Logical Methods in Computer Science
Vol. 7 (1:1) 2011, pp. 1–29
www.lmcs-online.org

Submitted Jul. 28, 2006
Published Feb. 11, 2011

ALGEBRAIC NOTIONS OF TERMINATION

JULES DESHARNAIS [a], BERNHARD MÖLLER [b], AND GEORG STRUTH [c]

[a] Département d'informatique et de génie logiciel, Pavillon Adrien-Pouliot, 1065, avenue de la Médecine, Université Laval, Québec, QC, Canada, G1V 0A6
e-mail address: Jules.Desharnais@ift.ulaval.ca

[b] Institut für Informatik, Universität Augsburg, Universitätsstr. 14, D-86135 Augsburg, Germany
e-mail address: moeller@informatik.uni-augsburg.de

[c] Department of Computer Science, The University of Sheffield, Sheffield S1 4DP, United Kingdom
e-mail address: g.struth@dcs.shef.ac.uk

Abstract. Five algebraic notions of termination are formalised, analysed and compared: wellfoundedness or Noetherity, Löb's formula, absence of infinite iteration, absence of divergence and normalisation. The study is based on modal semirings, which are additively idempotent semirings with forward and backward modal operators. To model infinite behaviours, idempotent semirings are extended to divergence semirings, divergence Kleene algebras and omega algebras. The resulting notions and techniques are used in calculational proofs of classical theorems of rewriting theory. These applications show that modal semirings are powerful tools for reasoning algebraically about the finite and infinite dynamics of programs and transition systems.

1. Introduction

Idempotent semirings and Kleene algebras are fundamental structures in computer science with widespread applications. Roughly, idempotent semirings are rings without subtraction and with idempotent addition; Kleene algebras also provide an operation for finite iteration or reflexive transitive closure. Initially conceived as algebras of regular events [19], Kleene algebras have been extended by tests to model regular programs [20] and by infinite iteration to analyse reactive systems [7], program refinement [35] and rewriting systems [31, 32]. More recently, modal operators for idempotent semirings and Kleene algebras have been introduced [8, 10, 24] in order to model properties of programs and transition systems more conveniently and to link algebraic and relational formalisms with traditional approaches such as dynamic and temporal logics.

1998 ACM Subject Classification: F.3.1, F.3.2, F.4.1.

Key words and phrases: Idempotent semirings, Kleene algebras, omega algebras, divergence semirings, modal operators, wellfoundedness, Noetherity, rewriting theory, program analysis, program termination.

[a,b,c] We gratefully acknowledge partial support of this research by NSERC (Natural Sciences and Engineering Research Council of Canada (J. Desharnais)) and within the Project InopSys (Interoperability of System Calculi) by DFG (Deutsche Forschungsgemeinschaft (B. Möller, G. Struth)).

DOI:10.2168/LMCS-7 (1:1) 2011

Here, we propose modal semirings and modal Kleene algebras as tools for termination analysis of programs and transition systems: for formalising specifications and calculating proofs that involve termination, and for analysing and comparing different notions of termination. Benefits of this algebraic approach are simple abstract specifications, concise equational proofs, easy mechanisability and connections with automata-based decision procedures. Induction with respect to external measures, for instance, is avoided in favour of internal fixpoint reasoning. Abstract, point-free, proofs can often be obtained in the algebra of modal operators.

The first contribution is a specification and comparison of five notions of termination in modal semirings and modal Kleene algebras.

(1) We translate the standard set-theoretic notions of Noetherity and wellfoundedness and demonstrate their adequacy by several examples.
(2) We translate Löb's formula from modal logic (cf. [5]) and show its compatibility with the set-theoretic notions. We prove this modal correspondence result for a second-order frame property entirely by simple equational reasoning.
(3) We express termination as absence of infinite iteration in omega algebra [7]. This notion differs from the set-theoretic one.
(4) We extend modal semirings to divergence semirings, thus modelling the sources of possible nontermination in a state space. The corresponding notion of termination is proved compatible with the set-theoretic one.
(5) We express termination via normalisation. This is again compatible with the set-theoretic notion.

This analysis shows that modal semirings and modal Kleene algebras are powerful tools for analysing and integrating notions of termination. Their rich model classes, as investigated in [10], and the flexibility to switch between relation-style and modal reasoning makes the present approach more general than previous relation-based [12, 27], non-modal [7, 35] and mono-modal ones [15] which inspired this work.

The second contribution is an application of our termination techniques in rewriting theory, continuing previous research [13, 31, 32] on abstract reduction systems. Here, we prove the wellfounded union theorem of Bachmair and Dershowitz [2] and a variant of Newman's lemma for non-symmetric rewriting [30] in modal Kleene algebra and divergence Kleene algebra. While the calculational proof of the commutative union theorem is novel, that of Newman's lemma requires less machinery than previous ones [12, 27]. Together with the results from [32], these exercises show that large parts of abstract reduction can conveniently be modelled in variants of modal Kleene algebra.

The remainder of this text is organised as follows. Section 2 defines idempotent semirings, tests and modal operators together with their basic properties, symmetries and dualities. Section 3 adds unbounded finite iteration to yield (modal) Kleene algebras. Section 4 translates the set-theoretic notion of Noetherity to modal semirings and presents some basic properties. Sections 5 to 9 introduce and compare notions of termination based on modal logic, omega algebra, divergence semirings and normalisation. In particular, the novel concepts of divergence semiring and divergence Kleene algebra are introduced in Section 7 and a basic calculus for these structures is outlined in Section 8. Section 10 and Section 11 present calculational proofs of the wellfounded union theorem and of Newman's lemma. Section 12 uses normalisation to relate confluence properties with normal forms. Section 13 contains a conclusion and an outlook.

2. Modal Semirings

2.1. **Idempotent Semirings.** We start with the definition of the algebraic structure that underlies the other algebras introduced in this paper.

Definition 2.1. Let $S = (S, +, \cdot, 0, 1)$ be an algebra.

(1) S is a *semiring* if
   - $(S, +, 0)$ is a commutative monoid,
   - $(S, \cdot, 1)$ is a monoid,
   - multiplication distributes over addition from the left and right and
   - 0 is a left and right zero of multiplication.

(2) S is an *idempotent semiring* if S is a semiring and addition is idempotent, that is $a + a = a$.

We will usually omit the multiplication symbol. Two properties of semirings are particularly interesting for our purposes.

- Every semiring $S = (S, +, \cdot, 0, 1)$ induces an *opposite semiring* $S^{\mathrm{op}} = (S, +, \cdot^{\mathrm{op}}, 0, 1)$ in which the order of multiplication is swapped: $a \cdot^{\mathrm{op}} b = b \cdot a$. For every statement that holds in a semiring there is a dual one that holds in its opposite.
- Every idempotent semiring S admits a partial order, the *natural order* $\leq$ defined by $a \leq b$ iff $a + b = b$ for all $a, b \in S$. This turns $(S, +)$ into a semilattice. It is the only partial order for which addition is isotone in both arguments and for which 0 is the least element.

Idempotent semirings provide an algebraic model of sequential composition and angelic non-deterministic choice of actions.

Example 2.2. The set $2^{M \times M}$ of binary relations over a set M forms an idempotent semiring. Relations serve as a standard semantics for programs and transition systems, and as Kripke frames for modal logics. Relational composition $\circ$ is given by

$$(x, y) \in R \circ S \;\Leftrightarrow\; \exists z : (x, z) \in R \wedge (z, y) \in S \;,$$

and $I_M = \{(a, a) \,|\, a \in M\}$ is the identity relation, while $\emptyset$ is the empty relation. Then $\mathrm{REL}(M) = (2^{M \times M}, \cup, \circ, \emptyset, I)$ is an idempotent semiring with set inclusion as the natural ordering. □

Example 2.3. Another idempotent semiring is formed by the formal languages over an alphabet under union and concatenation. Let Σ^* be the set of finite words over some finite alphabet Σ. We denote the empty word by ε and the concatenation of words v and w by vw. A (formal) language over Σ is a subset of Σ^*. Concatenation is lifted to languages by setting $L_1.L_2 = \{vw \,|\, v \in L_1, w \in L_2\}$. Then the structure $\mathrm{LAN}(\Sigma) = (2^{\Sigma^*}, \cup, ., \emptyset, \{\varepsilon\})$ is an idempotent semiring with language inclusion as its natural ordering. □

2.2. **Tests in Semirings.** Elements of general idempotent semirings abstractly represent sets of transitions. Assertions or sets of states are represented by special elements called tests [20] that form a Boolean subalgebra of the idempotent semiring. In the idempotent semiring $\mathrm{REL}(M)$ of relations, tests can be represented as partial identity relations, that is, as elements below the multiplicative unit 1. Join and meet of these elements coincide with their sum and product. This motivates the following abstract definition.

Definition 2.4. A *test* in an idempotent semiring S is an element $p \leq 1$ that has a *complement* relative to 1, that is, there is a $q \in S$ with $p + q = 1$ and $pq = 0 = qp$. The set of all tests of S is denoted by $\mathsf{test}(S)$.

Straightforward calculations show that $\mathsf{test}(S)$ is closed under $+$ and $\cdot$ and has 0 and 1 as its least and greatest element. Moreover, the complement of a test p is uniquely determined by this definition; we denote it by $\neg p$. Hence $\mathsf{test}(S)$ indeed forms a Boolean algebra, that is, a complemented distributive lattice. We will consistently write $a, b, c \ldots$ for arbitrary semiring elements and $p, q, r, \ldots$ for tests. We will freely use the standard Boolean operations on $\mathsf{test}(S)$, for instance implication $p \to q = \neg p + q$ and relative complementation $p - q = p \cdot \neg q$, with their usual laws. We impose that $\neg$, as a unary operator, binds more tightly than $+$ or $\cdot$.

The above definition of tests deviates slightly from that in [20] in that it does not allow an arbitrary Boolean algebra of subidentities as $\mathsf{test}(S)$, but only the maximal complemented one. The reason is that the axiomatisation of the modal operators presented below forces this anyway (see [10]).

2.3. **Galois Connections.** A *Galois connection* (cf. [21]) is a pair of mappings $f^\flat : B \to A$ and $f^\sharp : A \to B$ between posets $(A, \leq_A)$ and $(B, \leq_B)$ such that, for all $a \in A$ and $b \in B$,

$$f^\flat(b) \leq_A a \Leftrightarrow b \leq_B f^\sharp(a) \ .$$

The mappings $f^\flat$ and $f^\sharp$ are called the *lower* and *upper adjoints* of the Galois connection.

In the remainder we omit the indices of the partial order relations involved. Moreover, we will freely use the standard pointwise lifting of partial orders to functions. Lower and upper adjoints enjoy many properties.

(1) $f^\flat(x) = \mathsf{inf}\,\{y : x \leq f^\sharp(y)\}$ and $f^\sharp(y) = \mathsf{sup}\,\{x : f^\flat(x) \leq y\}$, whence lower and upper adjoints uniquely determine each other.
(2) $f^\flat$ and $f^\sharp$ satisfy the *cancellation properties* $f^\flat \circ f^\sharp \leq id$ and $id \leq f^\sharp \circ f^\flat$.
(3) Lower adjoints are *completely additive*: they preserve all existing suprema. Dually, upper adjoints are *completely multiplicative*: they preserve existing infima.

Since the function $(p\,\cdot) = \lambda x \,.\, p \cdot x$ on tests is the lower adjoint in the Galois connection $p \cdot q \leq r \Leftrightarrow q \leq p \to r$ and the function $(p+) = \lambda x \,.\, p + x$ on tests is the upper adjoint in the Galois connection $q - p \leq r \Leftrightarrow q \leq p + r$, we obtain that

$$(p\,\cdot) \text{ is completely additive,} \qquad \text{and } (p+) \text{ is completely multiplicative.} \tag{2.1}$$

The Galois connection for $(p\,\cdot)$ is equivalent to the *shunting rule*

$$p \cdot q \leq r \Leftrightarrow p \leq \neg q + r \ , \tag{shunting}$$

which is frequently used in calculations. To facilitate its use we state many assertions of the form $a = 0$ in the equivalent form $a \leq 0$ (the reverse inequation $0 \leq a$ holds anyway, since 0

is the least element of the respective idempotent semiring). An example is the special case $r = 0$ of shunting, namely $p \cdot q \leq 0 \Leftrightarrow p \leq \neg q$.

2.4. **Modal Operators.** Forward and backward diamond operators can be introduced as abstract preimage and image operators on idempotent semirings [24].

Definition 2.5. An idempotent semiring is called *modal* if for every element $a \in S$ there are operators $|a\rangle, \langle a| : \mathsf{test}(S) \to \mathsf{test}(S)$ that satisfy the following axioms:

$$|a\rangle p \leq q \Leftrightarrow \neg q a p \leq 0, \qquad \langle a| p \leq q \Leftrightarrow p a \neg q \leq 0, \tag{dia1}$$

$$|ab\rangle p = |a\rangle(|b\rangle p), \qquad \langle ab| p = \langle b|(\langle a| p). \tag{dia2}$$

Let us explain the axioms for the forward diamond. Let a model a set of transitions of a system and let the test p represent a subset of the state space on which a acts. Then the set $r = |a\rangle p$ represents the set of all states from which there is a transition to p, that is, the inverse image of p under a. If r is contained in another set q, then it is impossible to make an a-transition from outside q, that is, from the complement $\neg q$, into the set p. In other words, $\neg q a p$, which represents that part of a that has only transitions from the set $\neg q$ into the set p, must be empty. This is expressed by (dia1). The axiom (dia2) stipulates that the forward diamonds behave locally or modularly with respect to composition: the inverse image under ab coincides with the inverse image under a of the inverse image under b.

This axiomatisation is equivalent to the purely equational, domain-based one in [10], since we can define the domain and codomain of an element a as

$$\mathsf{dom}\, a = |a\rangle 1, \qquad \mathsf{cod}\, a = \langle a| 1.$$

Conversely,

$$|a\rangle p = \mathsf{dom}(ap), \qquad \langle a| p = \mathsf{cod}(pa).$$

Next we define forward and backward box operators as the De Morgan duals of diamonds:

$$|a] p = \neg |a\rangle \neg p, \qquad [a| p = \neg \langle a| \neg p.$$

Using De Morgan's laws and shunting one obtains the following properties of the box operators from (dia1) and (dia2):

$$p \leq |a] q \Leftrightarrow p a \neg q \leq 0, \qquad p \leq [a| q \Leftrightarrow \neg q a p \leq 0, \tag{box1}$$

$$|ab] p = |a](|b] p), \qquad [ab| p = [b|([a| p). \tag{box2}$$

The property (box1) means that the test $|a]q$ represents the set of all states from which all transitions (if any) lead into the set q. Hence $|a]q$ is an algebraic version of the weakest-liberal-precondition operator [11]; it can be used for an algebraic treatment of the calculus of partial correctness (see [24] and Example 7.8 for a summary). Property (box2) shows that also the box operators are well behaved with respect to composition.

2.5. **Algebra of Modal Operators.** The algebra of modal operators over an idempotent semiring has been studied in detail in [24]. Here we only present a brief synopsis.

Clearly, forward and backward operators of the same kind are duals with respect to opposition. Moreover, by (dia1) and (box1), boxes and diamonds are adjoints of a Galois connection:

$$|a\rangle p \le q \Leftrightarrow p \le [a|q, \qquad \langle a|p \le q \Leftrightarrow p \le |a]q. \tag{2.2}$$

Consequently, diamonds are (completely) additive and strict and boxes are (completely) multiplicative and co-strict, in particular,

$$\begin{array}{cc} |a\rangle(p+q) = |a\rangle p + |a\rangle q, & \langle a|(p+q) = \langle a|p + \langle a|q, \\ |a](pq) = |a]p \cdot |a]q, & [a|(pq) = [a|p \cdot [a|q, \\ |a\rangle 0 = 0, & \langle a|0 = 0, \\ |a]1 = 1, & [a|1 = 1. \end{array}$$

This entails interactions of the operators with subtraction and implication, since every additive endofunction f and every multiplicative endofunction g on a Boolean algebra satisfy, for all elements p and q,

$$f(p) - f(q) \le f(p - q), \qquad g(p \to q) \le g(p) \to g(q). \tag{2.3}$$

Next we present the behaviour of diamond and box with respect to addition:

$$\begin{array}{cc} |a + b\rangle p = |a\rangle p + |b\rangle p, & \langle a + b|p = \langle a|p + \langle b|p, \\ |a + b]p = |a]p \cdot |b]p, & [a + b|p = [a|p \cdot [b|p. \end{array}$$

Finally, we look at tests within boxes and diamonds. For $p, q \in \mathsf{test}(S)$,

$$|q\rangle p = qp = \langle q|p, \qquad |q]p = q \to p = [q|p. \tag{2.4}$$

In particular,

$$\begin{array}{cc} |0\rangle p = 0 = \langle 0|p, & |0]p = 1 = [0|p, \\ |1\rangle p = p = \langle 1|p, & |1]p = p = [p|p. \end{array}$$

2.6. **Modal Operators as Semiring Elements.** Many properties of modal semirings can be expressed more succinctly in the endofunction space $\mathsf{test}(S) \to \mathsf{test}(S)$. The semiring operations are lifted pointwise as

$$(f \pm g)(p) = f(p) \pm g(p)\ , \qquad (f \sqcap g)(p) = f(p) \cdot g(p)\ , \qquad (f \cdot g)(p) = f(g(p))$$

and likewise for the other Boolean operations. In particular, $\mathbf{1} = |1\rangle = \langle 1|$ and $\mathbf{0} = |0\rangle = \langle 0|$ are the identity and the constant 0-valued function on tests, respectively. Some immediate consequences of the pointwise lifting are the properties

$$(f \pm g)h = gh \pm gh\ , \qquad (f \sqcap g)h = fh \sqcap gh\ .$$

Moreover, we obtain distribution properties such as

$$|a + b\rangle = |a\rangle + |b\rangle, \qquad |a + b] = |a] \sqcap |b], \tag{2.5}$$

for addition, and covariant and contravariant laws

$$|ab\rangle = |a\rangle|b\rangle, \qquad \langle ab| = \langle b|\langle a|, \tag{dia2'}$$

for composition, which we apply tacitly most of the time.

This lifting yields further interesting operator-level laws. The Galois connections extend to endofunctions f and g on $\mathsf{test}(S)$:

$$|a\rangle f \le g \Leftrightarrow f \le [a|g, \qquad \langle a|f \le g \Leftrightarrow f \le |a]g. \tag{2.6}$$

This implies the following cancellation properties:

$$|a\rangle[a| \leq \mathbf{1} \leq [a||a\rangle, \qquad \langle a||a] \leq \mathbf{1} \leq |a]\langle a|. \tag{2.7}$$

Cancellation and isotony of the operators allow the following calculation:

$$f|a] \leq g \Rightarrow f|a]\langle a| \leq g\langle a| \Rightarrow f \leq g\langle a| \Rightarrow f|a] \leq g\langle a||a] \Rightarrow f|a] \leq g \ .$$

A similar derivation works for antitone operators. Hence we have the co-Galois connections

$$\begin{array}{ll} f|a] \leq g \Leftrightarrow f \leq g\langle a| & \text{if } f \text{ and } g \text{ are isotone,} \\ f|a\rangle \leq g \Leftrightarrow f \leq g[a| & \text{if } f \text{ and } g \text{ are antitone.} \end{array}$$

Moreover, diamonds are isotone and boxes are antitone, that is,

$$a \leq b \Rightarrow |a\rangle \leq |b\rangle, \quad \text{and} \quad a \leq b \Rightarrow |b] \leq |a]. \tag{2.8}$$

Diamonds and boxes satisfy variants of (2.3), that is,

$$|a\rangle f - |a\rangle g \leq |a\rangle(f - g), \qquad |a](f \to g) \leq |a]f \to |a]g. \tag{2.9}$$

Finally, the above laws entail the following lifting property.

Proposition 2.6. *The set of forward diamonds and the set of backward diamonds in a modal semiring each form an idempotent semiring.*

The point-free style and the properties of the operator algebra yield more concise specifications and proofs in the following sections.

3. Modal Kleene Algebras

Kleene algebras are idempotent semirings with an additional operation of finite iteration. Algebras that describe infinite iteration will be defined in Section 6.

Since the iteration operators will be defined as least or greatest fixpoints, we recapitulate some basic facts about these.

3.1. **Elements of Fixpoint Theory.** Let f be an endofunction on a poset $(A, \leq)$. Then $a \in A$ is a *pre-fixpoint* of f if $f(a) \leq a$. The notion of *post-fixpoint* is order-dual, and a is a *fixpoint* of f if it is both a pre- and a post-fixpoint. The least fixpoint of f is denoted μf, and the greatest fixpoints of f is denoted νf, whenever they exist. We write $\mu x \,.\, f$ and $\nu x \,.\, f$ to make the variables in f explicit.

By definition, if f, g are endofunctions with $f \leq g$ and the respective fixpoints exist, then $\mu f \leq \mu g$ and $\nu f \leq \nu g$.

The fixpoint theorem of Knaster and Tarski [33] states that μf and νf exist whenever $(A, \leq)$ is a complete lattice and f is isotone.

A useful proof rule is the principle of *greatest fixpoint fusion* (see, for example, [3] for the dual principle of least fixpoint fusion). It does not need the assumption of a complete lattice. Consider partial orders $(A, \leq_A)$ and $(B, \leq_B)$, and let $f : A \to B$, $g : A \to A$ and $h : B \to B$ be isotone mappings. Assume that f is completely multiplicative, which means that f is also the upper adjoint of a Galois connection between A and B, and that $fg = hf$. Then f is also the upper adjoint of a Galois connection between the set of post-fixpoints of g and the set of post-fixpoints of h. In particular, if g has a greatest post-fixpoint νg, then h also has a greatest post-fixpoint νh and $\nu h = f(\nu g)$. Since fixpoints correspond to recursions, this means that f can be fused with the recursion in g into the recursion for νh.

3.2. **Kleene Algebras.** Operations for finite iteration can be axiomatised in terms of least fixpoints.

Definition 3.1 ([19])**.** A *left-inductive Kleene algebra* is a structure $(S, ^*)$ such that S is an idempotent semiring and the star operation $^* : S \to S$ satisfies, for all $a, b, c \in S$, the *left unfold* and *left induction* axioms

$$1 + aa^* \leq a^*, \qquad b + ac \leq c \Rightarrow a^*b \leq c.$$

Right-inductive Kleene algebras are their duals with respect to opposition, that is, they satisfy the *right unfold* and *right induction* axioms $1 + a^*a \leq a^*$ and $b + ca \leq c \Rightarrow ba^* \leq c$.

By these axioms, $a^*b = \mu x.b + ax$ and $ba^* = \mu x.b + xa$. By isotony of the least fixpoint operator μ therefore the star operation is isotone with respect to the natural order.

Example 3.2. Extending the relation semiring $\mathrm{REL}(M)$ from example 2.2 by a reflexive transitive closure operation yields a left-inductive Kleene algebra: Define, for all $R \in \mathrm{REL}(M)$, the relation R^* as the reflexive transitive closure of R, that is, $R^* = \bigcup_{i \geq 0} R^i$, with $R^0 = I$ and $R^{i+1} = R \circ R^i$. We call $\mathrm{REL}(M)$ the *relational* Kleene algebra over M. □

Example 3.3. Another left-inductive Kleene algebra is formed by expanding the language semiring $\mathrm{LAN}(\Sigma)$ from Example 2.3 by the Kleene star. The definition is, as usual, $L^* = \{w_1 w_2 \dots w_n \mid n \geq 0, w_i \in L\}$. We call $\mathrm{LAN}(\Sigma)$ the *language* Kleene algebra over Σ. The operations $\cup$, . and * are 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*. □

Proposition 3.7 below shows that diamond operators form left-inductive Kleene algebras as well. Various further models are discussed in [10].

It can be shown that in a left-inductive Kleene algebra the star satisfies $aa^* = a^*a$; consequently, also the right unfold law $1 + a^*a \leq a^*$ holds.

Definition 3.4. In a left-inductive Kleene algebra, the *transitive closure* of a is

$$a^+ = aa^*.$$

We will freely use the well known properties of a^+.

Definition 3.5. [19] A *Kleene algebra* is a structure that is both a left-inductive and a right-inductive Kleene algebra.

In a Kleene algebra we have $a^+ = aa^* = a^*a$.

Definition 3.6. A Kleene algebra S is called *modal* if S is a modal semiring.

It turns out that no extra axiom for the interaction between star and the modal operators is needed since the following properties can be shown [10]:

$$p + |a\rangle|a^*\rangle p = |a^*\rangle p, \qquad p + |a^*\rangle|a\rangle p = |a^*\rangle p, \qquad q + |a\rangle p \leq p \Rightarrow |a^*\rangle q \leq p. \tag{3.1}$$

These are used to prove the following statement [24].

Proposition 3.7. *The set of forward diamonds and the set of backward diamonds in a left-inductive modal Kleene algebra each form a left-inductive Kleene algebra.*

In fact, $\mathbf{1} + |a\rangle|a^*\rangle = |a^*\rangle$, $\mathbf{1} + |a^*\rangle|a\rangle = |a^*\rangle$ and $f + |a\rangle g \leq g \Rightarrow |a^*\rangle f \leq g$ hold for arbitrary endofunctions f and g on a test algebra. This justifies setting $|a\rangle^* = |a^*\rangle$. Variants for the other modal operators follow by duality.

As shown in Proposition 2 of [14], the operator-level left star induction law is equivalent to the induction axiom of propositional dynamic logic

$$|a\rangle^* - \mathbf{1} \leq |a\rangle^*(|a\rangle - \mathbf{1}). \tag{3.2}$$

4. Termination via Noetherity

In this section we abstract the notions of wellfoundedness and Noetherity from the relation semiring $\mathrm{REL}(M)$ to modal semirings. In set theory, a relation R on a set M is wellfounded within a subset $N \subseteq M$ iff every non-empty subset of N has an R-minimal element. It is a standard exercise to show that this is equivalent to the absence of infinitely descending R-chains in N. An element of N is R-minimal in N iff it has no R-predecessor in N, or, equivalently, if it is not in the image $\langle R|N$ of N under R. Abstracting R to a semiring element a and N to a test p leads to the following definition.

Definition 4.1. For a modal semiring S and $a \in S, p \in \mathsf{test}(S)$, the *a-minimal part* of p is $\mathsf{min}_a\, p = p - \langle a|p$. In point-free style, $\mathsf{min}_a = \mathbf{1} - \langle a|$. Dually, the *a-maximal part* is $\mathsf{max}_a = \mathbf{1} - |a\rangle$.

On the one hand, therefore, a is wellfounded iff $\mathsf{min}_a\, p$ is non-empty whenever p is. On the other hand, an infinitely descending a-chain corresponds to a $p \neq 0$ for which $\mathsf{min}_a\, p = 0$. Absence of infinitely descending a-chains therefore means that 0 is the only p that satisfies $\mathsf{min}_a\, p \leq 0$.

Since wellfoundedness and Noetherity are dual with respect to opposition, and since we are mainly interested in termination, that is, absence of strictly ascending sequences of actions, we will restrict our attention to Noetherity.

Definition 4.2. An element a of a modal semiring S is *Noetherian* if, for all $p \in \mathsf{test}(S)$,

$$\mathsf{max}_a\, p \leq 0 \Rightarrow p \leq 0.$$

Dually, a is *wellfounded* if, for all $p \in \mathsf{test}(S)$,

$$\mathsf{min}_a\, p \leq 0 \Rightarrow p \leq 0.$$

Similar definitions for related structures have been given in [1, 12, 15, 27]. The following result is immediate from the definitions in Section 3.1.

Corollary 4.3. *Assume a modal semiring S and $a \in S, p \in \mathsf{test}(S)$.*
(1) $\mathsf{max}_a\, p \leq 0$ *iff p is a post-fixpoint of the endofunction $|a\rangle$ on $\mathsf{test}(S)$.*
(2) *a is Noetherian iff 0 is the unique post-fixpoint of $|a\rangle$, that is, iff for all $p \in \mathsf{test}(S)$,*

$$p \leq |a\rangle p \Rightarrow p \leq 0.$$

We now relate Noetherity and finite iteration.

Lemma 4.4. *Assume a modal Kleene algebra S and $a \in S, p \in \mathsf{test}(S)$. Define the endofunction $h_p : \mathsf{test}(S) \to \mathsf{test}(S)$ by $h_p(x) = p + |a\rangle x$.*
(1) $\mu h_p = |a^*\rangle p$.

(2) *If the greatest fixpoint $\nu|a\rangle$ of $|a\rangle$ exists, then the greatest fixpoint νh_p exists, too, and $\nu h_p = \mu h_p + \nu|a\rangle$.*
(3) *With the assumptions of Part (2), if a is Noetherian then h_p has the unique fixpoint μh_p.*
(4) *If, for all p, the function h_p has a unique fixpoint, then a is Noetherian.*

Proof.
(1) This follows from (3.1).
(2) The proof uses greatest fixpoint fusion (cf. Section 3.1) with $f(x) = \mu h_p + x$, $g = |a\rangle$ and $h = h_p$. Since $f = (\mu h_p +)$ is completely multiplicative by (2.1), it suffices to show that $fg = h_p f$. This is implied by star induction (3.1) and additivity of $|a\rangle$:
$$f(g(x)) = |a\rangle^* p + |a\rangle x = p + |a\rangle|a\rangle^* p + |a\rangle x = p + |a\rangle(|a\rangle^* p + x) = h_p(f(x)).$$
(3) If a is Noetherian, then Corollary 4.3(2) implies that $\nu|a\rangle = 0$, and the claim follows from (2).
(4) Uniqueness and (2) imply, for all p, that $\mu h_p = \nu h_p = \mu h_p + \nu|a\rangle$, which by definition of the natural order is equivalent to $\nu|a\rangle \leq \mu h_p$. Since for $p = 0$ we have by definition $h_p = |a\rangle$, we therefore obtain $\nu|a\rangle \leq \mu h_0 = \mu|a\rangle$. But strictness of $|a\rangle$ shows $\mu|a\rangle = 0$. □

A similar result for regular algebras appears in [4]. Our setting is more general in that we do not require completeness of the lattice induced by the natural order.

We now collect some algebraic properties of max.

Lemma 4.5. *Let S be a modal semiring. Let $a, b \in S$ and $p \in \mathsf{test}(S)$.*
(1) $\mathsf{max}_{a+b} = \mathsf{max}_a \sqcap \mathsf{max}_b$.
(2) $\mathsf{max}_0 = \mathbf{1}$.
(3) $\mathsf{max}_1 = \mathbf{0}$.
(4) $\mathsf{max}_a\,|a\rangle \leq |a\rangle\,\mathsf{max}_a$.
(5) *If S is a modal Kleene algebra then* $\mathsf{max}_a\,|a\rangle^* \leq |a\rangle^*\,\mathsf{max}_a$.
(6) $a \leq b \Rightarrow \mathsf{max}_b \leq \mathsf{max}_a$.
(7) *For $m = \mathsf{max}_a\,1$ we have $m = \neg\mathsf{dom}\,a = |a]0$. Hence $ma = 0$ and $ma^* = m$.*
(8) $\mathsf{max}_{a^*} = \mathbf{0}$.

Proof.
(1) By Boolean algebra,
$$\mathsf{max}_{a+b} = \mathbf{1} - (|a\rangle + |b\rangle) = (\mathbf{1} - |a\rangle) \sqcap (\mathbf{1} - |b\rangle) = \mathsf{max}_a \sqcap \mathsf{max}_b.$$
(2) and (3) follow immediately from the definition of max.
(4) Using the definition of relative complementation and (2.9), we calculate
$$\mathsf{max}_a\,|a\rangle = (\mathbf{1} - |a\rangle)|a\rangle = \mathbf{1}|a\rangle - |a\rangle|a\rangle = |a\rangle\mathbf{1} - |a\rangle|a\rangle \leq |a\rangle(\mathbf{1} - |a\rangle) = |a\rangle\,\mathsf{max}_a.$$
(5) The proof is similar to that of (4), but uses the regular identity $aa^* = a^*a$ in the third step.
$$\begin{aligned}\mathsf{max}_a\,|a\rangle^* &= (\mathbf{1} - |a\rangle)|a\rangle^* = \mathbf{1}|a\rangle^* - |a\rangle|a\rangle^* \\ &= |a\rangle^*\mathbf{1} - |a\rangle^*|a\rangle \leq |a\rangle^*(\mathbf{1} - |a\rangle) = |a\rangle^*\,\mathsf{max}_a.\end{aligned}$$
(6) Immediate from (1).
(7) The first claim is immediate from the definitions. Next, $\neg\mathsf{dom}\,a\ a \leq 0$ by (dia1) (set $p = 1$ and $q = \mathsf{dom}\,a = |a\rangle 1$). Finally, by star unfold,
$$ma^* = m(1 + aa^*) = m + maa^* = m + 0a^* = m + 0 = m.$$

(8) This follows from (3), $1 \leq a^*$ and antitony of max. □

Property (7) is used in the discussion of normalisation in Section 9. It means that $\mathsf{max}_a\, 1$ represents the states from which no a-transitions are possible, that is, the normal forms under the transition system represented by a. Lemma 4.5 is useful for proving some standard properties of Noetherian elements.

Lemma 4.6. *Assume a modal semiring S.*

(1) *Zero is the only Noetherian test.*
(2) *If a sum is Noetherian then so are its summands.*
(3) *Noetherity is downward closed.*
(4) *If S is a modal Kleene algebra then an element is Noetherian iff its transitive closure is.*

Proof. Let $a, b \in S$ and $p, q \in \mathsf{test}(S)$.

(1) It follows immediately from Lemma 4.5(2) that 0 is Noetherian.
For the converse direction, let $p \neq 0$. By (2.4) and idempotence of tests we have $|p\rangle p = pp = p$. In particular, $p \leq |p\rangle p$, that is, p is a (post-)fixpoint of $|p\rangle$ different from 0. Hence p is not Noetherian by Corollary 4.3(2).
(2) Immediate from Lemma 4.5(1).
(3) Immediate from (2).
(4) By (3) and $a \leq a^+$, Noetherity of a^+ implies that of a.
Let, conversely, a be Noetherian and assume that $\mathsf{max}_{a^+}\, p \leq 0$. Then, by definition of max, shunting, isotony of $|a^*\rangle$ and the regular identities $a^*a^+ = a^+a^* = aa^*a^* = aa^*$, we obtain

$$\begin{aligned} \mathsf{max}_{a^+}\, p \leq 0 &\Leftrightarrow p - |a^+\rangle p \leq 0 \quad \Leftrightarrow p \leq |a^+\rangle p \\ &\Rightarrow |a^*\rangle p \leq |a^*\rangle|a^+\rangle p \Leftrightarrow |a^*\rangle p \leq |a\rangle|a^*\rangle p, \end{aligned}$$

that is, that $|a\rangle^* p$ is expanded by $|a\rangle$. Hence Noetherity of a implies $|a\rangle^* p \leq 0$ and therefore $p \leq 0$, since $p \leq |a\rangle^* p$. □

Lemma 4.6(1) implies that 1 is not Noetherian. The Noetherian relations $\{(1,2)\}$ and $\{(2,1)\}$ show that the converse direction of Lemma 4.6(2) does not hold; the wellfounded union theorem in Section 10 presents conditions that enforce this converse implication. Lemma 4.6(3) implies that Noetherian elements must be irreflexive. Finally, if a non-trivial test is below an element then this element cannot be Noetherian. In particular, a^* is not Noetherian since $1 \leq a^*$.

5. Termination via Löb's Formula

We now investigate two alternative equational characterisations of termination. The first one involves the transitive closure whereas the second one does not and hence works only for elements with transitive diamonds.

Definition 5.1. An element a of a modal semiring is *diamond-transitive* or *d-transitive* if $|a\rangle|a\rangle \leq |a\rangle$.

Obviously, transitivity implies d-transitivity, but not vice versa. Consider, for instance, the path semiring consisting of sets of node sequences in a graph under union and path concatenation via a common intermediate node (also known as fusion product). In this

case the natural order is set inclusion. Tests are sets of nodes (each represented as a sequence of length one). For such a set p, the forward diamond $|a\rangle p$ yields the inverse image of p under a, that is, the set of all nodes from which an a-path leads to some node of p. Now let n be an arbitrary node and let a consist just of the single path $\langle n, n\rangle$. Then $a \cdot a = \{\langle n, n, n\rangle\} \not\subseteq a$, so that a is not transitive. But

$$|a\rangle p = \begin{cases} \{\langle n\rangle\} & \text{if } \langle n\rangle \in p, \\ \emptyset & \text{otherwise,} \end{cases}$$

so that $|a\rangle|a\rangle \leq |a\rangle$ and a is d-transitive.

Definition 5.2. A modal semiring S is *extensional* if, for all $a, b \in S$,

$$|a\rangle \leq |b\rangle \Rightarrow a \leq b.$$

Equivalently, S is extensional if, for all $a, b \in S$,

$$|a\rangle = |b\rangle \Rightarrow a = b.$$

In an extensional modal semiring, d-transitivity implies transitivity. Obviously, path semirings are not extensional.

We now come to Löb's formula $\Box(\Box p \to p) \to \Box p$ from modal logic (cf. [5]). It expresses wellfoundedness of transitive Kripke frames. To represent this formula algebraically, we first pass to a multi-modal view. We replace $\Box$ by $|a]$ and then dualise the box, by De Morgan's laws, to a form involving diamonds; in particular, the subformula $|a]p \to p$ turns into $p - |a\rangle p = \mathsf{max}_a\, p$. Finally, the main implication is replaced by the natural order on tests. This gives rise to the following notions.

Definition 5.3. An element a of a modal Kleene algebra is

(1) *pre-Löbian* if $|a\rangle \leq |a\rangle^+ \mathsf{max}_a$;
(2) *Löbian* if $|a\rangle \leq |a\rangle\, \mathsf{max}_a$.

When a is pre-Löbian, every state from which there is an a-step into a state set p admits a sequence of a-steps that leads into some a-maximal state of p. Let us see that this implies Noetherity of a. Suppose that a admits an infinite sequence of transitions. Let p represent the set of all states in such a sequence. Then every state in p admits an a-step into p, while $\mathsf{max}_a p = 0$, which is a contradiction. Below we will show that, conversely, also all Noetherian elements are pre-Löbian.

Of course, every Löbian element of a modal Kleene algebra is pre-Löbian. For the converse direction we have the following result.

Lemma 5.4. *A d-transitive element of a modal semiring is Löbian iff it is pre-Löbian.*

Proof. By Proposition 3.7 and standard properties of transitive closure, the diamond of a d-transitive element is its own transitive closure. □

The next statements relate Löbian and Noetherian elements.

Theorem 5.5. *An element of a modal Kleene algebra is Noetherian iff it is pre-Löbian.*

Proof. Consider a modal Kleene algebra S and $a \in S$. Set $f = |a\rangle$ and $g = \mathsf{max}_a = \mathbf{1} - f$. ($\Leftarrow$) Let a be pre-Löbian, which is equivalent to $f - f^+ g \leq \mathbf{0}$. Let $g(p) \leq 0$, that is, $p \leq f(p)$. We must show that $p \leq 0$. We calculate

$$p \leq f(p) = f(p) - f^+(0) = f(p) - f^+(g(p)) \leq 0.$$

The second step uses strictness of diamonds. The third step uses the assumption on g. The fourth step uses the assumption that a is pre-Löbian.
($\Rightarrow$) Let a be Noetherian. This implies that a is pre-Löbian if we can show that $f - f^+g \leq f(f - f^+g)$. We calculate

$$\begin{aligned} f - f^+g &= f - ff^*g \\ &\leq f(\mathbf{1} - f^*g) \\ &= f(\mathbf{1} - (\mathbf{1} + f^+)g) \\ &= f(\mathbf{1} - (g + f^+g)) \\ &= f((\mathbf{1} - g) - f^+g) \\ &\leq f(f - f^+g). \end{aligned}$$

The first step uses the definition of f^+. The second step uses the identity (2.9). The fifth step uses the Boolean identity $p-(q+r) = (p-q)-r$. The last step uses isotony and the fact that $\mathbf{1}-g = \mathbf{1}-(\mathbf{1}-f) \leq f$. This follows from the Boolean identities $p-(p-q) = pq \leq q$. □

Corollary 5.6. *A d-transitive element of a modal semiring is Noetherian iff it is Löbian.*

Proof. This is immediate from Theorem 5.5 and Lemma 5.4. As in that lemma, the required transitive closures exist in the operator semiring by the assumption of d-transitivity. □

Let us discuss the intuition behind the proofs of Theorem 5.5 and Corollary 5.6. If a is pre-Löbian, then $|a\rangle - |a\rangle^+ \mathsf{max}_a \leq \mathbf{0}$. For a given p, the application $(|a\rangle - |a\rangle^+ \mathsf{max}_a)(p)$ of the left-hand side of this identity to a set p denotes the set of all states that admit a-steps leading outside the basin of attraction for termination in p. Now if p had no a-maximal elements then *every* a-step would lead outside the (empty) basin of attraction, unless p itself were empty. The first part of the proof of Theorem 5.5 formalises this argument.

Now let a be Noetherian and assume that the set of states from which a-steps lead outside the basin of attraction is non-empty, that is, a is not pre-Löbian. By Noetherity, this set has an a-maximal element: a contradiction. This motivates the second part of the proof.

The general algebraic connection between Noetherity and Löb's formula is not novel. Goldblatt [15] has given a similar calculational proof in the more general setting of Boolean algebras with operators. In fact, inspection of the proof of Theorem 5.5 shows that no further properties of modal Kleene algebra are needed. Given a strict additive $f : B \to B$ on a Boolean algebra B, Goldblatt defines the transitive closure f^+ of f by the identities

$$f^+(p) = f(p + f^+(p)), \qquad f^+(p) - f(p) \leq f^+(f(p) - p).$$

While the first identity follows immediately from the operator-level unfold law $\mathbf{1}+ff^* = f^*$ and the definition of f^+ in Kleene algebra (Definition 3.4)), the second identity follows from the induction axiom of propositional dynamic logic (3.2) written as $f^* - \mathbf{1} \leq f^*(f - \mathbf{1})$.

A main contribution of this section is to show that Goldblatt's proof can be adapted to Kleene algebra.

The relation between Löb's formula and Noetherity, as expressed in Corollary 5.6, is interesting for the correspondence theory of modal logic. While the traditional proof of the correspondence uses model-theoretic semantic arguments based on infinite chains, the algebraic proof is entirely calculational and avoids infinity. This is quite beneficial for mechanisation.

6. Termination via Absence of Infinite Iteration

Cohen has extended Kleene algebra with an operator for infinite iteration [7] and presented applications of this omega algebra in concurrency control. His approach has been adapted to reasoning about program refinement in [35]. Omega algebra has also been used for proving theorems about rewriting systems that depend on termination [31, 32]. This section compares the notion of Noetherity induced by infinite iteration with the standard one. It turns out that the former can behave in rather undesirable ways. Section 7 presents an alternative approach that still is very similar to omega algebra, but captures the standard notion.

The omega operator is defined, dually to the Kleene star, as a greatest post-fixpoint.

Definition 6.1. An *ω-algebra* is a structure (S, ω) such that S is a Kleene algebra and, for all $a, b, c \in S$, the omega operator ${}^\omega : S \to S$ satisfies the *unfold axiom* and the *co-induction axiom*

$$a^\omega \leq aa^\omega, \qquad c \leq ac + b \Rightarrow c \leq a^\omega + a^*b.$$

Thus, $a^\omega = \nu x.ax$ is a greatest fixpoint; therefore ω is isotone with respect to the natural ordering. The Kleene algebra $\mathrm{REL}(M)$ of relations can be extended to an ω-algebra in the standard way (see, for example, [27]).

The natural notion of termination for ω-algebra is of course absence of infinite iteration.

Definition 6.2. An element a of an ω-algebra is *ω-Noetherian* if $a^\omega \leq 0$.

Like in Section 2 for the Kleene star, it seems interesting to lift the axioms of ω-algebra to the operator level. This is very simple for the unfold axiom. The lifting of the induction axiom of Kleene algebra uses the demodalisation axiom (dia1) to eliminate a diamond from the left-hand side of an identity. In the co-induction axiom of ω-algebra, however, the diamond of interest occurs at a right-hand side and there is no law like demodalisation to handle it. Therefore, the lifting seems to require additional assumptions.

Lemma 6.3. *The diamonds over an extensional modal ω-algebra form an ω-algebra.*

Proof. We show that $|a\rangle^\omega = |a^\omega\rangle$ satisfies the unfold and co-induction axiom of ω-algebra.

For the unfold axiom, $|a\rangle^\omega = |a^\omega\rangle \leq |aa^\omega\rangle = |a\rangle|a^\omega\rangle = |a\rangle|a\rangle^\omega$, by isotony of diamonds.

For the co-induction axiom, assume $|c\rangle \leq |a\rangle|c\rangle + |b\rangle = |ac + b\rangle$, whence $c \leq ac + b$ by extensionality. Then $c \leq a^\omega + a^*b$ follows from the co-induction axiom and therefore $|c\rangle \leq |a^\omega\rangle + |a^*b\rangle = |a\rangle^\omega + |a\rangle^*|b\rangle$ by isotony of diamonds. □

The following lemma compares Noetherity and ω-Noetherity. In particular, it shows that their interrelation does not depend on extensionality of the modal semiring.

Lemma 6.4. *Over modal ω-algebras we have the following results.*

(1) *Noetherian elements are ω-Noetherian.*
(2) *ω-Noetherian elements can, but need not be, Noetherian,*
(3) *not even if extensionality is assumed.*

Proof. (1) Let a be Noetherian. Then $|a^\omega\rangle \leq |a\rangle|a^\omega\rangle$ implies that $|a^\omega\rangle p \leq 0$ for all tests p. Setting $p = 1$ and $q = 0$ in (dia1) shows $a^\omega \leq 0$.

(2) In the ω-algebra $LAN(\Sigma)$ of languages of finite words, $a^\omega = 0$ if $1 \sqcap a \leq 0$, but also $1 = |a\rangle 1$, whenever $a \neq 0$. Thus every a satisfying these conditions is ω-Noetherian, but not Noetherian. Moreover, 0 is ω-Noetherian and Noetherian.

(3) Consider the standard ordering $\leq$ on $\mathbb{N}$ and let S consist of all subrelations of $\leq$ under the usual relational operations. In particular, the identity relation $1 = I_{\mathbb{N}}$ is the multiplicative unit. Since S forms a complete lattice and the defining functions of a^* and a^ω are isotone, the star and omega operators exist for all elements by the Knaster-Tarski theorem, and the structure is an ω-algebra. Also, as a relational structure, it is extensional. Now the successor function σ on $\mathbb{N}$ is an element of S and $\sigma^\omega = \nu x \,.\, \sigma \cdot x$. Thus we must solve the identity $x = \sigma \cdot x$. Obviously, the empty set is the only solution, since every solution of this identity must also be a solution of $x = \sigma^k \cdot x$ for all $k \in \mathbb{N}$. But for each pair $m \leq n$ there is a unique $i \in \mathbb{N}$ such that $(m, n) \in \sigma^i$, so that choosing $k > i$ shows that (m, n) cannot be a member of any solution. Therefore $\sigma^\omega = 0$ and σ is ω-Noetherian.

However, σ is a total function on $\mathbb{N}$ and therefore $|\sigma\rangle 1 = \mathsf{dom}\, \sigma = 1 \neq 0$. Consequently, $\mathsf{max}_\sigma 1 = 1 - |\sigma\rangle 1 = 0$, but $1 \neq 0$, that is, σ is not Noetherian. □

This lemma is a first indication that Noetherity characterises nontermination more precisely than ω-Noetherity. A more thorough discussion is provided in the next section.

7. Termination via Absence of Divergence

We now introduce an alternative view of infinite iteration on a test algebra that handles the problems with ω-algebra. It seems interesting for modelling the dynamics of infinite processes and reactive systems in general.

Definition 7.1. Let S be a modal semiring and $a \in S$.

(1) A test $\nabla a \in \mathsf{test}(S)$ is called the *divergence* of a if it satisfies, for all $a \in S$ and $p \in \mathsf{test}(S)$, the *unfold axiom* and the *co-induction axiom*

$$\nabla a \leq |a\rangle \nabla a, \qquad p \leq |a\rangle p \Rightarrow p \leq \nabla a.$$

(2) When ∇a exists, we call a *convergent* if $\nabla a = 0$ and *divergent* otherwise.
(3) (S, ∇) is a *divergence semiring* (∇-semiring) if ∇a exists for all $a \in S$.
(4) (S, ∇) is a *divergence Kleene algebra* (∇-Kleene algebra) if it is a divergence semiring and S is a Kleene algebra.
(5) (S, ∇) is a *divergence ω-algebra* (∇-ω-algebra) if it is a divergence semiring and S is an ω-algebra.

The above axioms characterise ∇a uniquely as the greatest fixpoint of $|a\rangle$. As a unary operator, ∇ always binds most strongly.

Similar axioms have been used in [15] for defining mono-modal *foundational algebras*.

Since $|a\rangle p = \neg |a] \neg p$, existence of ∇a also implies existence of the least fixpoint $\neg \nabla a$ of $|a]$; this is the *halting predicate* of the modal μ-calculus (cf. [16]) which represents the set of states from which no infinite a-computations emanate. Since this will play a role in later examples, we introduce a separate operator for it.

Definition 7.2. We call the test $\Delta\, a = \neg \nabla a = \mu |a]$ the *convergence* of a.

∇-Kleene algebras behave similarly to ω-algebras.

Lemma 7.3. *Let S be a ∇-Kleene algebra, let $a \in S$ and $p, q \in \mathsf{test}(S)$. The ∇-co-induction axiom is equivalent to*

$$p \leq |a\rangle p + q \Rightarrow p \leq \nabla a + |a^*\rangle q. \tag{7.1}$$

Proof. Assume the co-induction axiom and $p \leq |a\rangle p + q$, that is, that p is expanded by the function $\lambda x.|a\rangle x + q$. By Lemma 4.4(2), $\nu x.|a\rangle x + q = |a^*\rangle q + \nu|a\rangle$, and therefore also $p \leq |a^*\rangle q + \nu|a\rangle = |a^*\rangle q + \nabla a$, as claimed.
Conversely, setting $q = 0$ in (7.1) yields the co-induction axiom. □

The law (7.1) is often more suitable for computations than the co-induction axiom.

Existence of divergences can be guaranteed under additional assumptions.

Lemma 7.4. *Every modal semiring with complete test algebra is a ∇-semiring. Every modal Kleene algebra with complete test algebra is a ∇-Kleene algebra.*

Proof. For every element a of a modal semiring with complete test algebra, $|a\rangle$ is isotone and hence, by the Knaster-Tarski theorem, has a greatest fixpoint that satisfies the axioms of Definition 7.1. The claim about modal Kleene algebras follows from the one about modal semirings and the definitions. □

The co-induction axiom for ∇-semirings comprises Noetherity as a special case.

Lemma 7.5.

(1) *Every Noetherian element of a modal semiring converges.*
(2) *Every convergent element of a ∇-semiring is Noetherian.*

Thus, for Noetherian elements we can do without divergence and hence without the presuppositions for its existence, such as completeness of the test algebra. This is important for our applications in Section 10.

The following statement shows that the situation for ω-Noetherian elements is different; it is a corollary to Lemma 6.4 (the language counterexample) and Lemma 7.5.

Corollary 7.6. *ω-Noetherian elements of divergence ω-algebras may be divergent.*

Therefore divergence, which corresponds to the standard notion of Noetherity, provides a more refined view of termination than ω-Noetherity: the divergence characterises those states from which infinite paths can emanate, while omega iteration tells whether the algebra can represent these infinite paths in some way.

Let us illustrate this with the examples from the proof of Lemma 6.4. In the language semiring $LAN(\Sigma)$ all elements $a \neq 0$ with $a \sqcap 1 = 0$ are non-Noetherian but ω-Noetherian. The distinction vanishes in the encompassing algebra of languages over finite and infinite words, since it explicitly contains the infinite words as limits of iterated compositions of non-empty finite words. In the algebra of relations presented in the proof of Lemma 6.4(3), the successor relation σ on $\mathbb{N}$ was shown to be non-Noetherian but ω-Noetherian. This is caused by the restriction to relations that are subrelations of the standard order $\leq$ on $\mathbb{N}$. The analysis there shows that in a relation a satisfying $a \leq \sigma a$ the inverse image of every number needs to be closed under $\sigma^* = \leq$, which is not possible for subrelations of $\leq$. In the encompassing full relation algebra $\mathrm{REL}(\mathbb{N})$ over $\mathbb{N}$, however, such relations do exist; in particular, there σ^ω is the universal relation.

We now give a sufficient criterion for the coincidence of ω-Noetherity and Noetherity. It uses the fact that in each ω-algebra 1^ω is the greatest element. This follows from setting $a = 1$ and $b = 0$ in the co-induction axiom. We define $\top = 1^\omega$. In particular, $\mathsf{dom}\,\top = 1$ since $\mathsf{dom}\,1 = 1$ and dom is isotone.

Lemma 7.7. *Let S be an ω-algebra.*
(1) $\mathsf{dom}\,a^\omega \leq \nabla a$ *holds for all $a \in S$.*

(2) $\forall a\,.\,a\top = (\mathsf{dom}\,a)\top \Rightarrow \forall a.\nabla a \leq \mathsf{dom}\,a^\omega$, *that is, under this assumption* ω*-Noetherity and Noetherity coincide.*

Proof.

(1) By isotony of diamonds and the unfold law of ω-algebra, $|a^\omega\rangle \leq |a\rangle|a^\omega\rangle$. This matches the antecedent of the ∇-co-induction axiom. The claim then follows by modus ponens.

(2) First note that every test p satisfies

$$\mathsf{dom}(p\top) = \mathsf{dom}(p\,\mathsf{dom}\,\top) = \mathsf{dom}(p1) = \mathsf{dom}\,p = p. \qquad (\dagger)$$

Now, by ∇-unfold and the assumption,

$$\nabla a\top \leq (|a\rangle\nabla a)\top = \mathsf{dom}\,(a\,\nabla a\,)\top = a\,\nabla a\,\top.$$

Therefore $\nabla a\,\top \leq a^\omega$ by ω-coinduction, and the claim follows by ($\dagger$) and isotony of domain. □

The premise $\forall a.a\top = (\mathsf{dom}\,a)\top$ of (2) is equivalent to the explicit domain representation

$$\mathsf{dom}\,a = a\top \sqcap 1,$$

which holds in relation algebras but not in the relational structure defined in the proof of Lemma 6.4(3). The equivalence is shown as follows. Assume $\forall a\,.\,a\top = (\mathsf{dom}\,a)\top$. We use the fact [22] that for $p \in \mathsf{test}(S)$ and arbitrary element b we have $pb = p\top \sqcap b$ (even if the semiring S does not have a general meet operation). Now we obtain

$$a\top \sqcap 1 = (\mathsf{dom}\,a)\top \sqcap 1 = (\mathsf{dom}\,a)1 = \mathsf{dom}\,a.$$

Assume conversely $\mathsf{dom}\,a = a\top \sqcap 1$. Subdistributivity of meet and the fact that $\top$ is the greatest element then yield

$$(\mathsf{dom}\,a)\top = (a\top \sqcap 1)\top \leq a\top\top = a\top.$$

Section 10 provides examples where proofs can faithfully be translated from ω-algebra to ∇-Kleene algebra. And even beyond termination analysis, ∇-Kleene algebras are interesting for modelling infinite behaviour of programs, transition systems and reactive systems. Let us give two examples.

Example 7.8. As mentioned before, the forward box is an algebraic counterpart of the weakest liberal precondition operator wlp that is used in the partial correctness semantics of imperative programs. Algebraically, programs are just state transitions, that is, elements of a (modal) Kleene algebra. The conditional and the while loop are then expressed as (see, for example, [20])

$$\mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b = pa + \neg pb,$$
$$\mathsf{while}\ p\ \mathsf{do}\ a = (pa)^*\neg p,$$

while validity of Hoare triples can be defined by

$$\vdash \{p\}\ a\ \{q\} \Leftrightarrow p \leq |a]q \Leftrightarrow p \leq \mathsf{wlp}(a)(q).$$

This has been used in [24] to give purely algebraic proofs of soundness and relative completeness for the calculus of Hoare triples.

The theory can be extended to total and general correctness by passing to *commands* of the form (a, p) where a is an arbitrary semiring element that models transitions and p is a test that represents the states from which termination is guaranteed (see, for example, [26]

for an approach based on predicate logic). Then the weakest precondition operator wp can be defined as

$$\mathsf{wp}(a,p)(q) = p \cdot \mathsf{wlp}(a)(q).$$

In [25] it has been shown that the set of commands can be made into another modal semiring in which the forward box expresses the wp operator. It turns out that the above-mentioned soundness and completeness proofs apply to the algebra of commands as well and yield a sound and relatively complete Hoare calculus for total correctness. Its rule for the do-od loop, a generalisation of the while loop, reads, for command k and test p,

$$\frac{\{p\}\ k\ \{p\}}{\{\Delta\, k \cdot p\}\ \mathsf{do}\, k\, \mathsf{od}\ \{p \cdot \neg \mathsf{grd}\, k\}}$$

where $\mathsf{grd}\, k$, the *guard* of k, coincides with $\mathsf{dom}\, k$ (which is determined by the a component of k) and the convergence $\Delta\, k$ from Definition 7.2 represents the set of states from where iteration of k cannot lead to an infinite computation. For details we refer to [25]. □

Example 7.9. In [23], the class of Boolean quantales, which can conservatively be extended into modal ω and ∇-algebras by the explicit definitions $a^\omega = \nu x\,.\,ax$ and $\nabla a = \nu p\,.\,|a\rangle p$, has been used to give algebraic semantics for the temporal logics $\mathsf{CTL}, \mathsf{CTL}^*$ and LTL. The starting point is a straightforward translation of the standard semantics of CTL^* in terms of states and computation paths into algebraic terms. Again, tests represent sets of states while semiring elements now represent sets of paths. Every CTL^* formula φ is then interpreted by a semiring element $[\![\varphi]\!]$. A simplified semantics for the sublogic CTL is obtained as follows. Structural induction shows that for every CTL formula φ the CTL^* semantics has the form $[\![\varphi]\!] = p\top$ for some test p. This algebraically reflects the fact that CTL formulas are state formulas corresponding to sets of states rather than sets of paths; the element $p\top$ represents the set of all paths that start in the set p. The simplified semantics is then extracted by setting $[\![\varphi]\!]_d = \mathsf{dom}\,[\![\varphi]\!]$; this returns a test, that is, an abstract representation of a set of states. The algebraic background is that $\mathsf{dom}\,(p\top) = p$ for a test p. Now the convergence operator enters the play, since it turns out that the always-finally operator has the simplified semantics

$$[\![\mathsf{AF}\varphi]\!]_d = \Delta\,(\neg p \cdot a),$$

where $p = [\![\varphi]\!]_d$, and a is the element that generates the computation paths; it can be thought of as a set of paths of length two that corresponds to a transition relation. For details we refer to [23]. □

8. Basic Divergence Calculus

The unfold and co-induction axioms of ∇-Kleene algebras lead to properties that are analogous to those of ω-algebras. However, because of the different axiomatisations, we cannot transfer them without proof. Here we collect only some properties that are needed in a later section.

Lemma 8.1. *Let S be a ∇-Kleene algebra and let $a, b \in S$.*

(1) $\nabla 0 = 0$ *and* $\nabla 1 = 1$,
(2) $\nabla a = |a\rangle \nabla a$,
(3) $\nabla a = |a\rangle^* \nabla a$,
(4) $a \leq b \Rightarrow \nabla a \leq \nabla b$,

(5) $\nabla a = \nabla(a^+)$,
(6) $\nabla(a+b) = \nabla(a^*b) + |a^*b\rangle^* \nabla a$,
(7) $|b^*\rangle(\nabla(b^*a)) = \nabla(b^*a)$.

Proof.

(1) The first property follows by ∇-unfold, the second one by ∇-co-induction.
(2) ($\leq$) is just the unfold axiom. ($\geq$) reduces, by co-induction, to $|a\rangle\nabla a \leq |a\rangle|a\rangle\nabla a$, which follows from the unfold axiom and isotony.
(3) ($\leq$) follows from the regular identity $1 \leq a^*$ and isotony. ($\geq$) reduces, by the unfold axiom, to $|a^*\rangle\nabla a \leq |a\rangle|a^*\rangle\nabla a$. But $|a^*\rangle\nabla a = |a^*\rangle|a\rangle\nabla a = |a\rangle|a^*\rangle\nabla a$ holds by (2) and the regular identity $aa^* = a^*a$.
(4) Let $a \leq b$. For $\nabla a \leq \nabla b$ it suffices, by co-induction, to show that $\nabla a \leq |b\rangle\nabla a$. But $\nabla a \leq |a\rangle\nabla a \leq |b\rangle\nabla a$ holds by unfold and isotony.
(5) ($\leq$) follows from isotony of ∇ (4) and the regular identity $a \leq a^+$. ($\geq$) reduces, by co-induction, to $\nabla(a^+) \leq |a\rangle\nabla(a^+)$. We calculate

$$\nabla(a^+) \leq |a^+\rangle\nabla(a^+) = |a\rangle|a^*\rangle\nabla(a^+) = |a\rangle|(a^+)^*\rangle\nabla(a^+) = |a\rangle\nabla(a^+).$$

The third step follows by the regular identity $a^* = (a^+)^*$. The last step uses (3).
(6) ($\leq$) reduces, by co-induction (variant (7.1)), to

$$\nabla(a+b) \leq \nabla a + |a^*b\rangle\nabla(a+b) = \nabla a + |a^*\rangle(|b\rangle\nabla(a+b)),$$

which, again by co-induction (7.1), reduces to

$$\nabla(a+b) \leq |a\rangle\nabla(a+b) + |b\rangle\nabla(a+b) = |a+b\rangle\nabla(a+b).$$

But this holds by the unfold axiom.
($\geq$) We calculate

$$\begin{aligned}\nabla(a^*b) + |(a^*b)\rangle^*\nabla a &= \nabla(a^*b) + |(a^*b)^*\rangle\nabla a \\ &\leq \nabla((a+b)^+) + |(a+b)^*\rangle\nabla(a+b) \\ &= \nabla(a+b) + \nabla(a+b) \\ &= \nabla(a+b).\end{aligned}$$

The first step follows from the regular identities $a^*b \leq (a+b)^+$ and $(a^*b)^* \leq (a+b)^*$ and isotony. The second step follows from (5) and (3).
(7) We calculate

$$\nabla(b^*a) = |b^*a\rangle\nabla(b^*a) = |b^*\rangle|b^*a\rangle\nabla(b^*a) = |b^*\rangle\nabla(b^*a).$$

The first and last steps use (2). The second step uses the regular identity $b^*b^* = b^*$. □

9. Termination via Normalisation

After this introduction to the divergence calculus, we now resume the connection between semiring elements and transition systems. Remember from Lemma 4.5(7) that, for transition system a, the test $\mathsf{max}_a 1 = \neg\mathsf{dom}\, a$ can be viewed as an abstract representation of the *normal forms* with respect to a-transitions, that is, the states from which no (further) a-transitions are possible. The process of normalisation, that is, repeated a-transitions until a normal form has been reached (if there is one) is then described by the following notion.

Definition 9.1. The *normaliser* of an element a of a modal Kleene algebra is

$$\mathsf{nml}\, a = a^* \,(\mathsf{max}_a\, 1) = a^* \,\neg\mathsf{dom}\, a.$$

In the relation semiring, $\mathsf{nml}\, a$ relates every element to the set of its normal forms under iterated a-transitions (if any). From the definition we immediately obtain the following special cases.

Corollary 9.2. $\mathsf{nml}\, 0 = 1$ *and* $\mathsf{dom}\, a = 1 \Rightarrow \mathsf{nml}\, a = 0$.

The first of these expressions means that if there are no transitions, then every state is a normal form, but one that is related only to itself. The second one means that a total transition element has no normal forms at all, and hence no element can be related to a normal form.

Another property is that normalisers are multiplicatively idempotent.

Lemma 9.3. $(\mathsf{nml}\, a)(\mathsf{nml}\, a) = \mathsf{nml}\, a$.

Proof. We calculate, using Lemma 4.5(7) and the multiplicative idempotence of tests,

$$a^* \,(\mathsf{max}_a\, 1)\; a^* \,(\mathsf{max}_a\, 1) = a^* \,(\mathsf{max}_a\, 1)\,(\mathsf{max}_a\, 1) = a^* \,(\mathsf{max}_a\, 1).$$ □

Next, Noetherity implies that normal forms exist for all domain elements.

Lemma 9.4. *For every Noetherian element a of a modal Kleene algebra,* $\mathsf{dom}\,\mathsf{nml}\, a = 1$.

Proof. By Theorem 5.5 a is pre-Löbian. Now we calculate, using that by definition always $\mathsf{dom}\, a \leq 1$, and setting $m = \mathsf{max}_a\, 1 = \neg\mathsf{dom}\, a$,

$$\begin{aligned}\mathsf{dom}\,\mathsf{nml}\; a &= \mathsf{dom}(a^* m) = |a^*\rangle m = |1 + a^+\rangle m = m + |a^+\rangle(\mathsf{max}_a\, 1)\\ &\geq m + |a\rangle 1 = \neg\mathsf{dom}\, a + \mathsf{dom}\, a = 1.\end{aligned}$$

The decisive step is the inequality; it uses the defining property of pre-Löbian elements from Definition 5.3(1). □

The converse of this statement does not hold.

Example 9.5. Consider the relation semiring over a two-element set $\{A, B\}$ and let $a = \{(A, A), (A, B)\}$. Then $\mathsf{nml}\; a = \{(A, B), (B, B)\}$ and $\mathsf{dom}\,\mathsf{nml}\; a = \{(A, A), (B, B)\} = 1$. But $\{(A, A)\} \subseteq a$ is not Noetherian and therefore, by Lemma 4.6(3), neither is a. □

The following example relates normalisation and ω-Noetherity.

Example 9.6. The algebra $\mathrm{LAN}(\Sigma)$ of formal languages is both an ω-algebra and a modal Kleene algebra with test set $\{0, 1\}$. We have already shown that $|a\rangle 1 = \mathsf{dom}\, a = 1 \neq 0$ when $a \neq 0$. Hence an element a is Noetherian iff $a = 0$. Moreover, distinguishing the cases $a = 0$ and $a \neq 0$, Corollary 9.2 shows that $\mathsf{nml}\, a = \neg\mathsf{dom}\, a = \mathsf{max}_a\, 1$ (and hence also $\mathsf{dom}\,\mathsf{nml}\, a = \neg\mathsf{dom}\, a$). This expresses the fact that, by totality of concatenation, a non-empty language can be iterated indefinitely without reaching a normal form. But we also have $a^\omega = 0$ whenever $1 \sqcap a = 0$. Therefore, $a^\omega = 0$ does not imply that $\mathsf{dom}\,\mathsf{nml}\, a = 1$, while $\nabla a = 0$ still implies this fact. □

Again, this shows that ω-algebra models nontermination less finely than the notions of Noetherity or divergence.

10. Additivity of Termination

We now turn to transition systems induced by term rewriting or reduction rules. Abstract reduction is that part of rewriting theory that disregards the term structure. It is essentially relational. Many statements of abstract reduction that depend on termination can be proved in ω-algebra [31, 32], among them a variant of the wellfounded union theorem of Bachmair and Dershowitz [2]. Since we have seen that termination is characterised in ω-algebra less sharply than in ∇-Kleene algebra, it is interesting and important to reconsider that proof. We will see that our new proofs again yield precise reconstructions of the standard diagrammatic argument. Thus modal Kleene algebra also admits an algebraic semantics for abstract reduction systems.

The connection between Kleene algebra and rewriting is as follows. An *abstract reduction system* (cf. [34]) is simply a set endowed with a family of binary relations. The operations on relations considered in rewriting are composition, union, conversion and symmetric, transitive and reflexive transitive closure. Therefore, properties of abstract rewrite systems can be expressed in modal Kleene algebra (conversion is obtained via the backward modal operators).

Definition 10.1. Let S be a Kleene algebra and let $a, b \in S$.
(1) *a locally semi-commutes* over b if $ba \leq a^+b^*$.
(2) *a semi-commutes* over b if $b^*a \leq a^+b^*$.
(3) *a quasi-commutes* over b if $ba \leq a(a+b)^*$.

Semi-commutation and quasi-commutation state conditions for shifting certain steps to the left of others. In general, sequences of a-steps and b-steps can be split into a "good" part with all a-steps occurring to the left of b-steps and into a "bad" part in which both kinds of steps are mixed.

For working with ∇-Kleene algebras, we lift these properties to the operator level. As in Section 5 for transitivity, we introduce notions of diamond-commutation.

Definition 10.2. We say that *a locally d-semi-commutes* over b if $|b\rangle|a\rangle \leq |a\rangle^+|b\rangle^*$, and likewise for the other notions.

Again, the d-commutation properties are more general than the respective commutation properties; they are equivalent when the modal Kleene algebra is extensional. To avoid extensionality we will henceforth base our statements and proofs on d-commutation.

But first, we mention two auxiliary properties used to relate semi-commutation and quasi-commutation. The first one has been shown in [32], the second one lifts corresponding properties in [19].

Lemma 10.3.
(1) *For all elements a and b of a Kleene algebra,*

$$(a+b)^* = a^*b^* + a^*b^+a(a+b)^*. \tag{10.1}$$

(2) *For all a, b and c of a modal Kleene algebra,*

$$|ba\rangle \leq |ac\rangle \Rightarrow |b\rangle^*|a\rangle \leq |a\rangle|c\rangle^*, \qquad |ba\rangle \leq |ac\rangle \Rightarrow |b\rangle^+|a\rangle \leq |a\rangle|c\rangle^+. \tag{10.2}$$

The following lemma relates semi-commutation and quasi-commutation. A proof in ω-algebra has been given in [32]. Here, we show that it translates to modal Kleene algebra. Remember that, by Lemma 7.5(1), we can freely use the calculus of ∇-Kleene algebra for Noetherian elements already in modal Kleene algebra.

Lemma 10.4. *Let S be a modal Kleene algebra and let $a, b \in S$ with a Noetherian. The following properties are equivalent.*

(1) *a locally d-semi-commutes over b.*
(2) *a d-semi-commutes over b.*
(3) *a d-quasi-commutes over b.*

Proof. We only show equivalence between local semi-commutation and quasi-commutation. The proof for semi-commutation is similar. We set $f = |a\rangle$ and $g = |b\rangle$.

Let a locally d-semi-commute over b. By pure Kleene algebra and without any Noetherity assumptions, $gf \leq f^+g^* = ff^*g^* \leq f(f+g)^*$.

Let now a d-quasi-commute over b. First, as in [32], we show that $h = f(f+g)^*$ satisfies $h \leq f^+(g^* + h)$:

$$\begin{array}{rcll} f(f+g)^* & = & f(f^*g^* + f^*g^+f(f+g)^*) & \text{by (10.1)} \\ & = & f^+(g^* + g^+f(f+g)^*) & \text{distributivity and def. } f^+ \\ & \leq & f^+(g^* + f(f+g)^{*+}(f+g)^*) & \text{by assumed d-quasi-commutation and (10.2)} \\ & \leq & f^+(g^* + f(f+g)^*) & \text{regular identity } c^{*+}c^* \leq c^*. \end{array}$$

The above identity written point-wise means that, for all $p \in \mathsf{test}(S)$,

$$h(p) \leq f^+(h(p)) + f^+(g^*(p)).$$

Modulo $|a\rangle^+ = |a^+\rangle$, this matches the left-hand side of the co-induction rule (7.1) of ∇-Kleene algebra for $\nabla(a^+)$. Since a is Noetherian, so is a^+ by Lemma 4.6(4). Therefore $\nabla(a^+)$ exists by Lemma 7.5(1), namely $\nabla(a^+) = 0$. Hence

$$g(f(p)) \leq h(p) \leq \nabla(a^+) + (f^+)^*(f^+(g^*(p))) = f^+(g^*(p)),$$

as required, where the first step uses the assumption of d-quasi-commutation. □

The proof of Lemma 10.4 simulates a previous one in ω-algebra. In [32] it has been argued that the latter formally reconstructs the previous diagrammatic proof from [30]. Therefore the new proof shares this property. However, our other formal notions of Noetherity provide the flexibility to use different techniques, when necessary. An alternative proof that uses Noetherity directly is given in [9].

Lemma 10.5. *Let S be a divergence Kleene algebra. Let $a, b \in S$ and let a d-quasi-commute over b. Then Noetherity of a implies Noetherity of b^*a.*

Proof. From Lemma 7.5(1) we know that Noetherity of a implies convergence of a. We now show that convergence of a implies convergence of b^*a. Suppose $\nabla a \leq 0$. From the quasi-commutation assumption and Lemma 10.4 we infer $|b^*a\rangle \leq |a^+b^*\rangle$. Therefore, by Lemma 8.1(2) and Lemma 8.1(7),

$$\nabla(b^*a) = |b^*a\rangle\nabla(b^*a) \leq |a^+b^*\rangle\nabla(b^*a) = |a^+\rangle\nabla(b^*a).$$

Now $\nabla(b^*a) \leq |a^+\rangle\nabla(b^*a)$ implies $\nabla(b^*a) \leq \nabla(a^+)$ by co-induction, from which the claim $\nabla(b^*a) \leq 0$ follows by Lemma 8.1(5) and Noetherity of a. By Lemma 7.5(2) convergence of b^*a implies Noetherity of b^*a and we are done. □

Lemma 10.5 generalises Lemma 2 of [2]. Again, its proof simulates an earlier calculation in ω-algebra and directly corresponds to a diagrammatic proof [13, 32].

We now generalise the quasi-commutation theorem of Bachmair and Dershowitz (Theorem 1 of [2]).

Theorem 10.6. *Let S be a divergence Kleene algebra. Let $a, b \in S$ be such that a d-quasi-commutes over b. Then $a + b$ is Noetherian iff a and b are Noetherian:*

$$\nabla(a + b) \leq 0 \Leftrightarrow \nabla a + \nabla b \leq 0.$$

Proof. By Lemma 4.6(2), Noetherity of a sum is inherited by its summands. So it remains to show the converse direction. Let $\nabla a + \nabla b \leq 0$. First, denesting $\nabla(a+b)$ using Lemma 8.1(6) yields

$$\nabla(a + b) = \nabla(b^* a) + |b^* a\rangle^* \nabla b.$$

Now $\nabla(b^* a)$ vanishes by Lemma 10.5, using the assumption of d-quasi-commutation and Noetherity of a, and $|b^* a\rangle^* \nabla b$ vanishes by Noetherity of b and strictness of diamonds. Thus also $\nabla(a + b) \leq 0$. □

These results show that proofs for abstract reduction systems in modal Kleene algebra are as simple as those in ω-algebra. The original proofs in [2] are rather informal, while also previous diagrammatic proofs (see, for example, [30]) suppress many steps. Contrarily, the algebraic proofs are complete, formal and still simple. An extensive discussion of the relationship between the proofs in ω-algebra and their diagrammatic counterparts can be found in [13, 32]. In particular, the algebraic proofs mirror precisely the diagrammatic ones and follow essentially the line of reasoning from [2]. While this also holds for the modal proofs, it is not true for a relational proof of a similar, but somewhat more general theorem in [12] that uses the weaker condition $ba \leq a(a + b)^* + b$ instead of quasi-commutation. ω-algebra has been used for proving further statements from concurrency control [7] and abstract rewriting [32] in a simple calculational way. We conjecture that they all translate to modal Kleene algebra.

11. Newman's Lemma

We now turn from quasi-commutation and semi-commutation to commutation and confluence. In rewriting theory, the generalisation from confluence to commutation has led to a theory of term rewriting for non-symmetric transitive relations and pre-congruences that comprises the traditional equational case [29, 30]. In particular, it introduces commutation-based variants of Church-Rosser theorems and of Newman's lemma. While the former can be proved in plain Kleene algebra [31, 32], it has been conjectured in [32] that a proof of Newman's lemma in pure ω-algebra is impossible; that approach seems to cover only the regular fragment of abstract reduction, i.e, working at one end of a derivation expression, whereas proofs of Newman's lemma seem to require a context-free setting, since they also have to work in the interior of such expressions.

We reconstruct a previous diagrammatic proof of a variant of Newman's lemma for non-symmetric rewriting in modal Kleene algebra. Independently, the same statement has been obtained by purely syntactic considerations in [12]. There, it has been proven in a relation algebra without complementation that is more expressive than the algebras considered here. A relation-algebraic proof of the equational variant of Newman's lemma (cf. [34]) has been given in [27]. This proof, however, depends on normal forms which are not present in the

non-symmetric case. In general, the results from [29, 30] show that confluence properties should be conceptually separated from such normal forms.

A straightforward relational specification of commutation and confluence requires the operation of relational conversion, which is not present in Kleene algebra. In [12], residuals (or factors) are used as a restricted form of conversion. We simulate conversion in modal Kleene algebra by semiring opposition, that is, by switching between forward and backward modal operators.

Definition 11.1. Let S be a modal Kleene algebra and let $a, b \in S$.

(1) a and b *d-commute* if $\langle b^* || a^* \rangle \leq |a^*\rangle\langle b^*|$.
(2) a and b *locally d-commute* if $\langle b || a \rangle \leq |a^*\rangle\langle b^*|$.
(3) An element is *(locally) d-confluent* if it (locally) d-commutes with itself.

As with transitivity and semi-commutation, the d-variants are strictly more general than the "classical" diamond-free ones (for example, in a semiring with a converse operation $^\smile$ such as the relation semiring, that a and b commute iff $(b^\smile)^* a^* \leq a^* (b^\smile)^*$).

Alternatively, if forward and backward modal operators are not both available, commutation can be expressed by an algebraic variant of the Geach formula $|b\rangle|d] \leq |a]|c\rangle$ from modal logic (cf. [6]). The equivalences

$$|b\rangle|d] \leq |a]|c\rangle \Leftrightarrow \langle a||b\rangle|d] \leq |c\rangle \Leftrightarrow \langle a||b\rangle \leq |c\rangle\langle d|$$

follow from the Galois and co-Galois connections.

We now prove the following variant of Newman's lemma.

Theorem 11.2. *Let S be a modal Kleene algebra with complete test algebra. If $a + b$ is Noetherian and a and b locally d-commute then a and b d-commute.*

Proof. We use $dc(p, a, b)$ to express that two elements a and b d-commute when restricted to a set p of starting states:

$$dc(p, a, b) \Leftrightarrow \langle b^* | \langle p \rangle | a^* \rangle \leq |a^*\rangle\langle b^*|.$$

The notation $\langle p \rangle$ indicates that, since p is a test, it does not matter whether we use the forward or backward diamond. Then a and b d-commute iff $dc(1, a, b)$ holds. By isotony of diamonds, dc is downward closed in its first argument, that is, $dc(p, a, b)$ and $q \leq p$ imply $dc(q, a, b)$. Moreover, by completeness of the test algebra,

$$r = \mathsf{sup}\,\{p : dc(p, a, b)\}$$

exists. It represents the set of all states on which a and b d-commute. In particular, r itself satisfies $dc(r, a, b)$. This holds since diamonds and, by (2.1), also meets in a Boolean algebra are completely additive.

Together with downward closure of dc this implies that

$$p \leq r \Leftrightarrow dc(p, a, b). \tag{11.1}$$

We use the dual variant $|a + b]q \leq q \Rightarrow 1 \leq q$ of Noetherity of $a + b$ to show that $r = 1$, which, by the above remark, establishes d-commutation.

To obtain a suitable sufficient condition, we calculate

$$\begin{array}{lll} |a+b]r \leq r & \Leftrightarrow \forall p.(p \leq |a+b]r \Rightarrow p \leq r) & \text{order theory} \\ & \Leftrightarrow \forall p.(\langle a+b|p \leq r \Rightarrow p \leq r) & \text{Galois connection (2.2)} \\ & \Leftrightarrow \forall p.(\langle a|p \leq r \wedge \langle b|p \leq r \Rightarrow p \leq r) & \text{additivity of diamonds} \\ & & \quad \text{and Boolean algebra} \\ & \Leftrightarrow \forall p.(dc(p_a,a,b) \wedge dc(p_b,a,b) \Rightarrow dc(p,a,b)) & \text{by (11.1),} \end{array}$$

where, for $x \in \{a,b\}$, p_x abbreviates $\langle x|p = \mathsf{cod}(px)$.

So, assuming $dc(p_a,a,b) \wedge dc(p_b,a,b)$, we must now show $dc(p,a,b)$. By the star unfold law and distributivities,

$$\langle b^*|\langle p\rangle|a^*\rangle \leq \langle b^*|\langle p\rangle + \langle b^*|\langle b|\langle p\rangle|a\rangle|a^*\rangle + \langle p\rangle|a^*\rangle.$$

The outer two of these summands are below $|a^*\rangle\langle b^*|$ by isotony of diamonds and Kleene algebra. For the middle summand we first show

$$\langle p\rangle|a\rangle \leq |a\rangle\langle p_a\rangle, \qquad \langle b|\langle p\rangle \leq \langle p_b\rangle\langle b|. \tag{11.2}$$

For the left identity, we calculate

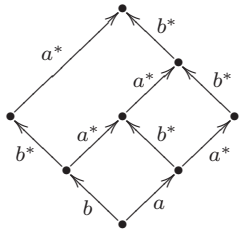
$$\langle p\rangle|a\rangle = |pa\rangle = |pa\ \mathsf{cod}(pa)\rangle \leq |a\ \mathsf{cod}(pa)\rangle = |a\rangle\langle p_a\rangle.$$

The proof of the right identity is dual.

Now the main claim is shown by the following calculation.

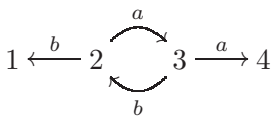
$$\begin{array}{lll} \langle b^*|\langle b|\langle p\rangle|a\rangle|a^*\rangle & \leq \langle b^*|\langle p_b\rangle\langle b||a\rangle\langle p_a\rangle|a^*\rangle & \text{idempotence of } \langle p\rangle\text{, (11.2) twice} \\ & & \quad \text{and isotony of diamonds} \\ & \leq \langle b^*|\langle p_b\rangle|a^*\rangle\langle b^*|\langle p_a\rangle|a^*\rangle & \text{local d-commutation of } a \text{ and } b \\ & \leq \langle b^*|\langle p_b\rangle|a^*\rangle|a^*\rangle\langle b^*| & \text{assumption } dc(p_a,a,b) \\ & \leq \langle b^*|\langle p_b\rangle|a^*\rangle\langle b^*| & \text{regular identity } c^*c^* = c^* \\ & & \quad \text{lifted to diamonds} \\ & \leq |a^*\rangle\langle b^*|\langle b^*| & \text{assumption } dc(p_b,a,b) \\ & \leq |a^*\rangle\langle b^*| & \text{above regular identity again.} \end{array}$$ □

The last calculation in the proof can be visualised by the following diagram in which the bottom point is in p and the two points in the next higher layer are in p_b and p_a, respectively.



We conclude by noting that the assumption of Noetherity of $a+b$ cannot be weakened to separate Noetherity of a and b.

Example 11.3 ([29])**.** Consider the following relations a and b.



Relations a and b locally commute:

– $\langle b||a\rangle\{1\} = \langle b|a\rangle\{2\} = \emptyset$.
– $\langle b||a\rangle\{3\} = \{1\} \leq \{1,2,3\} = |a\rangle^*\langle b|^*\{3\}$.
– $\langle b||a\rangle\{4\} = \{2\} \leq \{2,3,4\} = |a\rangle^*\langle b|^*\{4\}$.
– The remaining cases follow from the atomic ones by additivity.

However, a and b do not commute, even though both are (separately) Noetherian:

– $\langle b||a\rangle|a\rangle\{4\} = \{1\} \not\leq \{2,3,4\} = |a\rangle^*\langle b|^*\{4\}$.

$a + b$ is not Noetherian: An infinite $a + b$-chain alternates between 2 and 3. □

12. Confluence and Unique Normal Forms

From the relational setting it is well known that confluence implies uniqueness of normal forms. This means that there the normaliser $\mathsf{nml}\, a = a^* (\mathsf{max}_a\, 1)$ (cf. Section 9) is a (partial) function, that is, a deterministic relation. A relation a is a partial function iff $a^\smile a \leq 1$ [27]. Again, this property can be abstracted to the level of modal operators.

Definition 12.1. An element a of a modal semiring is *d-deterministic* if

$$\langle a||a\rangle \leq \mathbf{1},$$

or, equivalently, if $|a\rangle \leq |a]$.

Of course, d-determinism is a special case of local d-confluence or d-commutation. It is immediate from the definition that every test is d-deterministic. The analogue to the above-mentioned relational property can be stated as follows.

Lemma 12.2. *The normaliser of a d-confluent element of a modal Kleene algebra is d-deterministic.*

Proof. Set $m = \mathsf{max}_a\, 1 = \neg\mathsf{dom}\, a$. First, note that by (2.4) $|p\rangle q = \langle p|q = pq \leq q$ for all tests p, q and hence

$$|p\rangle = \langle p| \leq \mathbf{1}. \tag{†}$$

Then we calculate as follows.

$$\begin{aligned}
\langle \mathsf{nml}\, a||\mathsf{nml}\, a\rangle &= \langle a^*m||a^*m\rangle && \text{def. } \mathsf{nml}\\
&= \langle m|\langle a^*||a^*\rangle|m\rangle && \text{by (dia2')}\\
&\leq \langle m||a^*\rangle\langle a^*||m\rangle && \text{confluence of } a\\
&= |m\rangle|a^*\rangle\langle a^*|\langle m| && \text{by (†)}\\
&= |ma^*\rangle\langle ma^*| && \text{by (dia2')}\\
&= |m\rangle\langle m| && \text{Lemma 4.5(7)}\\
&\leq \mathbf{1} && \text{by (†).}
\end{aligned}$$

□

This statement is independent of termination properties. It has been added to further demonstrate the applicability of modal Kleene algebra in rewriting theory.

Example 12.3. The relation a from Example 9.5 is confluent but not Noetherian and has the unique normal form B. The normaliser of a is deterministic, as stated in Lemma 12.2. □

13. Conclusion

We have shown that modal semirings, modal Kleene algebras and divergence Kleene algebras are versatile tools for termination analysis, introducing and comparing different notions of termination and applying our techniques to examples from rewriting theory. All proofs are abstract, concise and calculational. A particular result of our analysis is a critique of an earlier approach to termination based on omega algebra. Together with previous work [31, 32], our case studies on rewriting, more precisely, on abstract reduction systems, show that parts of this theory can be reconstructed in modal Kleene algebra and divergence Kleene algebra. Due to its simplicity, the approach has considerable potential for mechanisation and automation. There are strong connections to automata-based decision procedures [24].

The proof of Newman's lemma and the associated diagram show that modal Kleene algebra allows induction in the interior part of an expression. This is not possible in pure Kleene algebra or omega algebra due to the shape of the star induction and omega coinduction axioms. Thus modal Kleene algebra supports "context-free" induction, whereas pure Kleene or omega algebra admits only its "regular" subcase. To achieve the same purpose, residuals are used in [12] to move the locus of induction from the interior of an expression to one of its ends and back.

The results of the present paper contribute to establishing modal Kleene algebra as a formalism that enhances cross-theory reasoning between different calculi for program analysis. Moreover, our techniques have successfully been mechanised using off-the-shelf first-order automatic theorem provers. Case studies on this can be found, for instance, in [17]. Therefore the integration into formal methods like Alloy [18], B [1] or Z [28], and applications to the analysis of programs, protocols and reactive systems are within reach. We envision three lines for future research:

- the investigation of discrete dynamical systems based on modal semirings, convergence and divergence;
- the study of the free algebras and the development of decision procedures in this setting, based on those for Kleene algebras without modalities;
- the application of the approach in the termination analysis of programs and the development of tools that support this analysis.

Acknowledgements

The authors would like to thank Roland Backhouse, Ernie Cohen, Roland Glück, Peter Höfner, Gunther Schmidt and Kim Solin for inspiring discussions and the anonymous referees of the IFIP-TCS 2004 conference and of LMCS for helpful comments on earlier versions.

References

[1] J.-R. Abrial. *The B-Book*. Cambridge University Press, 1996.
[2] L. Bachmair and N. Dershowitz. Commutation, transformation, and termination. In J. H. Siekmann, editor, *8th International Conference on Automated Deduction*, volume 230 of *Lecture Notes in Computer Science*, pages 5–20. Springer, 1986.
[3] R. Backhouse. Galois connections and fixed point calculus. In R. Backhouse, R. Crole, and J. Gibbons, editors, *Algebraic and Coalgebraic Methods in the Mathematics of Program Construction*, volume 2297 of *Lecture Notes in Computer Science*, pages 89–148. Springer, 2002.
[4] R. Backhouse et al. Fixed point calculus. *Information Processing Letters*, 53:31–136, 1995.
[5] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, 2001.

[6] B. F. Chellas. *Modal Logic: An Introduction*. Cambridge University Press, 1980.
[7] E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *5th International Conference on Mathematics of Program Construction, MPC 2000*, volume 1837 of *Lecture Notes in Computer Science*, pages 45–59. Springer, 2000.
[8] J. Desharnais, B. Möller, and G. Struth. Modal Kleene algebra and applications—a survey. *Journal on Relational Methods in Computer Science*, 1:93–131, 2004.
[9] J. Desharnais, B. Möller, and G. Struth. Termination in modal Kleene algebra. In J.-J. Levy, E. W. Mayr, and J. C. Mitchell, editors, *3rd International Conference on Theoretical Computer Science*, pages 647–660. Kluwer, 2004.
[10] J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM Transactions on Computational Logic*, 7:798–833, 2006.
[11] E.W. Dijkstra. *A Discipline of Programming*. Prentice Hall, 1976.
[12] H. Doornbos, R. C. Backhouse, and J. van der Woude. A calculational approach to mathematical induction. *Theoretical Computer Science*, 179:103–135, 1997.
[13] M. Ebert and G. Struth. Diagram chase in relational system development. In M. Minas, editor, *3rd IEEE workshop on Visual Languages and Formal Methods (VLFM'04)*, volume 127 of *Electronic Notes in Theoretical Computer Science*, pages 87–105. Elsevier, 2005.
[14] T. Ehm, B. Möller, and G. Struth. Kleene modules. In R. Berghammer, B. Möller, and G. Struth, editors, *Relational and Kleene-Algebraic Methods in Computer Science: 7th International Seminar on Relational Methods in Computer Science and 2nd International Workshop on Applications of Kleene Algebra, Bad Malente, Germany, May 12-17, 2003, Revised Selected Papers*, volume 3051 of *Lecture Notes in Computer Science*, pages 112–124. Springer, 2004.
[15] R. Goldblatt. An algebraic study of well-foundedness. *Studia Logica*, 44(4):422–437, 1985.
[16] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.
[17] P. Höfner and G. Struth. Automated reasoning in Kleene algebra. In F. Pfenning, editor, *CADE 2007*, volume 4603 of *Lecture Notes in Artificial Intelligence*, pages 279–294. Springer, 2007.
[18] D. Jackson. *Software Abstractions*. The MIT Press, 2006.
[19] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.
[20] D. Kozen. Kleene algebra with tests. *ACM Transactions on Programming Languages and Systems*, 19(3):427–443, 1997.
[21] A. Melton, D.A. Schmidt, and G.E. Strecker. Galois connections and computer science applications. In D. Pitt, S. Abramsky, A. Poigné, and D. Rydeheard, editors, *Category Theory and Computer Programming*, volume 240 of *Lecture Notes in Computer Science*, pages 299–312. Springer, 1986.
[22] B. Möller. Lazy Kleene algebra. In D. Kozen, editor, *Mathematics of Program Construction*, volume 3125 of *Lecture Notes in Computer Science*, pages 252–273. Springer, 2004. Revised version: B. Möller. Kleene getting lazy. Science of Computer Programming 65, 195–214 (2007).
[23] B. Möller, P. Höfner, and G. Struth. Quantales and temporal logics. In M. Johnson and V. Vene, editors, *Algebraic Methodology and Software Technology (AMAST 2006)*, volume 4019 of *Lecture Notes in Computer Science*, pages 263–277. Springer, 2006.
[24] B. Möller and G. Struth. Algebras of modal operators and partial correctness. *Theoretical Computer Science*, 351:221–239, 2006.
[25] B. Möller and G. Struth. wp is wlp. In W. MacCaull, M. Winter, and I. Düntsch, editors, *Relational Methods in Computer Science*, volume 3929 of *Lecture Notes in Computer Science*, pages 200–211. Springer, 2006.
[26] G. Nelson. A generalization of Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 11:517–561, 1989.
[27] G. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer, 1993.
[28] M. Spivey. *The Z notation: A reference manual*. International Series in Computer Science. Prentice Hall, 1992. Available under `http://spivey.oriel.ox.ac.uk/~mike/zrm/`.
[29] G. Struth. Non-symmetric rewriting. Technical Report MPI-I-96-2-004, Max-Planck-Institut für Informatik, 1996.
[30] G. Struth. *Canonical Transformations in Algebra, Universal Algebra and Logic*. PhD thesis, Institut für Informatik, Universität des Saarlandes, Germany, 1998.

[31] G. Struth. Calculating Church-Rosser proofs in Kleene algebra. In H.C.M. de Swart, editor, *Relational Methods in Computer Science, 6th International Conference*, volume 2561 of *Lecture Notes in Computer Science*, pages 276–290. Springer, 2002.
[32] G. Struth. Abstract abstract reduction. *Journal of Logic and Algebraic Programming*, 66(2):239–270, 2006.
[33] A. Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–309, 1955.
[34] Terese, editor. *Term Rewriting Systems*. Cambridge University Press, 2003.
[35] J. von Wright. From Kleene algebra to refinement algebra. In B. Möller and E. Boiten, editors, *6th International Conference on Mathematics of Program Construction, MPC 2002*, volume 2386 of *Lecture Notes in Computer Science*, pages 233–262. Springer, 2002.