Kleene Algebra with Domain

JULES DESHARNAIS
Université Laval
and
BERNHARD MÖLLER
Universität Augsburg
and
GEORG STRUTH
University of Sheffield

We propose Kleene algebra with domain (KAD), an extension of Kleene algebra by simple equational axioms for a domain and a codomain operation. KAD considerably augments the expressiveness of Kleene algebra, in particular for the specification and analysis of programs and state transition systems. We develop the basic calculus, present the most interesting models and discuss some related theories. We demonstrate applicability by two examples: algebraic reconstructions of Noethericity and propositional Hoare logic based on equational reasoning.

Categories and Subject Descriptors: D.2.4 [**Software Engineering**]: Program Verification—*correctness proofs*; F.3.1 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs—*assertions*; *invariants*; *logics of programs*; *mechanical verification*; *pre- and postconditions*; *specification techniques*; F.3.2 [**Logics and Meanings of Programs**]: Semantics of Programming Languages—*algebraic approaches to semantics*; I.1.3 [**Symbolic and Algebraic Manipulation**]: Languages and Systems—*special-purpose algebraic systems.*

General Terms: Theory, Verification.

Additional Key Words and Phrases: Idempotent semiring, Kleene algebra, domain, codomain, image and preimage operation, equational reasoning, state transition systems, program development and analysis.

1. INTRODUCTION

Programs and state transition systems are often modelled in a bipartite world populated by propositions and actions. While propositions express static properties of states, actions model their dynamics. Propositions are usually organised in a Boolean algebra, while the sequential, non-deterministic and iterative behaviour of

Research partially sponsored by DFG project Mo-690/5-1.

Authors' addresses: J. Desharnais, Département d'informatique et de génie logiciel, Université Laval, Québec QC G1K 7P4, Canada, e-mail: Jules.Desharnais@ift.ulaval.ca; B. Möller, Institut für Informatik, Universität Augsburg, Universitätsstr. 14, D-86135 Augsburg, Germany, e-mail: moeller@informatik.uni-augsburg.de; G. Struth, Department of Computer Science, University of Sheffield, Sheffield S1 4DP, UK, e-mail: G.Struth@dcs.shef.ac.uk.

actions can conveniently be modelled by a Kleene algebra. Reasoning about programs and state transition systems requires cooperation between the two parts of the world. This can be achieved by two mappings, one sending actions and propositions to propositions in order to express properties of actions, the other sending propositions to actions in order to model propositions as tests, measurements or observations on states. This is needed in particular for programming constructs like conditionals or loops.

There are two prominent complementary realisations of this two-world picture: Propositional dynamic logic (PDL) and its algebraic variants (cf. [Harel et al. 2000; Kozen 1979; Németi 1981; Pratt 1988; 1991; Trnkova and Reiterman 1987]) and Kleene algebra with tests (KAT) [Kozen 1997]. In PDL, only propositions are first-class citizens. This gives the approach a logical flavour. 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 that turn propositions into actions. Modal operators introduce a very versatile and intuitive style of reasoning, in particular when actions are binary relations. In KAT, in contrast, 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 as particular actions, by embedding them as a Boolean subalgebra into the Kleene algebra of actions. Thus only the mapping from propositions to actions is present. Since KAT does not depend on extensionality, it admits a rich model class beyond relations. Consequently, many properties of programs and state transition systems can succinctly be expressed and analysed in PDL or KAT. Each approach has its particular merits, both concerning expressivity and complexity. PDL, for instance, is EXPTIME-complete [Harel et al. 2000], while the equational theory of KAT is PSPACE-complete [Kozen and Smith 1996].

The present paper shows how the worlds of KAT and PDL can be fruitfully combined. To this end, we propose Kleene algebra with domain (KAD), an extension of KAT by a domain operation. Domain forms a missing link between algebraic, relational and modal approaches; it provides equal opportunities for propositions and actions. KAD not only integrates the advantages of its predecessors, it also offers additional flexibility and symmetry and yields new structural insights. In particular, it gives a uniform view of hitherto separate approaches to program analysis and development: modal formalisms such as PDL, algebraic formalisms such as KAT, set-based formalisms such as B [Abrial 1996] and Z [Spivey 1988] and semantic formalisms based on predicate transformers. It also allows equational cross-theory reasoning between all these approaches. As in KAT, propositions are embedded into actions. As in PDL, there is a mapping from actions to propositions: the domain operation. Adding such a mapping to KAT is only natural: relations are a standard model for KAT as well as for modal logics like PDL. Domain, or more precisely preimage, provides the standard interpretation of the modal diamond operator in this model. KAD provides an abstract algebraic formalism for reasoning with this modality.

Here, the focus is on motivating the definitions, developing the basic calculus

and discussing the most interesting models of KAD. We also provide two examples that underpin its applicability. Many interesting questions, for instance concerning completeness, representability, expressivity, complexity, the precise relation to modal algebras and a more extensive investigation of applications are the subject of other publications, see [Desharnais et al. 2004a] for a survey. More precisely, the main contributions of the present paper are the following.

—We propose finite equational axiomatisations of domain and codomain operations for certain idempotent semirings and Kleene algebras.

—We develop a basic domain calculus for KAD. Our axioms capture many natural properties of the relational domain operator and provide new insights into its algebra.

—We show that the domain operation is well behaved on the standard models of Kleene algebra.

—We define preimage and image operations in KAD. These are interesting for the specification and analysis of programs and state transition systems. They allow the definition of modal operators.

—We show that Noethericity and well-foundedness can be expressed in KAD. This allows termination analysis by algebraic calculation.

—We algebraically reconstruct Hoare logic in KAD. This gives an abstract axiomatic semantics and equational calculus for imperative programming languages.

Besides these main contributions we present further results. We show independence of the domain and codomain axioms of KAD. We discuss their compatibility with those for related structures. 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 idempotent semirings with domain are. We derive implementation schemata for efficient reachability algorithms.

Domain has previously been axiomatised in extensions of Kleene algebra like quantales and relation algebras (cf. [Aarts 1992; Desharnais and Möller 2001; Desharnais et al. 2000; Schmidt and Ströhlein 1993]), but there is no straightforward transfer. KAD offers several benefits. It generalises previous approaches and therefore admits a richer model class. It focuses on the essential operations for programs and state transition systems. And it is first-order, whence better suited for automated reasoning.

The remainder of this text is organised as follows. Section 2 introduces idempotent semirings, Kleene algebras and their standard models. Section 3 introduces idempotent semirings with tests, KAT and again the standard models. Section 4 presents an equational axiomatisation of domain for idempotent semirings. We show independence of the axioms, provide some standard models and outline a basic domain calculus. A further important concept, locality of domain and codomain, paves the way to multi-modal logics, in particular PDL. Section 5 presents two notions of duality that couple the concepts of domain and codomain. In Section 6, image and preimage operators are derived from the domain and codomain operations. Section 7 presents basic properties of domain and codomain in KAD, including algebraic techniques for induction and reachability analysis. Section 8 contains

some basic meta-results on KAD. Section 9 compares our domain axioms with those for related structures. Section 10 algebraically reconstructs Noethericity and well-foundedness in KAD. Section 11 reconstructs Hoare logic in KAD. Section 12 draws a conclusion and points out some further work.

2. IDEMPOTENT SEMIRINGS AND KLEENE ALGEBRA

This section introduces idempotent semirings and Kozen's variants of Kleene algebras. It also discusses some important models, such as the relational model, the language model, the path model, the $(\min, +)$- and $(\max, +)$-models and some of Conway's small finite Kleene algebras. We will later tie them in with the domain approach.

Kleene algebras axiomatise the regular operations of addition, multiplication and Kleene star as they arise in formal languages and in the analysis of programs and state transition systems. Traditionally, there are two main approaches, one based on semirings, one on lattices. Here, we will reserve the notion of *Kleene algebra* exclusively for the former.

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 distributes over addition in both arguments and 0 is a left and right annihilator with respect to multiplication $(a \cdot 0 = 0 = 0 \cdot a)$.

As usual in algebra, we write ab for $a \cdot b$ and stipulate that multiplication binds stronger than addition. A semiring is *trivial* if $0 = 1$, since then all elements are zero. We will consider only non-trivial semirings, unless otherwise stated.

Every semiring A comes with an *opposite* semiring A^{op} in which the order of multiplication is swapped. If a statement holds in a semiring, a dual one holds in its opposite. This duality will later relate domain and codomain.

A semiring is *idempotent* (an *i-semiring*) if its addition is. The relation $\leq$ defined for all a, b on an i-semiring A by $a \leq b \Leftrightarrow a + b = b$ is a partial ordering, in fact the only partial ordering on A for which 0 is the least element and for which addition and multiplication are isotone in both arguments. It is therefore called the *natural ordering* on A. It follows that inequalities and equations are interdefinable. We will use the notion of *equation* or *identity* freely for both kinds of expressions.

Obviously, every i-semiring A is a semilattice $(A, \leq)$ with addition as join and with least element 0. Thus $a \leq c \wedge b \leq c \Leftrightarrow a + b \leq c$ holds for all $a, b, c \in A$.

2.2 Kleene Algebras

A *Kleene algebra* [Kozen 1994a] is a structure $(A, +, \cdot, ^*, 0, 1)$ such that $(A, +, \cdot, 0, 1)$ is an i-semiring, * is a unary operation, a^*b is the least pre-fixed point of the function $\lambda x.b + ax$ and ba^* is the least pre-fixed point of $\lambda x.b + xa$. Formally, the *Kleene star* * satisfies, for all $a, b, c \in A$, the *star unfold* axioms

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

$$1 + a^*a \leq a^* \tag{2}$$

and the *star induction* axioms

$$b + ac \leq c \Rightarrow a^*b \leq c, \tag{3}$$
$$b + ca \leq c \Rightarrow ba^* \leq c. \tag{4}$$

The expressions a^*b and ba^* are uniquely characterised by the respective axioms.

We now recall some standard properties of Kleene algebras (cf. [Kozen 1994a]). The identities are familiar from formal language theory (cf. [Eilenberg 1974]).

LEMMA 2.1. *Let A be a Kleene algebra. For all $a, b, c \in A$ we have the identities*

$$1 \leq a^*, \tag{5}$$
$$a^*a^* = a^*, \tag{6}$$
$$\forall\, i \in \mathbb{N}\,.\, a^i \leq a^*, \tag{7}$$
$$a^{**} = a^*, \tag{8}$$
$$(ab)^*a = a(ba)^*, \tag{9}$$
$$(a + b)^* = a^*(ba^*)^*, \tag{10}$$
$$a^*b = b + a^*ab = b + aa^*b \tag{11}$$

and the quasi-identities

$$a \leq 1 \Rightarrow a^* = 1, \tag{12}$$
$$a \leq b \Rightarrow a^* \leq b^*, \tag{13}$$
$$ac \leq cb \Rightarrow a^*c \leq cb^*, \tag{14}$$
$$ca \leq bc \Rightarrow ca^* \leq b^*c. \tag{15}$$

2.3 Example Structures

The classes of idempotent semirings and Kleene algebras are quite rich. We now present some standard models. We will later show that the domain and codomain operations are well-behaved on them. The first examples present some finite Kleene algebras with at most four elements from Conway's book (cf. [Conway 1971], p. 101). They will later be used as counterexamples.

EXAMPLE 2.2. The structure $A_2 = (\{0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

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

is an i-semiring, called the *two-element Boolean semiring*. The operations $+$ and $\cdot$ play the roles of disjunction and conjunction. A_2 can uniquely be extended to a Kleene algebra by setting $0^* = 1^* = 1$. □

EXAMPLE 2.3. The structure $A_3^1 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

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

is an i-semiring. It can uniquely be extended to a Kleene algebra by setting $0^* = 1^* = 1$ and $a^* = a$. □

EXAMPLE 2.4. The structure $A_3^2 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1
0	0	a	1
a	a	a	1
1	1	1	1

$\cdot$	0	a	1
0	0	0	0
a	0	0	a
1	0	a	1

is an i-semiring. It can uniquely be extended to a Kleene algebra by setting $a^* = 0^* = 1^* = 1$. □

EXAMPLE 2.5. The structure $A_3^3 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1
0	0	a	1
a	a	a	1
1	1	1	1

$\cdot$	0	a	1
0	0	0	0
a	0	a	a
1	0	a	1

is an i-semiring. It is like A_3^2 except for the value of aa. It can uniquely be extended to a Kleene algebra by setting $a^* = 0^* = 1^* = 1$. □

EXAMPLE 2.6. The structure $A_4^1 = (\{a, b, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1	b
0	0	a	1	b
a	a	a	1	b
1	1	1	1	b
b	b	b	b	b

$\cdot$	0	a	1	b
0	0	0	0	0
a	0	0	a	a
1	0	a	1	b
b	0	a	b	b

is an i-semiring. It can be extended to a Kleene algebra by setting $0^* = a^* = 1^* = 1$ and $b^* = b$. □

Conway has shown that there are eighteen non-isomorphic four-element Kleene algebras.

EXAMPLE 2.7. Consider the structure $\mathsf{REL}(M) = (2^{M\times M}, \cup, \circ, \emptyset, \Delta)$ over a set M, where $2^{M\times M}$ denotes the set of binary relations over M, $\cup$ denotes set union, $\circ$ denotes relational product, $\emptyset$ denotes the empty relation and Δ denotes the identity relation $\{(a, a) \mid a \in M\}$. Then $\mathsf{REL}(M)$ is an i-semiring with set inclusion as the natural ordering. It can be extended to a Kleene algebra by defining R^* as the reflexive transitive closure of R for all $R \in \mathsf{REL}(M)$, that is, $R^* = \bigcup_{i\geq 0} R^i$, with $R^0 = \Delta$ and $R^{i+1} = R \circ R^i$. We call $\mathsf{REL}(M)$ the (full) *relational* i-semiring or Kleene algebra over M. □

EXAMPLE 2.8. Let $(A, +, \cdot, 0, 1)$ be a semiring and M be a finite set. Then the set $A^{M\times M}$ can be viewed as the set of $|M| \times |M|$ matrices with indices in M and elements in A. Now consider the structure $\mathsf{MAT}(M, A) = (A^{M\times M}, +, \cdot, \mathbf{0}, \mathbf{1})$ where

$+$ and $\cdot$ are matrix addition and multiplication, and $\mathbf{0}$ and $\mathbf{1}$ are the zero and unit matrices. Then $\mathsf{MAT}(M, A)$ again forms a semiring, the *matrix semiring* over M and A. $\mathsf{MAT}(M, A)$ is idempotent if A is. In this case, the natural order is the componentwise one.

If A is the two-element Boolean semiring A_2, this yields another representation of $\mathsf{REL}(M)$ as $\mathsf{MAT}(M, A)$ in terms of adjacency matrices.

If A is a Kleene algebra then $\mathsf{MAT}(M, A)$ can be extended to a Kleene algebra (see [Conway 1971]) by partitioning a non-singleton matrix into submatrices a, b, c, d, of which a and d are square, and setting

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

where $f = a + bd^*c$. □

Example 2.9. Let Σ^* be the set of finite words over some finite alphabet Σ and consider the structure $\mathsf{LAN}(\Sigma) = (2^{\Sigma^*}, \cup, ., \emptyset, \{\varepsilon\})$, where 2^{Σ^*} denotes the set of languages over Σ, and $\cup$ denotes set union, $L_1.L_2 = \{vw \,|\, v \in L_1, w \in L_2\}$, where vw denotes concatenation of v and w, $\emptyset$ denotes the empty language and ε denotes the empty word. Then $\mathsf{LAN}(\Sigma)$ is an i-semiring and language inclusion is its natural ordering. It can be extended to a Kleene algebra by defining $L^* = \{w_1 w_2 \ldots w_n \,|\, n \geq 0, w_i \in L\}$ in the standard way. We call $\mathsf{LAN}(\Sigma)$ the *language* i-semiring or Kleene algebra over Σ. The operations $\cup$, . 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 regular subsets is called *algebra of regular events*. There is a natural homomorphism L from the term algebra over the signature of Kleene algebra generated by a set Σ onto the algebra $\mathsf{REG}(\Sigma)$ of regular events over Σ^*, given by $L(a) = \{a\}$ for each $a \in \Sigma$, $L(a+b) = L(a) \cup L(b)$ and $L(a \cdot b) = L(a).L(b)$. In [Kozen 1994a] it has been shown that $\mathsf{REG}(\Sigma)$ is the free Kleene algebra generated by Σ. In this sense, Kleene algebra is the algebra of regular events and we can freely use all *regular identities*, that is, all valid identities of the algebra of regular events, in our calculations. □

Example 2.10. 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). ε can be viewed as the empty path. The partial operation of *fusion product* of elements of Σ^* is, for all $s, t \in \Sigma^*$ and $x, y \in \Sigma$, defined as

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

It glues paths together at a common point. It is extended to subsets of Σ^* by

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

Then $\mathsf{PAT}(\Sigma) = (2^{\Sigma^*}, \cup, \bowtie, \emptyset, \Sigma \cup \{\varepsilon\})$ is an i-semiring called the *path i-semiring* over Σ. It can be extended to a path Kleene algebra as in the i-semiring of relations. □

EXAMPLE 2.11. 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 $\mathsf{MAT}(Q, \mathsf{LAN}(\Sigma))$ record possible sequences of labels (traces) that connect two states. When there is no possible transition between two states, the corresponding matrix element is the empty language. □

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* [Kuich 1997]. Its natural ordering is the converse of the standard ordering on $\mathbb{N}_\infty$. Hence 0 — the semiring multiplicative unit — is the largest element, so that by (12) $(\min, +)$ can uniquely be extended to a Kleene algebra by setting $n^* = 0$ for all $n \in \mathbb{N}_\infty$. □

EXAMPLE 2.13. Let $\mathbb{N}_{-\infty} = \mathbb{N} \cup \{-\infty\}$ 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* [Gaubert and Plus 1997]. 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 Kleene algebra. For $a > 0$ the set $\{a^n \mid n \in \mathbb{N}\} = \{na \mid n \in \mathbb{N}\}$ is unbounded, whereas, according to (7), it should have a^* as an upper bound. □

3. SUBIDENTITIES AND KLEENE ALGEBRA WITH TESTS

We now take the first step towards the axiomatisation of domain and codomain operations on i-semirings. We discuss the subidentities of idempotent semirings and Kleene algebras. Subidentities are those elements that lie below the multiplicative unit. A subset of these, the *tests*, will allow us to embed propositions into the space of actions. This leads to idempotent semirings with tests and Kleene algebras with tests. Finally, we discuss some important models of these structures.

As a motivating example, consider the relational i-semiring from Example 2.7. 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 subset of M. Setting $n = |M|$, the empty set is characterised by the $n \times n$ zero matrix, the set M 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. Consequently, we will model domain and codomain in an i-semiring as mappings into the set of subidentities.

3.1 Subidentities

An element of an i-semiring A is a *subidentity* if it is smaller than 1. It is easy to show that the set of subidentities of an i-semiring forms an i-semiring.

LEMMA 3.1. *For subidentities in an i-semiring, multiplication*

(i) *is a lower bound operation,*
(ii) *need not be idempotent, whence not a greatest lower bound operation.*

PROOF.

(i) Let A be an i-semiring with subidentities p, q. Then $p = p1 \geq pq \leq 1q = q$. Thus pq is a lower bound of p and q.

(ii) In the i-semiring A_3^2 from Example 2.4, a is a subidentity that is not multiplicatively idempotent. Rather we have $aa = 0 < a$, and so aa is not the greatest lower bound of a and a.

□

By contrast, in the relational i-semiring and many related structures, the subidentities form a Boolean algebra or at least a lattice (cf. Example 3.5). In i-semirings, further properties are needed for modelling sets, propositions or tests. There are essentially two alternatives (cf. [Kozen 1997]). First, one can impose the restriction that all subidentities form a Boolean algebra. Second, one can explicitly embed a Boolean algebra of tests into the algebra of subidentities. We will adopt the second, more general alternative.

3.2 Test-Semirings and Kleene Algebras with Tests

Following Kozen, we say that a *test semiring* (a *t-semiring*) is an i-semiring A with a distinguished Boolean subalgebra $\mathsf{test}(A)$ of the algebra of subidentities with greatest element 1, least element 0 and join operation $+$, such that $\mathsf{test}(A)$ is closed under multiplication. We call $\mathsf{test}(A)$ the *test algebra* of A. A t-semiring is a *Kleene algebra with tests* if the t-semiring is also a Kleene algebra [Kozen 1997]. The class of Kleene algebras with tests is denoted by KAT.

We will henceforth use letters $a, b, c, \ldots$ for arbitrary semiring elements (actions) and the letters $p, q, r, \ldots$ for tests (propositions). Moreover, we denote by p' the complement of test p in $\mathsf{test}(A)$ and by $p \sqcap q$ the meet of p and q. We will freely use the standard concepts and laws of Boolean algebra.

LEMMA 3.2. *Every i-semiring is a t-semiring.*

PROOF. Let A be an i-semiring. If $0 = 1$ then the claim is trivially satisfied. Otherwise, let $\mathsf{test}(A) = \{0, 1\}$ with $p \sqcup q = p + q$, $p \sqcap q = pq$ for all $p, q \in \mathsf{test}(A)$ and $1' = 0$, $0' = 1$. This yields a Boolean subalgebra. □

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

LEMMA 3.3. *In every t-semiring,*

(i) *multiplication of tests is idempotent,*

(ii) *the product of two tests is their meet.*

PROOF. Let $p, q \in \mathsf{test}(A)$ for some t-semiring A. By Lemma 3.1(i), $pq \leq p \sqcap q$.

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

(ii) Let $r \leq p$ and $r \leq q$ for some $r \in \mathsf{test}(A)$. Then $r = rr \leq pq \in \mathsf{test}(A)$ by (i) and isotonicity. Hence pq is the greatest lower bound of p and q in $\mathsf{test}(A)$ and therefore equal to $p \sqcap q$.

□

The following lemma collects some properties of test semirings that are helpful for computing with abstract image and preimage operations in Section 6.

LEMMA 3.4. *In a t-semiring A with $a \in A$ and $p, q \in \mathsf{test}(A)$, the following properties are equivalent.*

$$pa \leq aq, \qquad aq' \leq p'a, \qquad paq' \leq 0, \qquad pa = paq.$$

PROOF. Let $pa \leq aq$. We calculate, for the second inequality,

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

Let $aq' \leq p'a$. Then $paq' \leq pp'a = 0a = 0$.
Let $paq' \leq 0$. Then $pa = pa1 = pa(q + q') = paq + paq' = paq$.
Let $pa = paq$. Then $pa = paq \leq aq$. □

The equivalence of the following properties follows from Lemma 3.4 by duality with respect to semiring opposition.

$$ap \leq qa \qquad q'a \leq ap', \qquad q'ap \leq 0, \qquad ap = qap.$$

3.3 Example Structures

We now consider some models of test semirings and Kleene algebras with tests. First, note that Conway's algebras from Section 2 (that is, Example 2.2 to Example 2.6) are all discrete and therefore not very interesting.

EXAMPLE 3.5. In $\mathsf{REL}(M)$, there are $2^{|M|}$ 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. □

EXAMPLE 3.6. In $\mathsf{LAN}(\Sigma)$, the only subidentities are $\emptyset$ and $\{\varepsilon\}$. They also form the only possible test algebra; hence $\mathsf{LAN}(\Sigma)$ is always discrete. □

EXAMPLE 3.7. In the path i-semiring $\mathsf{PAT}(\Sigma)$ over Σ, a subidentity $P \subseteq \Sigma \cup \{\varepsilon\}$ models a set of nodes or states, where ε also serves as the only "pseudo-node" or "pseudo-state" in an empty sequence. □

EXAMPLE 3.8. 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 ∞, so that the tropical semiring is discrete. □

EXAMPLE 3.9. In the max-plus semiring, the only multiplicatively idempotent subidentities are $-\infty$ and 0. These two elements also form the only possible test algebra, so that the max-plus semiring is discrete. □

4. DOMAIN

In this section, we introduce several equivalent axiomatisations of a domain operation on test semirings, among them an 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 4.3.

—A notion of *domain* that is necessary for more advanced applications, for instance multi-modal operators parameterised by actions.

We also show independence of the equational axioms and provide examples.

4.1 Domain in the Relational i-Semiring

As a motivation, consider again the relational i-semiring of Example 2.7. Let R be a binary relation on some set M. Then the domain $\delta(R)$ of R is given by the set

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

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

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

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

First, $\delta(R)$ is the least $X \subseteq \Delta$ with $R \subseteq X \circ R$. Second, using Example 3.5, the complement $\delta(R)'$ of $\delta(R)$ in the Boolean lattice of subidentities of $\mathsf{REL}(M)$ — the set of all pairs below Δ that are not in $\delta(R)$ — is the greatest $X \subseteq \Delta$ with $X \circ R \subseteq \emptyset$. Without the restriction to subidentities, solutions might not be subidentities. Since, by Example 3.5, the subidentities of $\mathsf{REL}(M)$ form a Boolean algebra, Lemma 3.4 implies that the definitions in terms of least and greatest solutions are equivalent.

4.2 Predomain Axioms

As a first step in abstracting to semirings, we introduce some auxiliary concepts. Let A an i-semiring and $a, b \in A$. We say that b is a *left preserver* of 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. We say that a is a *left annihilator* of b if $ab = 0$. The concepts of *right preservation*, *right stability*, *right invariance* and *right annihilation* are dual with respect to semiring opposition.

Although a more general approach based on subidentities might be possible, the Boolean structure of the test algebra is very convenient for making our definitions coherent.

LEMMA 4.1. *Let A be a t-semiring and $a \in A$. The element $p \in \mathsf{test}(A)$ is the least left preserver of a in $\mathsf{test}(A)$ iff for all $q \in \mathsf{test}(A)$,*

$$p \leq q \Leftrightarrow a \leq qa. \tag{16}$$

PROOF. We show that (16) is equivalent to

$$a \leq pa, \tag{17}$$

$$a \leq qa \Rightarrow p \leq q. \tag{18}$$

Equation (18) is one direction of (16). Setting $p = q$ in (16) yields (17). Moreover, $a \leq pa \leq qa$ follows immediately from (17) and $p \leq q$. □

LEMMA 4.2. *Let A be a t-semiring and $a \in A$. Then p is the greatest left annihilator of a in $\mathsf{test}(A)$ iff for all $q \in \mathsf{test}(A)$,*

$$q \leq p \Leftrightarrow qa \leq 0. \tag{19}$$

PROOF. We must show that (19) is equivalent to

$$pa \leq 0, \tag{20}$$
$$qa \leq 0 \Rightarrow q \leq p. \tag{21}$$

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

As to the existence of least left preservers and greatest left annihilators, two facts should be distinguished. For a given i-semiring, least left preservers and greatest left annihilators can always be obtained by choosing the discrete t-semiring. But a given t-semiring with fixed test algebra need not admit arbitrary least left preservers and greatest left annihilators. The following example is due to Dexter Kozen.

LEMMA 4.3. *There is a t-semiring where certain elements do not have least left preservers and greatest left annihilators in the test algebra.*

PROOF. Let M be an infinite set and let T consist of the finite or cofinite subsets of M. Then $(2^M, T, \cup, \cap, \emptyset, M)$ is a Boolean algebra that is also a t-semiring. Its test algebra T is incomplete. A test q is a left preserver of $p \subseteq M$ iff $p \cap q = p$.

Let now p be infinite, but not cofinite, and assume that r is a least left preserver of p. Then $p \subsetneq r$ and therefore $r - p \neq \emptyset$. For $x \in r - p$, the set $r - \{x\}$ is again cofinite and $p - \{x\} = p$. Therefore $p \cap (r - \{x\}) = r \cap (p - \{x\}) = r \cap p = p$, that is, $r - \{x\}$ is again a left preserver. This is a contradiction. □

The following example shows that the non-existence of least left preservers and greatest left annihilators does not depend on the incompleteness of the test algebra.

LEMMA 4.4. *There is a t-semiring with complete test algebra in which certain elements do not have least left preservers and greatest left annihilators in the test algebra.*

PROOF. We only sketch the proof; details can be found in [Möller 2005]. Let M be an infinite set. For $p \in 2^M$, let $\lfloor p \rfloor$ be a copy of p and let $\lfloor 2^M \rfloor$ be the set of all copies of subsets of M. We assume that $2^M \cap \lfloor 2^M \rfloor = \emptyset$ and set $S = 2^M \cup \lfloor 2^M \rfloor$. As usual, a *filter* on M is a non-empty collection of sets that is closed under finite intersections and upwards closed with respect to inclusion. An *ultrafilter* U is a filter that contains every subset of M or its complement, but not both. For $p, q \subseteq M$, define

$$p \rhd \lfloor q \rfloor = \begin{cases} \lfloor p \cap q \rfloor, & \text{if } p \in U, \\ p \cap q, & \text{otherwise,} \end{cases}$$

and

$+$	q	$\lfloor q \rfloor$
p	$p \cup q$	$\lfloor p \cup q \rfloor$
$\lfloor p \rfloor$	$\lfloor p \cup q \rfloor$	$\lfloor p \cup q \rfloor$

$\cdot$	q	$\lfloor q \rfloor$
p	$p \cap q$	$p \rhd \lfloor q \rfloor$
$\lfloor p \rfloor$	$q \rhd \lfloor p \rfloor$	$\lfloor p \cap q \rfloor$

Then it can be shown that $(S, 2^M, +, \cdot, \emptyset, M)$ is a t-semiring with complete test algebra 2^M.

Let C be the Fréchet filter of all cofinite subsets of M and let $p \subsetneq M$ be infinite, but not cofinite. Then $p' \neq 0$ and $p, p' \notin C$, but C can be extended in the standard

way to an ultrafilter U that contains p', but not p. Similarly to above, the set of left preservers of $\lfloor p \rfloor$ is

$$L = \{q \in U : p \subseteq q\},$$

but, by assumption, the infimum p of L is not in U, whence not in the test algebra. □

But properties of partial orderings imply that least left preservers and greatest left annihilators are unique if they exist. And they do exist, for instance, when the test algebra is finite.

The following proposition relates preservers and annihilators.

PROPOSITION 4.5. *Let A be a t-semiring. For all $a \in A$, let p be the least left preserver and let q be the greatest left annihilator of a in* $\mathsf{test}(A)$. *Then $p = q'$.*

PROOF. Immediate from Lemma 3.4. □

We now axiomatise a predomain operation on t-semirings as yielding the least left preserver. Proposition 4.5 provides an equivalent characterisation via the greatest left annihilator. Moreover, we present a further equivalent axiomatisation in terms of two simple equations. We also show independence of the equational axioms.

Definition 4.6. A structure (A, δ) is a *t-semiring with predomain* (a *δ-semiring*) if A is a t-semiring and the *predomain operation* $\delta : A \to \mathsf{test}(A)$ satisfies, for all $a \in A$ and $p \in \mathsf{test}(A)$,

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

By this definition, the presuppositions for existence of predomain are the same as for least left preservers above. While a semiring may be made into a t-semiring in various ways by choosing different test algebras, for a fixed test algebra predomain is always unique if it exists. A predomain operation always exists on discrete t-semirings. We distinguish between predomain and domain, since, as already noted, the weaker definition suffices for deriving many natural properties.

PROPOSITION 4.7. *Let A be a t-semiring and let $\delta : A \to \mathsf{test}(A)$ be a predomain operation. Then for all $a \in A$ and $p \in \mathsf{test}(A)$,*

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

PROOF. Immediate from Proposition 4.5. □

This characterisation uses the lattice dual of the greatest left annihilator property. We now present an equational characterisation of predomain.

THEOREM 4.8. *Let A be a t-semiring and let $\delta : A \to \mathsf{test}(A)$ be a mapping. Then δ satisfies (llp) iff it satisfies, for all $a \in A$ and $p \in \mathsf{test}(A)$, the identities*

$$a \leq \delta(a)a, \tag{d1}$$

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

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

$$\delta(a) \leq p \Rightarrow a \leq pa, \tag{22}$$

which is one direction of (llp). Obviously, (22) 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 isotonicity of multiplication.

Second, we show that (d2) is equivalent to

$$a \leq pa \Rightarrow \delta(a) \leq p, \tag{23}$$

which is the other direction of (llp). Obviously, (23) implies (d2), instantiating a by 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). □

We have thus presented three equivalent axiomatisations for predomain. Each is of particular interest. The equivalences (llp) and (gla) allow us to reduce certain expressions over δ-semirings to expressions over t-semirings that do not mention predomain. Moreover, both capture the basic algebraic intuition behind domain. The 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 connect δ-semirings with modal algebras and modal logics, which is, however, beyond the scope of this work. Third, they support a simple check whether some given mapping in some t-semiring is a predomain operation. The three axiomatisations taken together give us flexibility in calculations.

We now show that the equational axiomatisation is minimal and irredundant.

THEOREM 4.9. *(d1) and (d2) are independent in t-semirings.*

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

Set $\delta(0) = \delta(1) = 1$ in A_2 (Example 2.2). Then (d1) holds by neutrality of 1. But $\delta(01) = 1 \not\leq 0$. Thus (d2) does not hold.

Set $\delta(0) = \delta(1) = 0$ in A_2. Then (d2) holds, since 0 is the least element. But $1 \not\leq 0 = 01 = \delta(1)1$. Thus (d1) does not hold. □

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 is always a meaningful — albeit not very interesting — predomain definition for an i-semiring.

LEMMA 4.10. *A discrete t-semiring A admits precisely one predomain operation, namely $\delta(0) = 0$ and $\delta(a) = 1$ for all $0 \neq a \in A$.*

PROOF. We show that δ 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 $p = 1$ by discreteness and (d2) also holds.

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

Finally, uniqueness is immediate from Lemma 4.11(i) below. □

The arguments of this and the following section show that basing predomain on test algebras is indeed convenient: It leads to simple natural axioms; further meaningful properties can be derived in a simple way, as will be shown in the next section. Nevertheless there are interesting possibilities for generalisation. The test

algebra could, for instance, be only a Heyting algebra or a distributive lattice. Also, domain could more generally be defined as a mapping into the set of subidentities. Our definitions are a suitable starting point for such investigations.

4.3 Predomain Calculus

The statements of this section allow a more intuitive understanding of domain and yield a basic predomain calculus. We leave a comparison with relational properties to the reader.

LEMMA 4.11. *Let A be a δ-semiring. Let $a, b \in A$ and $p \in \mathsf{test}(A)$.*

(i) *δ is fully strict:*

$$\delta(a) \leq 0 \Leftrightarrow a \leq 0. \tag{24}$$

(ii) *δ is additive:*

$$\delta(a+b) = \delta(a) + \delta(b). \tag{25}$$

(iii) *δ is isotone:*

$$a \leq b \Rightarrow \delta(a) \leq \delta(b). \tag{26}$$

(iv) *δ is an identity on tests:*

$$\delta(p) = p. \tag{27}$$

(v) *δ is idempotent:*

$$\delta(\delta(a)) = \delta(a). \tag{28}$$

(vi) *δ yields a left invariant:*

$$a = \delta(a)a. \tag{29}$$

(vii) *δ satisfies an import/export law:*

$$\delta(pa) = p\delta(a). \tag{30}$$

(viii) *δ satisfies a sublocality law:*

$$\delta(ab) \leq \delta(a\delta(b)). \tag{31}$$

(ix) *δ commutes with complementation on tests:*

$$\delta(p)' = \delta(p'). \tag{32}$$

PROOF.

(i) $\delta(a) \leq 0 \Leftrightarrow a \leq 0a \Leftrightarrow a \leq 0$ follows from (llp).

(ii) Using (gla), we calculate

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

But $\delta(a+b) \leq p \Leftrightarrow \delta(a) + \delta(b) \leq p$ implies the claim.

(iii) Using (25), this is a standard result from lattice theory.

(iv) $p \leq \delta(p)p \leq \delta(p)$ follows immediately from (d1) and $p \leq 1$. $\delta(p) = \delta(p1) \leq p$ follows immediately from (d2).

(v) Immediate from (27).

(vi) By (d1) it remains to show that $\delta(a)a \leq a$, which follows from $\delta(a) \in \mathsf{test}(A)$.

(vii) By Boolean algebra and (25) 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 (27).

□

4.4 Domain Axioms

Our axiomatisation of domain in t-semirings still lacks a natural property of domain — called *locality* — that holds in the relational model but is independent of (d1) and (d2). Namely, for all binary relations R, S on a set M,

$$\delta(R \circ S) = \delta(R \circ \delta(S)).$$

Intuitively, for computing the domain of a relation $R \circ S$, local information about the domain of S suffices; information about the inner structure or the codomain of S is not needed. In δ-semirings, one half of locality is derivable, as Lemma 4.11(viii) shows. The other half is independent.

LEMMA 4.12. *There is a δ-semiring A and there are $a, b \in A$ such that*

$$\delta(a\delta(b)) \not\leq \delta(ab).$$

PROOF. Consider again the discrete t-semiring A_3^2 of Example 2.4. According to Lemma 4.10, the mapping $\delta : 0 \mapsto 0$, $\delta : 1 \mapsto 1$, and $\delta : a \mapsto 1$ is a predomain operation. Then $\delta(a\delta(a)) = \delta(a1) = 1$ and $\delta(aa) = \delta(0) = 0$. That is, $\delta(aa) \leq \delta(a\delta(a))$ holds, but not $\delta(aa) = \delta(a\delta(a))$. □

Due to independence of locality, we add the negated property of Lemma 4.12 to the predomain axioms for a full domain operation.

Definition 4.13. A *t-semiring with domain* (a *$\hat{\delta}$-semiring*) is a δ-semiring in which the predomain operation $\hat{\delta} : A \to \mathsf{test}(A)$ also satisfies, for all $a, b \in A$,

$$\hat{\delta}(a\hat{\delta}(b)) \leq \hat{\delta}(ab). \tag{d3}$$

COROLLARY 4.14. *Let A be a $\hat{\delta}$-semiring. Then, for all $a, b \in A$,*

$$\hat{\delta}(ab) = \hat{\delta}(a\hat{\delta}(b)). \tag{loc}$$

The addition of the locality axiom leads to an unexpected consequence — there is no longer any freedom in choosing the test set! This is stated formally as follows.

THEOREM 4.15. *In every $\hat{\delta}$-semiring S the set* $\mathsf{test}(S)$ *consists of all subidentities that have a complement relative to* 1.

PROOF. We show that every element $a \leq 1$ with complement equals its own domain and hence is a test. First, since $\hat{\delta}$ is a predomain operation, we have

$$a = \hat{\delta}(a)a \leq \hat{\delta}(a) \tag{33}$$

by $a \leq 1$. Next, assume the existence of $b \leq 1$ with $a + b = 1$ and $ab = 0 = ba$. Then, by the locality axiom,

$$0 = \hat{\delta}(0) = \hat{\delta}(ba) = \hat{\delta}(b\hat{\delta}(a))$$

and hence $b\hat{\delta}(a) = 0$. Now

$$\hat{\delta}(a) = (a + b)\hat{\delta}(a) = a\hat{\delta}(a) + b\hat{\delta}(a) = a\hat{\delta}(a) \leq a,$$

since $\hat{\delta}(a) \leq 1$. Together with (33) we obtain $a = \hat{\delta}(a)$. □

4.5 Integral Domain Semirings

We now impose a necessary and sufficient condition on a discrete δ-semiring to be a $\hat{\delta}$-semiring. In analogy to the definition of an integral domain in ring theory, a semiring A is *integral* if it has no zero divisors, that is, for all $a, b \in A$,

$$ab \leq 0 \Rightarrow a \leq 0 \vee b \leq 0. \tag{34}$$

LEMMA 4.16. *Every integral δ-semiring is a $\hat{\delta}$-semiring.*

PROOF. Let A be integral. Thus $ab \leq 0$ implies $a \leq 0$ or $b \leq 0$. For the claim it suffices to show that $\delta(ab) \leq p \Rightarrow \delta(a\delta(b)) \leq p$ for all $p \in \mathsf{test}(A)$. Using Proposition 4.7, we calculate

$$\delta(ab) \leq p \Leftrightarrow p'ab \leq 0 \Rightarrow p'a \leq 0 \vee b \leq 0 \Leftrightarrow \delta(a) \leq p \vee \delta(b) \leq 0.$$

Therefore, $\delta(a\delta(b)) \leq \delta(a) \leq p$ or $\delta(a\delta(b)) = \delta(a0) = \delta(0) = 0 \leq p$. □

For discrete semirings this condition is also necessary.

LEMMA 4.17. *A discrete t-semiring is a $\hat{\delta}$-semiring iff it is integral.*

PROOF. Let A be a discrete t-semiring. From Lemma 4.10 we know that δ defined by $\delta : 0 \mapsto 0$ and $\delta : a \mapsto 1$ for all $0 \neq a \in A$ is the unique predomain operation on A. Thus A is a δ-semiring.

Now let δ satisfy(d3), that is, $\delta(a\delta(b)) \leq \delta(ab)$, and let $ab \leq 0$. Thus $\delta(a\delta(b)) \leq \delta(ab) \leq 0$ and hence $a\delta(b) \leq 0$ by construction of δ. There are two cases.

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

—If $\delta(b) = 0$ then $b = 0$ by construction of δ.

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

The other direction follows from Lemma 4.16. □

4.6 Example Structures

We now consider some models of δ-semirings and $\hat{\delta}$-semirings.

EXAMPLE 4.18. In the Boolean semiring A_2 (Example 2.2), the test algebra coincides with A_2. Setting $\delta(x) = 0 \Leftrightarrow x = 0$ is compatible with the definition of δ in Lemma 4.10. Thus it satisfies (d1) and (d2). Since A_2 is integral, (d3) holds, too. Moreover, this definition is unique. □

EXAMPLE 4.19. In A_3^2 (Example 2.4), 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 4.10. Thus it satisfies (d1) and (d2). Since A_3^2 is integral, (d3) holds, too. Moreover, this definition is unique. □

EXAMPLE 4.20. The only possible test algebra of the language i-semiring (Example 2.9) 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 4.10. Thus it satisfies (d1) and (d2). Since the language model is integral (as a free algebra), (d3) holds, too. Moreover, this definition is unique. □

EXAMPLE 4.21. In the path i-semiring (Example 2.10), the test algebra is $2^{\Sigma \cup \{\varepsilon\}}$. For $S \subseteq \Sigma^*$, the set $\delta(S)$ consists of all starting (pseudo-)nodes in S. Although the semiring is not integral, (d3) holds. □

EXAMPLE 4.22. 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 4.10. Thus it satisfies (d1) and (d2). Since the tropical semiring is integral, (d3) holds, too. Moreover, this definition is unique. □

These examples show that our domain axioms are 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 axiomatisation of codomain for idempotent semirings. It is based on dualities: first on duality with respect to opposition in a semiring and second on duality with respect to an operation of conversion that can be added to t-semirings. These dualities allow an automatic transfer between statements about domain and codomain and save half of the work in proofs.

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

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

For a t-semiring this suggests to define a codomain operation as the least right preserver or the greatest right annihilator. Similarly to domain, there is a notion of *locality* that is independent of the other axioms.

5.1 Codomain Definition

Definition 5.1.

(i) A *t-semiring with precodomain* (a *ρ-semiring*) is a structure (A, ρ) such that (A^{op}, ρ) is a semiring with predomain.

(ii) A *t-semiring with codomain* (a *$\hat{\rho}$-semiring*) is a structure $(A, \hat{\rho})$ such that $(A^{\mathrm{op}}, \hat{\rho})$ is a semiring with domain.

LEMMA 5.2. *Let A be a t-semiring. Then (A, ρ) is a ρ-semiring iff, for all $a \in A$, one and therefore each of the following equivalent conditions holds.*

(i) $\rho(a)$ is the least right preserver of a, that is, for all $p \in \mathsf{test}(A)$,

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

(ii) $\rho(a)$ is the greatest right annihilator of a, that is, for all $p \in \mathsf{test}(A)$,

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

(iii) For all $p \in \mathsf{test}(A)$, the operation ρ satisfies the identities

$$a \leq a\rho(a), \tag{cd1}$$

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

Moreover, A is a $\hat{\rho}$-semiring if ρ also satisfies the locality law

$$\rho(\rho(a)b) \leq \rho(ab). \tag{cd3}$$

The proof follows from the definition of precodomain and, by duality with respect to opposition, from the results for predomain and domain in Section 4. In the same way, all further results of that section carry over to precodomain and codomain.

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 between t-semirings with domain and t-semirings with codomain, we uniformly speak about *test semirings with domain*.

LEMMA 5.3. *There is a non-integral $\hat{\delta}\hat{\rho}$-semiring.*

PROOF. We have seen that (d1), (d2), (d3), and (cd1), (cd2), (cd3), respectively, hold in the relational semiring. However, 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 $RS = \emptyset$. □

The path semiring is another non-integral $\hat{\delta}\hat{\rho}$-semiring.

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 leads to a second notion of duality.

Definition 5.4.

(i) An i-semiring with *preconverse* is a structure $(A, ^\circ)$ such that A is an i-semiring and $^\circ : A \to A$ is an operation that satisfies the equations

$$a^{\circ\circ} = a, \qquad (a + b)^\circ = a^\circ + b^\circ, \qquad (ab)^\circ = b^\circ a^\circ.$$

(ii) A t-semiring with *weak converse* is a t-semiring with preconverse such that all tests p satisfy

$$p^\circ \leq p.$$

(iii) An i-semiring with *converse* [Crvenkovič et al. 2000] is an i-semiring with preconverse that satisfies the equation

$$a \leq aa^\circ a.$$

Obviously, $1^\circ = 1$, $0^\circ = 0$ and $a \leq b \Leftrightarrow a^\circ \leq b^\circ$ holds in every i-semiring with preconverse. $p^\circ = p$ holds in every i-semiring with weak converse. Moreover, every i-semiring with converse is an i-semiring with weak converse.

We can now express the duality between domain and codomain within the test semiring rather than at the meta-level.

PROPOSITION 5.5. *Let A be a $\delta\rho$-semiring (or a $\hat{\delta}\hat{\rho}$-semiring) with weak converse. Then for all $a \in A$,*

$$\delta(a^\circ) = \rho(a), \tag{35}$$
$$\rho(a^\circ) = \delta(a). \tag{36}$$

PROOF. We show that $\delta(a^\circ)$ satisfies (cd1) and (cd2) if A is a $\delta\rho$-semiring and (cd3) if A is a $\hat{\delta}\hat{\rho}$-semiring, which implies (35) by uniqueness of the solution.

(cd1) By (d1), $a^\circ \leq \delta(a^\circ)a^\circ$, whence $a = a^{\circ\circ} \leq (\delta(a^\circ)a^\circ)^\circ = a^{\circ\circ}(\delta(a^\circ))^\circ = a\delta(a^\circ)$.
(cd2) By (d2), $\delta((ap)^\circ) = \delta(p^\circ a^\circ) = \delta(pa^\circ) \leq p$.
(cd3) By (loc), $\delta((ab)^\circ) = \delta(b^\circ a^\circ) = \delta(b^\circ\delta(a^\circ)) = \delta(b^\circ(\delta(a^\circ))^\circ) = \delta((\delta(a^\circ)b)^\circ)$.

The proof of (36) is dual. □

We could therefore take (35) for defining codomain in a t-semiring with weak converse.

COROLLARY 5.6. *Let A be a $\delta\rho$-semiring with weak converse. For all $a \in A$ and $p \in \mathsf{test}(A)$,*

$$\delta(a^\circ p) = \rho(pa), \tag{37}$$
$$\rho(a^\circ p) = \delta(pa). \tag{38}$$

5.3 Interdependence of Locality of Domain and Codomain

In this subsection we show that locality of domain and locality of codomain are not independent. We prepare the proof by an auxiliary property.

LEMMA 5.7. *A $\delta\rho$-semiring A satisfies locality (loc) iff for all $a, b \in A$,*

$$ab \leq 0 \Leftrightarrow \rho(a)\delta(b) \leq 0. \tag{39}$$

PROOF. We first show that (loc) implies (39).

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

The first and third steps of the proof use (24), the second step uses (loc), the fourth step uses (gra) and the last step is by Boolean algebra.

Now we show that (39) implies (loc). First, by (30) $\rho(a)\delta(b) = \rho(a\delta(b))$ and therefore, by (24) and (39)

$$ab \leq 0 \Leftrightarrow a\delta(b) \leq 0. \tag{40}$$

Using Boolean algebra, (40) 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 general properties of inequalities. □

Since (39) is symmetric in δ and ρ, we obtain the following interdependence result.

COROLLARY 5.8. *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 $N \subseteq M$ under a relation $R \subseteq M \times M$ is defined as

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

Replacing, like in the discussion of relational domain, the set N by the corresponding subidentity $\dot{N}$, we obtain the equivalent point-free definition $R : \dot{N} = \delta(R \circ \dot{N})$. Dually, the image of N under R is defined as

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

which is equivalent to the point-free definition $\dot{N} : R = \rho(\dot{N} \circ R)$.

As usual, we abstract from sets to semirings and define for every $\delta\rho$-semiring the *image* and *preimage* operators, both denoted by $:$, as mappings of type $\mathsf{test}(A) \times A \to \mathsf{test}(A)$ and $A \times \mathsf{test}(A) \to \mathsf{test}(A)$ for all $a \in A$ and $p \in \mathsf{test}(A)$ by

$$p : a = \rho(pa), \tag{41}$$

$$a : p = \delta(ap). \tag{42}$$

In particular, we can use $a : 1$ and $1 : a$ instead of $\delta(a)$ and $\rho(a)$ and overload this notation for the case of $\hat{\delta}$ and $\hat{\rho}$. Since the image and preimage operators are products, 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 dual with respect to opposition, there is again an automatic transfer of properties. 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 be a δ-semiring. For all $a \in A$ and $p, q \in \mathsf{test}(A)$,*

$$a : p \leq q \Leftrightarrow ap \leq qa, \tag{43}$$

$$a : p \leq q \Leftrightarrow q'ap \leq 0. \tag{44}$$

PROOF. Immediate from (llp) and Lemma 3.4, respectively. □

From (30) we get the following import/export rule for the preimage.

COROLLARY 6.2. *Let A be a δ-semiring. For all $a \in A$ and $p, q \in \mathsf{test}(A)$,*

$$p(a : q) = (pa) : q. \tag{45}$$

Lemma 6.1 has the following consequence that couples preimages and images.

LEMMA 6.3. *Let A be a $\delta\rho$-semiring. The preimage and image operations satisfy the following* opposition law. *For all $a \in A$ and $p, q \in \mathsf{test}(A)$,*

$$a : p \leq q \Leftrightarrow q' : a \leq p'. \tag{46}$$

PROOF. Immediate from Lemma 6.1. □

The opposition law is a weak analogue of the Schröder rule from the relational calculus. Lemma 6.3 has the following immediate consequence.

COROLLARY 6.4. *Let A be a $\delta\rho$-semiring. For all $a \in A$ and $p, q \in \mathsf{test}(A)$,*

$$(p : a)q \leq 0 \Leftrightarrow p(a : q) \leq 0. \tag{47}$$

Lemma 4.11 immediately yields the following property.

COROLLARY 6.5. *Let A be a δ-semiring. Then $:$ is strict, distributes over addition and hence is isotone in both arguments.*

The sublocality law becomes

$$(ab) : p \leq a : (b : p); \tag{48}$$

in the presence of (loc) this becomes an equality. Finally, locality yields the following interaction of domain with preimage and of codomain with image.

LEMMA 6.6. *Let A be a δ-semiring. Then for all $a, b \in A$,*

$$\hat{\delta}(ab) = a : \hat{\delta}(b). \tag{49}$$

The preimage operator $a : p$ is a modal diamond operator $\langle a \rangle p$ as used in propositional dynamic logic (PDL). Sections 10 and 11 will further exploit this connection.

7. DOMAIN AND KLEENE STAR

So far, we have investigated domain and codomain operations in absence of the Kleene star. In fact, no further axioms are needed in its presence. Therefore, in this section, we only need to consider its interaction with domain, codomain, image and preimage. Only image and preimage show nontrivial behaviour. In particular, when the Kleene star is restricted to occur only within domain and codomain operators, a finite equational axiomatisation instead of the star induction axioms (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 formal derivation from a less efficient specification is particularly simple.

Henceforth, Kleene algebras with tests are called δ-Kleene algebras, $\delta\rho$-Kleene algebras, etc. when they extend the respective t-semirings. When we do not want to distinguish between Kleene algebra with predomain and precodomain or Kleene algebra with domain and codomain, 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 $A \in \mathsf{KAP}$. Then for all $a \in A$,*

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

The Kleene star in combination with images or preimages is more interesting. The laws in the following statements are analogous to the unfold axioms (1) and (2) of Kleene algebra.

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

$$p + a\mathbin{:}(a^*\mathbin{:}p) \geq a^*\mathbin{:}p \leq p + a^*\mathbin{:}(a\mathbin{:}p).$$

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

PROOF. By (11),

$$a^*\mathbin{:}p = (1 + a^*a)\mathbin{:}p = (1\mathbin{:}p) + (a^*a)\mathbin{:}p \leq p + a^*\mathbin{:}(a\mathbin{:}p).$$

The last step uses (31). The second half of the claim is shown analogously. The equations follow by using (loc) instead of (31). □

Note the analogy to (11). By Lemma 7.2, $a^*\mathbin{:}p$ is a fixed point of the mapping $\lambda x.p + a\mathbin{:}x$ when $A \in \mathsf{KAD}$.

LEMMA 7.3. *Let $A \in \mathsf{KAP}$. For all $a \in A$ and $p \in \mathsf{test}(A)$,*

$$a\mathbin{:}p \leq p \Rightarrow a^*\mathbin{:}p \leq p. \tag{50}$$

PROOF. Using Lemma 6.1 and (14), we calculate

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

□

Lemma 7.3 can 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 variants of the statements of Lemma 7.2 that lead to more efficient evaluation of the expressions involved. Second, when the Kleene star is restricted to occur only within preimages, we will show in the following lemma that there are even equivalent equational characterisations.

LEMMA 7.4. *Let $A \in \mathsf{KAD}$. Let $a \in A$ and $p, q \in \mathsf{test}(A)$. The following properties are equivalent. By Lemma 7.3 they hold in* KAD.

$$a : p \leq p \Rightarrow a^* : p \leq p, \tag{50}$$
$$q + a : p \leq p \Rightarrow a^* : q \leq p, \tag{51}$$
$$a^* : p \leq p + a^* : (p'(a : p)), \tag{52}$$
$$a^* : p = p + (ap')^* : (a : p). \tag{53}$$

PROOF. We first show that (50), (51) and (52) are equivalent.

(50) implies (51). $a : p + q \leq p$ iff $a : p \leq p$ and $q \leq p$ and therefore $a^* : p \leq p$ by the assumption. Hence also $a^* : q \leq p$ by isotonicity.

(51) implies (52). For $a^* : p \leq p + a^* : (p'(a : p))$ it suffices by (51) 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 Lemma 7.2 for KAD.

(52) implies (50). 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 (51) implies (53) and that (53) implies (50). This yields simpler proofs than a direct circle.

(51) implies (53). First, $p + (ap')^* : (a : p) \leq p + a^* : (a : p) = a^* : p$ by isotonicity of the Kleene star, the fact that $p' \leq 1$ and Lemma 7.2 with (loc). For the converse direction, that is, $a^* : p \leq p + (ap')^* : (a : p)$, it suffices by (51) 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:

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

The first two steps use additivity of domain, the third step uses $(ap')^* : (a : p) \leq 1$, the fourth step uses that $(ap) : 1 = a : p$, the fifth step uses Lemma 7.2 for KAD.

(53) implies (50). Assume $a:p \leq p$. Then

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

The third step uses Lemma 7.2, the fourth step uses that $(ap'):p = \delta(ap'p) = \delta(0) = 0$, the fifth step uses $a:0 = 0$. □

Note the analogy of (51) to the star induction axiom $b + ac \leq c \Rightarrow a^*b \leq c$, that is, (3) of Kleene algebra.

COROLLARY 7.5. *Let $A \in \mathsf{KAD}$. For all $a, b, c \in A$ and $p \in \mathsf{test}(A)$,*

$$b:q + (ac):p \leq c:p \Rightarrow (a^*b):q \leq c:p. \tag{54}$$

PROOF. The claim follows from (51), replacing p by $c:p$, q by $b:q$ and using (loc). □

Lemma 7.2 describes an unfolding step of the preimage operation. However, when viewed as a recursion for actually computing the preimage (say in reachability algorithms on graphs), this is not the most efficient version. 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 (53).

The unfold and induction laws for preimages are of further interest. The natural ordering and the operations of addition and multiplication can be lifted point-wise to the level of preimage operations. This yields operator semirings and operator Kleene algebras and introduces a further level of abstraction. Details are presented in [Möller and Struth 2005].

8. KLEENE ALGEBRAS AS VARIETIES

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

As usual in this field, we identify varieties with equational classes. By Birkhoff's theorem, these are precisely the classes that are closed under subalgebras, products and homomorphic images. A variety is finitely based if it can be axiomatised by a finite set of equations. The following lemma is immediate.

LEMMA 8.1. *The class of $\delta\rho$-semirings is a finitely based variety.*

The next lemma is not so immediate. It has been shown in [Kozen 1994b; Pratt 1990] that Kleene algebras with a residuation operation are finitely based varieties. 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 [Hollenberg 1997] for algebras related to PDL.

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

PROOF. In [Conway 1971], p. 106, an algebra A_p is given that shows that the algebra of regular events (cf. Example 2.9) is not finitely based. For every finite set of equations and every prime number p there is a particular valid equation ϕ_p parameterised by p that is not deducible, and there is an algebra A_p parameterised by p that satisfies the finite set of equations, but not ϕ_p. According to Conway, every expression in the language of Kleene algebra 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 $b \leq 0$, so that the integrality condition (34) holds.

Now, in the presence of domain, we consider the discrete t-semiring on A_p. Then, by Lemma 4.10 and Lemma 4.17, the mapping defined by $\delta(0) = 0$ and $\delta(a) = 1$ for all $0 \neq a \in A_p$ satisfies (d1), (d2) and (loc). In particular $0 \neq 1$.

Thus the expansion of A_p satisfies the finite set of equations and the domain axioms, but not ϕ_p. Consequently, the given finite set of equations is not complete for KAP and KAD. □

9. DOMAIN AXIOMS FOR RELATED STRUCTURES

The definition of predomain via (llp) looks very similar to a Galois connection. The equational axioms (d1) and (d2) are also quite reminiscent of so-called cancellation properties and Lemma 4.11 lists several further properties that would typically follow from a Galois connection. But a closer look reveals that it is not possible to rewrite (llp) in the form $f(p) \preceq q \Leftrightarrow p \sqsubseteq g(q)$ for partial orderings $\preceq$ on set B and $\sqsubseteq$ on set A, for $f : A \to B$ and $g : B \to A$ and for $p \in A$ and $q \in B$. This explains why the present definition differs from its predecessors in related structures. The precise relation is as follows.

LEMMA 9.1. *Let A be a t-semiring with greatest element $\top$. Then for all $a \in A$ and $p \in \mathsf{test}(A)$,*

$$a \leq pa \Leftrightarrow a \leq p\top. \tag{55}$$

If A is a δ-semiring this implies the Galois connection

$$\delta(a) \leq p \Leftrightarrow a \leq p\top. \tag{56}$$

PROOF. We only show (55) from which (56) follows by (llp).
Let $a \leq pa$. Then $a \leq p\top$ follows by isotonicity.
Let $a \leq p\top$. Then $a = (p + p')a = pa + p'a \leq pa + p'p\top = pa$. □

Although the Galois connection (56) is equivalent to (llp) in t-semirings with greatest element, this does not hold in general semirings and does not yield there all desirable properties of predomain. We now investigate alternative conditions under which the Galois connection (56) becomes equivalent to (llp).

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 multiplication is additive in both arguments. l-monoids are extensively studied in [Birkhoff 1984]. *d-monoids* and *b-monoids* are l-monoids with lattice reducts that are distributive and Boolean, respectively. When A is a b-monoid with complement $\overline{a}$ for each $a \in A$, complementation restricted to subidentities can be defined as $p' = 1 \sqcap \overline{p} = 1 - p$. This turns the entire set of subidentities into a Boolean subalgebra of A.

LEMMA 9.2.

(i) *Let A be a b-monoid. Let $a \in A$ and p be an arbitrary subidentity. Then*

$$a \leq p\top \Leftrightarrow a \leq pa. \tag{57}$$

(ii) *In a b-monoid A, all subidentities are multiplicatively idempotent.*

(iii) *The left-to-right implication in (57) does not hold in all d-monoids with $\top$.*

PROOF.

(i) With the definition of p' as given above, the proof is the same as for Lemma 9.1.

(ii) Using isotonicity and (57) we calculate, for $p \leq 1$,

$$\mathsf{true} \Leftrightarrow p \leq p\top \Leftrightarrow p \leq pp \Leftrightarrow p = pp.$$

(iii) The i-semiring A_4^1 of Example 2.6 is clearly also a d-monoid with $\top = b$, since the natural ordering is a chain. It satisfies $a = ab = a\top$, but $a \not\leq 0 = aa$. Note that A_4^1 can be made into a discrete domain semiring, but no other test semiring, since the element a has no complement.

□

This lemma does not mention t-semirings and therefore is different from Lemma 9.1. It implies that b-monoids also admit a definition of domain via the Galois connection (56). These statements could be sharpened by taking Heyting algebras into account. This is, however, left for future work.

Computational algebras with a notion of iteration have also been based on l-monoids, usually on *complete* l-monoids, for which the underlying lattice possesses arbitrary infima and suprema. A *quantale* [Mulvey 1986], for instance, is a complete l-monoid in which multiplication distributes over arbitrary suprema in both arguments. Classical examples are the *standard Kleene algebras* of [Conway 1971] (where meet is not explicitly present but can be defined by completeness of the underlying lattice). Iteration on b-quantales has been studied, for instance, in [Desharnais and Möller 2001; Desharnais et al. 2000]. The sequential algebras of [Hoare and von Karger 1995] are also particular b-quantales. Now, the Knaster-Tarski theorem guarantees existence of the Kleene star as the least fixed point of an isotone function and of predomain and domain defined via the Galois connection (56) (cf. [Aarts 1992]). Lemma 9.2, however, shows that these results do not transfer to the more general case of (non-complete) t-semirings and Kleene algebras with tests.

But still our generalisation pays. First, it encompasses the definitions for the more special structures, whence admits a larger model class, but nevertheless leads to a simple calculus that entails many natural properties. Second, Kleene algebras are first-order structures whereas quantales are essentially higher-order. This makes Kleene algebras more suitable for automated reasoning. Third, the lattice-based approaches introduce operations like meet and complementation that are not always convenient in applications. The complement of a program, for instance, relates all states that are not in the input/output relation. While this is fine for sequential programs, it leads to difficulties in presence of parallelism. Kleene algebras offer the advantage of avoiding this.

10. RECONSTRUCTING NOETHERICITY

In this section we demonstrate the expressiveness 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 formulation of Noethericity is more generally applicable than that of ω-algebra [Cohen 2000], an extension of Kleene algebra with infinite iteration that is defined as a greatest fixed point by expressions similar to the star unfold and induction axioms. Moreover, adapting a result from [Goldblatt 1985], we show that for transitive relations our concept is also equivalent to an algebraic variant of Löb's formula from modal logic (cf. [Bull and Segerberg 1984; Chellas 1980]). Finally, we show that some well-known properties of well-founded relations can be calculated in KAD in a simple concise way.

According to the standard definition, a relation R on a set M is well-founded iff every non-empty subset of M has an R-minimal element. In a δ-semiring A, the minimal part of $p \in \mathsf{test}(A)$ with respect to some $a \in A$ can algebraically be characterised as $p - p\,{:}\,a$, that is, as the set of points that have no a-predecessor in p. So, by contraposition, the well-foundedness condition holds iff for all $p \in \mathsf{test}(A)$ one has $p - p\,{:}\,a \leq 0 \;\Rightarrow\; p \leq 0$. Using Boolean algebra we therefore obtain the following abstract characterisation of well-foundedness and its dual, Noethericity.

10.1 Noethericity: Axioms and Simple Properties

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

$$p \leq p\,{:}\,a \Rightarrow p \leq 0. \tag{58}$$

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

$$p \leq a\,{:}\,p \Rightarrow p \leq 0. \tag{59}$$

We now calculate abstract variants of some simple 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. In the context of termination, reflexivity is not a desirable property, as we will see. The transitive closure $a^+ = aa^*$ is more interesting than a^* itself. We say that a is *transitive* if $aa \leq a$.

LEMMA 10.1. *Let $A \in \mathsf{KAD}$. Let $a, b \in A$ and let $0 \neq 1$.*

(i) *0 is Noetherian.*
(ii) *Every test $p \neq 0$ is not Noetherian.*
(iii) *If a is Noetherian and $b \leq a$, then b is Noetherian.*
(iv) *If a is Noetherian, then the only test below a is 0. In particular, $1 \not\leq a$.*
(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) Every such p satisfies $p \leq pp = p : p$.

(iii) Let a be Noetherian and let $b \leq a$. Then $p \leq b : p \Rightarrow p \leq a : p \Rightarrow p \leq 0$. Thus b is Noetherian.

(iv) Assume $p \leq a$. Then by (iii) p is Noetherian, so that by (ii) we infer $p = 0$.

(v) Let a be dense and Noetherian. $a \leq aa$ implies $a : p \leq a : (a : p)$, by isotonicity and (31). Thus $a : p \leq 0$ for all $p \in \mathsf{test}(A)$. 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 (loc), $a^*a^* = a^*$ 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).

□

10.2 Noethericity and ω-Algebra

We now investigate how our Noethericity axiom relates to ω-algebras. We do not introduce the axioms for this class. Intuitively, while an expression a^* denotes finite iteration of a, a^ω denotes strictly infinite iteration. Consequently, in ω-algebra, Noethericity of a means absence of proper infinite iteration of a; thus $a^\omega = 0$. In our calculations we only need the property

$$a^\omega \leq aa^\omega. \tag{60}$$

LEMMA 10.2. *Let A be an ω-algebra that is also a δ-semiring. Then for all $a \in A$, if a is Noetherian then $a^\omega = 0$.*

PROOF. Let a be Noetherian. Using (31) we obtain

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

Thus $\delta(a^\omega) = 0$ by Noethericity axiom (59). By Lemma 4.11(i), this is the case if and only if $a^\omega = 0$. □

The converse implication does not hold. The language semiring of Example 2.9 can be extended to an ω-algebra by setting $a^\omega = \Sigma^*$ if $\varepsilon \in a$ and $a^\omega = 0$ otherwise. Then $a^\omega = 0$ if $1 \sqcap a = 0$. But for $a \neq 0$ also $a : p = p$ holds for all tests p, so that then a is not Noetherian.

10.3 Noethericity and Löb's Formula

We now investigate an alternative characterisation 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 characterised by Löb's formula (cf. [Bull and Segerberg 1984; Chellas 1980])

$$\Box(\Box p \to p) \to \Box p.$$

For our purposes, the dual version $\Diamond p \to \Diamond(p \wedge \neg\Diamond p)$ is more convenient, since it can immediately be translated into KAD:

$$a : p \leq a : (p - a : p). \tag{61}$$

Here we have transcribed $\Diamond p$ into $a : p$, where a is a Kleene element that represents the underlying Kripke frame, and $p - q$ stands for pq'.

We say that a is *Löbian* if it satisfies (61). In relational Kleene algebra, Löb's formula states that a is transitive and that there are no infinite a-chains. We will now relate Löb's formula and our Noethericity axiom. But first we need a technical lemma.

LEMMA 10.3. *Let $A \in \mathsf{KAD}$. Let $a \in A$ and $p, q \in \mathsf{test}(A)$.*

(i) $a : p - a : q \leq a : (p - q)$,

(ii) $a^+ : p = a : (p + a^+ : p)$.

PROOF.

(i) $a : p = a : (p(q + q')) = a : (pq) + a : (pq') \leq a : q + a : (pq')$. The result then follows from the definition of subtraction.

(ii) Immediate from Lemma 7.2 and the definition of a^+.

□

The following theorem is essentially due to [Goldblatt 1985].

THEOREM 10.4. *Let $A \in \mathsf{KAD}$ and let $a \in A$.*

(i) *a is Noetherian if it is Löbian.*

(ii) *If a is Noetherian then, for all $p \in \mathsf{test}(A)$,*

$$a : p \leq a^+ : (p - a : p). \tag{62}$$

(iii) *a is Löbian if it is Noetherian and transitive.*

PROOF.

(i) Let $p \leq a : p$. Thus equivalently $p - a : p \leq 0$ by Boolean algebra. Using (61) we calculate $p \leq a : p \leq a : (p - a : p) \leq a : 0 = 0$.

(ii) First, observe that (62) is equivalent to $a : p - a^+ : (p - a : p) \leq 0$. Thus by Noethericity of a it suffices to show that

$$a : p - a^+ : (p - a : p) \leq a : (a : p - a^+ : (p - a : p)).$$

We calculate

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

The first and second step use Lemma 10.3(ii) and (i). The third step uses $p-(q+r) = (p-q)-r$, which holds in Boolean algebra. The fourth step uses $p-(p-q) = pq \leq q$, which holds again in Boolean algebra, and isotonicity.

(iii) For transitive a we have $a = a^+$ as the following instantiation of (4) shows:

$$aa^* \leq a \Leftarrow a + aa \leq a.$$

Now the claim is immediate from (ii).

□

Theorem 10.4 is a modal correspondence result. In this view, Noethericity expresses a frame property, which is part of semantics, whereas Löb's formula represents a part of modal syntax. KAD allows expressing syntax and semantics in one single formalism. Moreover, while the traditional proof of correspondence uses an (informal) semantic argument, the present one is entirely calculational. Further investigations of Noethericity in the context of KAD are outside the scope of the present paper; see [Desharnais et al. 2004b] for more details.

11. RECONSTRUCTING HOARE LOGIC

In this section we consider another application of KAP: an algebraic reconstruction of propositional Hoare logic. This kind of analysis is a popular exercise for many programming logics and algebras, among them PDL [Fischer and Ladner 1979] and KAT [Kozen 2001]. Since KAP is an extension of KAT, our overall result is no surprise. However it is interesting for at least two reasons. First, the encoding of the inference rules of the Hoare calculus in KAP is more direct and so are their soundness proofs. Second, the properties of the standard partial correctness semantics for Hoare logic [Loeckx and Sieber 1987; Apt and Olderog 1997] mirror precisely those of domain, so that KAP yields a natural algebraic semantics. A particular advantage over KAT is the possibility to express the weakest liberal precondition operator as

$$\mathsf{wlp}(a,p) = (a:p')' = [a]p$$

and to reconstruct the entire wlp-calculus as an equation-based calculus in KAP. This is, however, beyond the scope of the present text; see [Möller and Struth 2005] for details.

We now encode the relevant programming constructs in KAT,

$$a\,;b = ab, \qquad \mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b = pa + p'b, \qquad \mathsf{while}\ p\ \mathsf{do}\ a = (pa)^*p',$$

and briefly recall the syntax and semantics of Hoare logic. Basic formulas are *partial correctness assertions* of the form $\{p\}\ a\ \{q\}$, where p and q (the *precondition* and *postcondition*) denote properties of the store and a denotes an action or 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 interpreted as a relation between input and output. Traditionally, the Hoare calculus uses the following inference rules for reasoning about programs.

$$\text{Assignment} \qquad \{p[e/x]\}\ x := e\ \{p\},$$

$$\text{Composition} \qquad \frac{\{p\}\ a\ \{q\} \quad \{q\}\ b\ \{r\}}{\{p\}\ a\,;b\ \{r\}},$$

$$\text{Conditional} \qquad \frac{\{p \wedge q\}\ a\ \{r\} \quad \{p' \wedge q\}\ b\ \{r\}}{\{q\}\ \mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b\ \{r\}},$$

$$\text{While} \qquad \frac{\{p \wedge q\}\ a\ \{q\}}{\{q\}\ \mathsf{while}\ p\ \mathsf{do}\ a\ \{p' \wedge q\}},$$

$$\text{Weakening} \qquad \frac{p_1 \to p \quad \{p\}\ a\ \{q\} \quad q \to q_1}{\{p_1\}\ a\ \{q_1\}}.$$

Assignment is a non-propositional inference rule that deals with the internal structure of states. It is therefore abstracted away in this approach. Following [Kozen 2001], we call the fragment of Hoare logic without assignment *propositional Hoare logic* (PHL) and define partial correctness assertions in KAT by

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

Using the dual of (44), we can rewrite this definition more directly as

$$\{p\}\ a\ \{q\} \Leftrightarrow p : a \leq q. \tag{63}$$

Accordingly, the inference rules of PHL can be encoded as

$$\text{Composition} \qquad p : a \leq q \wedge q : b \leq r \Rightarrow p : (ab) \leq r,$$

$$\text{Conditional} \qquad (pq) : a \leq r \wedge (p'q) : b \leq r \Rightarrow q : (pa + p'b) \leq r,$$

$$\text{While} \qquad (pq) : a \leq q \Rightarrow q : ((pa)^* p') \leq p'q,$$

$$\text{Weakening} \qquad p_1 \leq p \wedge p : a \leq q \wedge q \leq q_1 \Rightarrow p_1 : a \leq q_1.$$

THEOREM 11.1. *The encoded rules of* PHL *are derivable in* KAP. *Therefore* PHL *is sound with respect to this algebraic semantics.*

PROOF. (Composition): $p : (ab) \leq (p : a) : b \leq q : b \leq r$.
The first step uses (31), the second one the assumption and isotonicity.
(Conditional): $q : (pa + p'b) = (pq) : a + (p'q) : b \leq r + r = r$.
(While): $(pq) : a \leq q \Rightarrow q : (pa)^* \leq q \Rightarrow (q : (pa)^*)p' \leq qp' \Leftrightarrow q : ((pa)^* p') \leq p'q$.
The first step uses commutativity of tests and (50). The third step uses again import/export and commutativity of tests.
(Weakening): $p_1 : a \leq p : a \leq q \leq q_1$.

Now soundness means that for every PHL-provable partial correctness assertion there is a calculation in KAP using translated statements. This follows by induction on the structure of PHL-proofs and our previous considerations. □

Thus, soundness of PHL can be proved literally in four lines from our domain calculus in KAP. Compared to the KAT-based approach, our encodings and proofs

are more direct and intuitive. Compared to standard set-theoretic proofs (c.f [Apt and Olderog 1997; Loeckx and Sieber 1987]), our proof is about ten times shorter, without taking into account the fact that many logical and set-theoretic assumptions are left implicit there. Moreover, it has already been observed in [Kozen 2001] 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 KAP. PHL is too weak to derive all such formulas. Finally, Hoare logic is an example where the domain operator can be completely eliminated from all expressions by using (gla). Even more, 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 [Cohen 1994; Kozen 2001; Kozen and Smith 1996] yields decidability of this fragment.

In [Möller and Struth 2005], using KAD instead of the weaker KAP, even a fully algebraic proof of relative completeness of PHL is presented. As a conclusion, we can only support [Kozen 2001] that*the specialised syntax and deductive apparatus of Hoare logic are inessential and can be replaced by simple equational reasoning.* We also believe that KAP and KAD offer further advantages. They combine the intuitiveness and readability of specifications in Hoare logic and imperative program semantics with the algorithmic power and the equational reasoning of KAT.

12. CONCLUSION AND OUTLOOK

We have presented equational axioms for domain and codomain operations for certain idempotent semirings and Kleene algebras. This algebraic abstraction is intended as a unified view on modal, relational and algebraic 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: algebraic accounts of Noethericity and Hoare logic. Our results provide the foundations of KAD, introduce the basic calculus and form the basis for further investigations.

On the theory side, expressiveness, complexity, representability or completeness of KAD have not been investigated in this text. The same holds for the apparent relation to modal algebras, algebraic variants of PDL, temporal logics, the modal μ-calculus and process algebras. On the application side, it will be interesting to continue our work in program semantics and termination, rewriting theory, algorithm development and the analysis of hardware and software systems. Some results on these topics are surveyed in [Desharnais et al. 2004a].

In general, the flexibility and naturalness of KAD make it a promising tool for the specification and analysis of state transition systems. As often with Kleene algebra, KAD might offer a simple uniform calculus where different specialised formalisms and complicated reasoning had to be used before.

ACKNOWLEDGMENTS

We would like to thank Thorsten Ehm, Marcelo Frías, Hitoshi Furusawa and Dexter Kozen for discussions and helpful comments. We are particularly indebted to Wolfram Kahl for pointing out an error in a preliminary version. The constructive criticism of the anonymous referees helped in improving the presentation.

REFERENCES

Aarts, C. J. 1992. Galois connections presented calculationally. M.S. thesis, Eindhoven University of Technology, Department of Mathematics and Computing Science.

Abrial, J.-R. 1996. *The B-Book*. Cambridge University Press.

Apt, K.-R. and Olderog, E.-R. 1997. *Verification of Sequential and Concurrent Programs*, 2nd ed. Springer.

Birkhoff, G. 1984. *Lattice Theory*. Colloquium Publications, vol. 25. American Mathematical Society. Reprint.

Bull, R. and Segerberg, K. 1984. Basic modal logic. In *Handbook of Philosophical Logic*, D. Gabbay and F. Guenthner, Eds. Vol. II. D. Reidel, Chapter II.1, 1–88.

Chellas, B. F. 1980. *Modal Logic: An Introduction*. Cambridge University Press.

Cohen, E. 1994. Hypotheses in Kleene algebra. Unpublished manuscript.

Cohen, E. 2000. Separation and reduction. In *Proc. of Mathematics of Program Construction, 5th International Conference, MPC 2000*, R. Backhouse and J. N. Oliveira, Eds. LNCS, vol. 1837. Springer, 45–59.

Conway, J. H. 1971. *Regular Algebra and Finite State Machines*. Chapman and Hall.

Crvenkovič, S., Dolinka, I., and Ésik, Z. 2000. The variety of Kleene algebras with conversion is not finitely based. *Theoretical Computer Science 230*, 235–245.

Desharnais, J. and Möller, B. 2001. Characterizing determinacy in Kleene algebras. *Information Sciences 139,* 3–4, 253–273.

Desharnais, J., Möller, B., and Struth, G. 2004a. Applications of modal Kleene algebra — a survey. *JoRMiCS — Journal on Relational Methods in Computer Science 1*, 93–131. `http://www.cosc.brocku.ca/Faculty/Winter/JoRMiCS`.

Desharnais, J., Möller, B., and Struth, G. 2004b. Termination in modal Kleene algebra. In *Exploring new frontiers of theoretical informatics*, J.-J. Lévy, E. Mayr, and J. Mitchell, Eds. IFIP International Federation for Information Processing Series, vol. 155. Kluwer, 647–660.

Desharnais, J., Möller, B., and Tchier, F. 2000. Kleene under a demonic star. In *Algebraic Methodology and Software Technology*, T. Rus, Ed. LNCS, vol. 1816. Springer, 355–370.

Eilenberg, S. 1974. *Automata, Languages and Machines*. Vol. A. Academic Press.

Fischer, J. M. and Ladner, R. F. 1979. Propositional dynamic logic of regular programs. *J. Comput. System Sci. 18,* 2, 194–211.

Gaubert, S. and Plus, M. Jan. 1997. Methods and applications of (max,+) linear algebra. Tech. Rep. RR-3088, INRIA-Rocquencourt.

Goldblatt, R. 1985. An algebraic study of well-foundedness. *Studia Logica 44,* 4, 422–437.

Harel, D., Kozen, D., and Tiuryn, J. 2000. *Dynamic Logic*. MIT Press.

Hoare, C. A. R. and von Karger, B. 1995. Sequential calculus. *Information Processing Letters 53,* 3, 123–130.

Hollenberg, M. 1997. Equational axioms of test algebra. In *Computer Science Logic, 11th International Workshop, CSL'97*, M. Nielsen and W. Thomas, Eds. LNCS, vol. 1414. Springer, 295–310.

Kozen, D. 1979. A representation theorem for $*$-free PDL. Tech. Rep. RC7864, IBM.

Kozen, D. 1994a. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation 110,* 2, 366–390.

Kozen, D. 1994b. On action algebras. In *Logic and Information Flow*, J. van Eijck and A. Visser, Eds. MIT Press, 78–88.

Kozen, D. 1997. Kleene algebra with tests. *Trans. Programming Languages and Systems 19,* 3, 427–443.

Kozen, D. 2001. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic 1,* 1, 60–76.

Kozen, D. and Smith, F. 1996. Kleene algebra with tests: Completeness and decidability. In *Proc. of 10th International Workshop on Computer Science Logic (CSL'96)*, D. van Dalen and M. Bezem, Eds. LNCS, vol. 1258. Springer, 244–259.

Kuich, W. 1997. Semirings and formal power series: Their relevance to formal languages and automata. In *Handbook of Formal Language Theory*, G. Rozenberg and A. Salomaa, Eds. Vol. I. Springer-Verlag, 609–677.

Loeckx, J. and Sieber, K. 1987. *The Foundations of Program Verification*, 2nd ed. Wiley Teubner.

Möller, B. 2005. Complete tests do not guarantee domain. Tech. Rep. 2005-6, Universität Augsburg, Institut für Informatik.
`http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2005-6.pdf`.

Möller, B. and Struth, G. 2005. Algebras of modal operators and partial correctness. *Theoretical Computer Science*. To appear.

Mulvey, C. 1986. &. *Rend. Circ. Math. Palermo 2,* 12, 99–104.

Németi, I. 1981. Dynamic algebras of programs. In *Proc. FCT'81 — Fundamentals of Computation Theory*. LNCS, vol. 117. Springer, 281–291.

Pratt, V. 1988. Dynamic logic as a well-behaved fragment of relation algebras. In *Conference on Algebra and Computer Science*, D. Pigozzi, Ed. LNCS, vol. 425. Springer, 77–110.

Pratt, V. 1990. Action logic and pure induction. In *Logics in AI, European Workshop, JELIA'90*, J. van Eijck, Ed. LNCS, vol. 478. Springer, 97–110.

Pratt, V. 1991. Dynamic algebras: Examples, constructions, applications. *Studia Logica 50*, 571–605.

Schmidt, G. W. and Ströhlein, T. 1993. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer.

Spivey, J. M. 1988. *Understanding Z*. Cambridge University Press.

Trnkova, V. and Reiterman, J. 1987. Dynamic algebras with tests. *J. Comput. System Sci. 35*, 229–242.

Received October 2003; revised November 2004; accepted January 2005