarrow \Diamond p' \leq \Diamond((\Diamond p')'p'). \end{aligned}$$

Passing now to a multimodal view and replacing diamonds by preimage operators, we obtain the following representation of Löb's axiom in KAD.

$$a:p \leq a:(p(a:p)'). \quad (78)$$

We say that a is *Löbian* if it satisfies (78). In the relational model, Löb's axiom states that a is transitive and that there are no infinite a -chains. Note the surprising similarity to (64).

We will now relate Löb's axiom and our notion of Noethericity. But first we need a technical lemma.

Lemma 9.3. *Let $A \in \text{TSD}$. Let $a \in A$ and $p, q \in \text{test}(A)$.*

- (i) $p \leq (a:q)' \Leftrightarrow p:a \leq q'$.
- (ii) $aa \leq a \wedge p \leq (a:q)' \Rightarrow p:a \leq (a:q)'$.

Proof. (i) Immediate from the exchange law (54).

(ii) We calculate

$$p \leq (a:q)' \Leftrightarrow a:q \leq p' \Rightarrow a:(a:q) \leq p' \Leftrightarrow p:a \leq (a:q)'.$$

The first and last step use (i), the second step uses transitivity and ($\delta 1$). \square

The statement of the following theorem is closely related to the correspondence theory of modal logic. In this view, our property of Noethericity expresses a frame property, which is part of semantics, whereas our Löb axiom stands for a modal formula, which is part of syntax. In TSD we are able to express syntax and semantics in the same formalism. Moreover, while the traditional proof of correspondence uses an (informal) semantic argument, our proof is entirely calculational.

Theorem 9.1. *Let $A \in \text{TSD}$ and $a \in A$.*

- (i) *If a is Löbian then a is Noetherian.*
- (ii) *If a is Noetherian and transitive then a is Löbian.*

Proof. (i) Let $p \leq a:p$. Thus equivalently $p(a:p)' \leq 0$ by Boolean algebra. Insertion into (78) yields

$$p \leq a:p \leq a:(p(a:p)') \leq a:0 = 0.$$

(ii) Since the calculation of the Löb axiom is rather involved and depends on the interaction of images and preimages, we first give an informal account of the proof. Intuitively, the Löb axiom

$$a:p \leq a:(p(a:p)')$$

states that whenever there is an a -step into p , then there is also an a -step into the subset $\tau(p) = p(a:p)'$ of p from which no more a -steps into p are possible

(the *terminal part* of p). Thus for all p and forall a -steps into p there is an a -step into $\tau(p)$. Equivalently to (78), $q = (a:p)(a:\tau(p))'$, the set from which some a -step leads into p and none into the terminal part of p , must be empty. Now, if a is Noetherian it suffices to show that $q \leq a:q$. Is this the case? When a is transitive, then all predecessors of states that lead into p and $\tau(p)$ also lead into $\tau(p)$. Equivalently, all successors of states leading into p , but not into $\tau(p)$ must not lead into $\tau(p)$ and must therefore be accessible from q .

We now formally reconstruct this informal argument.

First, note that (78) is equivalent to $q = 0$ by Boolean algebra. By (75) it then suffices to show that $q \leq a:q$.

Second, note that $q \leq a:p$.

Third, let the successors of q in p be given by $r = (q:a)p$. We now show that $q \leq a:r$.

$$q(a:r) = \delta(qar) = \delta(qa\rho(qa)p) = \delta(qap) = q\delta(ap) = q.$$

The first step uses the definition of preimage and the import/export law (31). The second step expands $r = \rho(qa)p$. The third step uses (cd1). The fourth step uses again import/export. The last step uses $q \leq a:p$.

Fourth, it remains to show that $r \leq q$ and hence, by monotonicity, also $q \leq a:q$.

Since $q \leq (a:\tau p)'$, Lemma 9.3 (ii) yields that $q:a \leq (a:\tau p)'$ and hence also $r \leq (a:\tau p)'$.

Since $q \leq (a:\tau p)'$, Lemma 9.3 (i) shows $q:a \leq (\tau p)'$, hence $(q:a)p \leq p(\tau p)'$. But

$$p = p((a:p) + (a:p)') = p(a:p) + p(a:p)' = p(a:p) + \tau p,$$

so that $p(\tau p)' = p(a:p) \leq a:p$ and therefore also $r \leq a:p$. \square

Further investigations of Noethericity in the context of KAD are outside the scope of the present paper.

10 Reconstructing Hoare Logic

In this section we consider another application of KAD: the subsumption of propositional Hoare logic. This subsumption is a popular exercise for many logics and algebras for imperative programming languages. Hoare logic has, for instance, already been embedded into PDL [16] and KAT [26]. Since KAD is an extension of KAT, our subsumption result is no surprise. However we believe that it is interesting for three reasons. First, in KAD, an encoding of the inference rules of the Hoare calculus is much more crisp and clear and so are their correctness proofs. In general, Hoare-style reasoning about programs can be done in a more flexible way. Second, the properties of the standard partial correctness semantics [29,3] for Hoare logic mirror precisely those of domain, such that KAD may be considered a natural abstract algebraic semantics for propositional Hoare logic. Third, Hoare logic is an example where domain expressions can be completely eliminated from all expressions, using (gla). Even more, we will see

that all inference rules of Hoare logic can be translated into Horn clauses in KAT, where all antecedents are of the form $p = 0$. A technique for hypothesis elimination [7,26,27] yields decidability of this fragment.

First, we encode the relevant programming constructs in KA.

$$a ; b = ab \quad (79)$$

$$\text{if } p \text{ then } a \text{ else } b = pa + p'b, \quad (80)$$

$$\text{while } p \text{ do } a = (pa)^*p'. \quad (81)$$

We now briefly recall the syntax and semantics of Hoare logic. The basic formulas are *partial correctness assertions* of the form $\{p\} a \{q\}$, where p and q (the *precondition* and *postcondition*) denote Boolean expressions and a a program. Intuitively, p models a property of the input states of a program, while q models a property that is intended to hold at the output states. The program a is intuitively interpreted as a relation between input and output states. Traditionally, the Hoare calculus uses the following inference rules for reasoning about programs.

$$\begin{array}{l} \text{Assignment} \quad \frac{}{\{p[e/x]\} x := e \{p\}}, \\ \text{Composition} \quad \frac{\{p\} a \{q\} \quad \{q\} b \{r\}}{\{p\} a ; b \{r\}}, \\ \text{Conditional} \quad \frac{\{p \wedge q\} a \{r\} \quad \{p' \wedge q\} b \{r\}}{\{q\} \text{ if } p \text{ then } a \text{ else } b \{r\}}, \\ \text{While} \quad \frac{\{p \wedge q\} a \{q\}}{\{q\} \text{ while } p \text{ do } a \{p' \wedge q\}}, \\ \text{Weakening} \quad \frac{p_1 \rightarrow p \quad \{p\} a \{q\} \quad q \rightarrow q_1}{\{p_1\} a \{q_1\}}. \end{array}$$

Assignment is a non-propositional inference rule that deals with the internal structure of states. It is therefore disregarded in the embedding. Following [26], we call the fragment of Hoare logic without assignments *propositional Hoare logic* (PHL). Following [26] further, we define partial correctness assertions in KAT by

$$\{p\} a \{q\} \Leftrightarrow paq' \leq 0.$$

Using (52), we can rewrite this definition more directly as

$$\{p\} a \{q\} \Leftrightarrow p:a \leq q. \quad (82)$$

Accordingly, the inference rules of PHL can be encoded as

$$\begin{array}{l} \text{Composition} \quad p:a \leq q \wedge q:b \leq r \Rightarrow p:(ab) \leq r, \\ \text{Conditional} \quad (pq):a \leq r \wedge (p'q):b \leq r \Rightarrow q:(pa + p'b) \leq r, \\ \text{While} \quad (pq):a \leq q \Rightarrow q:((pa)^*p') \leq p'q, \\ \text{Weakening} \quad p_1 \leq p \wedge p:a \leq q \wedge q \leq q_1 \Rightarrow p_1:a \leq q_1. \end{array}$$

Theorem 10.1. *The encoded rules of PHL are derivable in KAP. Therefore PHL is sound with respect to this algebraic semantics.*

Proof. (i) (Composition)

$$p:(ab) \leq (p:a):b \leq q:b \leq r.$$

The first step uses (32), the second one the assumption and monotonicity.

(ii) (Conditional)

$$q:(pa + p'b) = (pq):a + (p'q):b \leq r + r = r.$$

(iii) (While)

$$(pq):a \leq q \Rightarrow q:(pa)^* \leq q \Rightarrow (q:(pa)^*)p' \leq qp' \Rightarrow q:((pa)^*p') \leq p'q.$$

The first step uses import/export (31) and (61). The third step uses again import/export.

(iv) (Weakening)

$$p_1:a \leq p:a \leq q \leq q_1.$$

Soundness of PHL means in our context that for every partial correctness assertion that can be proved in this calculus there is a calculation in KAD using translated statements. This follows by induction on the structure of proofs in PHL and our previous considerations. \square

Thus, given our domain calculus from the previous sections, soundness of PHL can be proved literally in four lines. Compared to the KAT-based approach in [26], we believe that our encodings and proofs in KAD are more concise, elegant and intuitive. Compared to standard set-theoretic proofs in textbooks (c.f [3,29]), our proof is about ten times shorter, without taking into account the fact that many logical and set-theoretic assumptions are left implicit in the textbook proofs and the proofs are only semi-formal.

Moreover, it has already been observed in [26] that all Horn clauses built from partial correctness assertions in Hoare logic that are valid with respect to the standard semantics are derivable in KAT. This result holds a fortiori for KAD. PHL is too weak to derive all such formulas [26].

A further investigation of PHL in KAP, notably a fully algebraic completeness proof, can be found in [30]. As a conclusion, we can only support [26] that given Kleene algebra, *the specialized syntax and deductive apparatus of Hoare logic are inessential and can be replaced by simple equational reasoning.* We also believe that KAD offers even further advantages. It allows us to combine the intuitiveness and readability of specifications in Hoare logic and imperative program semantics with the computational power of KAT. And finally, Kleene algebra offers at least an elegant formal calculus and a simple algebraic semantics for reasoning in and about Hoare logic.

11 Conclusion and Further Work

We have presented equational axioms for domain and codomain for certain idempotent semirings and extended these notions to KAD. This algebraic abstraction is intended as a unified view on approaches to program analysis and development as different as PDL, KAT, B and Z. We have outlined a calculus for KAD, defined preimage and image operators and presented two applications of KAD: an algebraic reconstruction of the notions of Noethericity and the subsumption of propositional Hoare logic. These and most of the other results in this text provide the foundations and introduce the basic calculus of KAD. They are the basis for further interesting work.

On the theoretical side, expressibility, complexity, completeness or representability of KAD have not been investigated in this text. The same holds for the apparent relation to modal algebras and in particular algebraic variants of PDL (cf. e.g. [14]).

On the practical side, it might be interesting to continue our investigations of termination analysis and greedy algorithms [31]. Moreover, a combination of the two methods for total correctness reasoning seems promising. First steps in this direction with a related Kleene algebra have already been taken in [40]. In general, the flexibility and naturalness of KAD seems very promising for the specification and analysis of state transition systems. As often with Kleene algebra, KAD might offer an abstract, simple, elegant, uniform calculus where different specialized formalisms and complicated reasoning had to be used before.

Acknowledgment: We would like to thank Manfred Broy, Thorsten Ehm and Marcelo Frías for discussions and helpful comments.

References

1. C. J. Aarts. Galois connections presented computationally. Master's thesis, Eindhoven University of Technology, Department of Mathematics and Computing Science, 1992.
2. J.-R. Abrial. *The B-Book*. Cambridge University Press, 1996.
3. K.-R. Apt and E.-R. Olderog. *Verification of Sequential and Concurrent Programs*. Springer, 2nd edition, 1997.
4. G. Birkhoff. *Lattice Theory*, volume 25 of *Colloquium Publications*. American Mathematical Society, 1984. Reprint.
5. R. Bull and K. Segerberg. Basic modal logic. In D. Gabbay and F. Guentner, editors, *Handbook of Philosophical Logic*, volume II, chapter II.1, pages 1–88. D. Reidel, 1984.
6. B. F. Chellas. *Modal Logic: An Introduction*. Cambridge University Press, 1980.
7. E. Cohen. Hypotheses in Kleene algebra. Unpublished manuscript, 1994.
8. E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *Proc. of Mathematics of Program Construction, 5th International Conference, MPC 2000*, volume 1837 of *LNCS*, pages 45–59. Springer, 2000.
9. J. H. Conway. *Regular Algebra and Finite State Machines*. Chapman and Hall, 1971.

10. S. Crvenkovič, I. Dolinka, and Z. Ésik. The variety of Kleene algebras with conversion is not finitely based. *Theoretical Computer Science*, 230:235–245, 2000.
11. J. Desharnais and B. Möller. Characterizing determinacy in Kleene algebras. *Information Sciences*, 139(3–4):253–273, 2001.
12. J. Desharnais, B. Möller, and F. Tchier. Kleene under a demonic star. In T. Rus, editor, *Algebraic Methodology and Software Technology*, volume 1816 of *LNCS*, pages 355–370. Springer, 2000.
13. E. W. Dijkstra. *A Discipline of Programming*. Prentice Hall, 1976.
14. T. Ehm, B. Möller, and G. Struth. Kleene modules. In R. Berghammer and B. Möller, editors, *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 21–27. Universität Kiel, Germany, 2003.
15. S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, 1974.
16. J. M. Fischer and R. F. Ladner. Propositional dynamic logic of regular programs. *J. Comput. System Sci.*, 18(2):194–211, 1979.
17. S. Gaubert and Max Plus. Methods and applications of $(\max, +)$ linear algebra. Technical Report RR-3088, INRIA- Rocquencourt, Jan. 1997.
18. D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.
19. C. A. R. Hoare and B. von Karger. Sequential calculus. *Information Processing Letters*, 53(3):123–130, 1995.
20. M. Hollenberg. Equational axioms of test algebra. In M. Nielsen and W. Thomas, editors, *Computer Science Logic, 11th International Workshop, CSL '97*, volume 1414 of *LNCS*, pages 295–310. Springer, 1997.
21. D. Kozen. On the duality of dynamic algebras and Kripke models. In E. Engeler, editor, *Workshop on Logic of Programs*, volume 125 of *LNCS*, pages 1–11. Springer, 1979.
22. D. Kozen. A representation theorem for $*$ -free PDL. Technical Report RC7864, IBM, 1979.
23. D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.
24. D. Kozen. On action algebras. In J. van Eijck and A. Visser, editors, *Logic and Information Flow*, pages 78–88. MIT Press, 1994.
25. D. Kozen. Kleene algebra with tests. *Trans. Programming Languages and Systems*, 19(3):427–443, 1997.
26. D. Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1(1):60–76, 2001.
27. D. Kozen and F. Smith. Kleene algebra with tests: Completeness and decidability. In D. van Dalen and M. Bezem, editors, *Proc. of 10th International Workshop on Computer Science Logic (CSL'96)*, volume 1258 of *LNCS*, pages 244–259. Springer, 1996.
28. W. Kuich. Semirings and formal power series: Their relevance to formal languages and automata. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Language Theory*, volume I, pages 609–677. Springer-Verlag, 1997.
29. J. Loeckx and K. Sieber. *The Foundations of Program Verification*. Wiley Teubner, 2nd edition, 1987.
30. B. Möller and G. Struth. Modal Kleene algebra and partial correctness. Technical report, Universität Augsburg, Institut für Informatik.
31. B. Möller and G. Struth. Greedy-like algorithms in Kleene algebra. In R. Berghammer and B. Möller, editors, *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 173–180. Universität Kiel, Germany, 2003.

32. C. Mulvey. &. *Rend. Circ. Math. Palermo*, 2(12):99–104, 1986.
33. I. Németi. Dynamic algebras of programs. In *Proc. FCT'81 — Fundamentals of Computation Theory*, volume 117 of *LNCS*, pages 281–291. Springer, 1981.
34. V. Pratt. Dynamic logic as a well-behaved fragment of relation algebras. In D. Pigozzi, editor, *Conference on Algebra and Computer Science*, volume 425 of *LNCS*, pages 77–110. Springer, 1988.
35. V. Pratt. Action logic and pure induction. In J. van Eijck, editor, *Logics in AI, European Workshop, JELIA '90*, volume 478 of *LNCS*, pages 97–110. Springer, 1990.
36. V. Pratt. Dynamic algebras: Examples, constructions, applications. *Studia Logica*, 50:571–605, 1991.
37. G. W. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer, 1993.
38. J. M. Spivey. *Understanding Z*. Cambridge University Press, 1988.
39. V. Trnkova and J. Reiterman. Dynamic algebras with tests. *J. Comput. System Sci.*, 35:229–242, 1987.
40. J. von Wright. From Kleene algebra to refinement algebra. In B. Möller and E. Boiten, editors, *Mathematics of Program Construction, 6th International Conference, MPC 2002*, volume 2386 of *LNCS*, pages 233–262. Springer, 2002.
41. D. Yetter. Quantales and (non-commutative) linear logic. *J. Symbolic Logic*, 55(1):41–64, 1990.