Termination in modal Kleene algebra

Jules Desharnais, Bernhard Möller, Georg Struth

Angaben zur Veröffentlichung / Publication details:

Desharnais, Jules, Bernhard Möller, and Georg Struth. 2004. "Termination in modal Kleene algebra." In *Exploring new frontiers of theoretical informatics: IFIP 18th World Computer Congress; TC1 3rd International Conference on Theoretical Computer Science (TCS2004); 22 - 27 August 2004, Toulouse, France: WCC 2004*, edited by Jean-Jacques Lévy, 653–66. Boston [u.a.]: Kluwer.

TERMINATION IN MODAL KLEENE ALGEBRA

Jules Desharnais[1], Bernhard Möller[2] and Georg Struth[2*]

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

[2] *Institut für Informatik, Universität Augsburg,*
Universitätsstr. 14, D-86135 Augsburg, Germany
{moeller,struth}@informatik.uni-augsburg.de

Abstract Modal Kleene algebras (MKAs) are Kleene algebras with forward and backward modal operators defined via domain and codomain operations. The paper formalizes and compares different notions of termination, including Löb's formula, in MKA. It studies exhaustive iteration and gives calculational proofs of two fundamental termination-dependent statements from rewriting theory: the well-founded union theorem by Bachmair and Dershowitz and Newman's lemma. These results are also of general interest for the termination analysis of programs and state transition systems.

1. Introduction

Kleene algebras, initially conceived as algebras of regular events [5, 12], have by now applications ranging from program development and analysis to rewriting theory and concurrency control. Recently, they have been extended to comprise infinite iteration [4] and abstract domain and codomain operations [6]. The latter extension leads to modal Kleene algebras: forward and backward boxes and diamonds are definable "semantically" in terms of domain and codomain operations.

We propose MKAs as a useful tool for termination analysis. It allows a simple and calculational style of reasoning that is also well-suited for mechanization. Induction with respect to "external" measures is avoided in favour of "internal" fixed-point reasoning and contraction law. Point-

*Partially supported by DFG Project InopSys (Interoperability of System Calculi).

free proofs in the algebra of modal operators introduce a new level of abstraction and conciseness.

Our main results are as follows. First, we investigate notions of Noethericity and well-foundedness in MKA, abstracted from set-theoretic relations (cf. [8]). We compare this notion with two alternatives. The first models termination as absence of proper infinite iteration. We show that this notion is not equivalent to the previous one, even under natural additional assumptions. It turns out that the notion of termination induced by MKA is the more natural and useful one. The second alternative arises in modal logic as Löb's formula [3] and is essentially equivalent to the first one. MKA can serve as an algebraic semantics for modal logics, allowing simple calculational correspondence proofs for second-order frame properties. Note however, that the star operation of Kleene algebra is usually not available in classical modal logic.

Second, we continue our research on abstract rewriting in Kleene algebra [16, 17]. We prove Bachmair's and Dershowitz's well-founded union theorem [2] and a variant of Newman's lemma (cf. [1]) in MKA. These proofs are simpler than previous results in related structures [8, 14]. Moreover, MKA provides an algebraic semantics for the usual rewrite diagrams; the algebraic proofs immediately reflect their diagrammatic counterparts. Together with our earlier results this shows that a large part of abstract rewriting is indeed conveniently modelled by MKA.

Because of space limitations we suppress some details and additional results that, however, can be found in [7].

2. Modal Kleene Algebra

A *semiring* is a structure $(K, +, \cdot, 0, 1)$ such that $(K, +, 0)$ is a commutative monoid, $(K, \cdot, 1)$ is a monoid, multiplication distributes over addition from the left and right and zero is a left and right annihilator, i.e., $a0 = 0 = 0a$ for all $a \in K$ (the operation symbol $\cdot$ is omitted here and in the sequel). The semiring is *idempotent* if it satisfies $a + a = a$ for all $a \in K$. Then K has a *natural ordering* $\leq$ defined for all $a, b \in K$ by $a \leq b$ iff $a + b = b$. It induces a semilattice with $+$ as join and 0 as the least element; addition and multiplication are isotone w.r.t. $\leq$.

A *Kleene algebra* [12] is a structure $(K, ^*)$ such that K is an idempotent semiring, and the *star* * satisfies, for $a, b, c \in K$, the *unfold* and *induction laws*

$$1 + aa^* \leq a^*, \quad (*\text{-}1) \qquad\qquad b + ac \leq c \Rightarrow a^*b \leq c, \quad (*\text{-}3)$$

$$1 + a^*a \leq a^*, \quad (*\text{-}2) \qquad\qquad b + ca \leq c \Rightarrow ba^* \leq c. \quad (*\text{-}4)$$

Therefore, a^* is the least pre-fixpoint and the least fixpoint of the mappings $\lambda x.ax + b$ and $\lambda x.xa + b$ and the star is $\leq$-isotone.

Models of KA are for instance the set-theoretic relations under set union, relational composition and reflexive transitive closure, the sets of regular languages (regular events) over some finite alphabet, the algebra of path sets in a directed graph under path concatenation and the algebra of imperative programs with angelic choice, composition and iteration.

A *Boolean algebra* is a complemented distributive lattice. A *test semiring* is a structure $(K, \mathsf{test}(K))$, where K is an IL-semiring and $\mathsf{test}(K) \subseteq K$ is a Boolean algebra embedded into K, such that join and meet in $\mathsf{test}(K)$ coincide with the restrictions of $+$ and $\cdot$ of K to $\mathsf{test}(K)$, resp., and such that 0 and 1 are the least and greatest elements of $\mathsf{test}(K)$. Hence $p \leq 1$ for all $p \in \mathsf{test}(K)$. But in general, $\mathsf{test}(K)$ is only a subalgebra of the subalgebra of all elements below 1 in K.

We will consistently use the letters $a, b, c \ldots$ for semiring elements and $p, q, r, \ldots$ for Boolean elements. The symbol $\neg$ denotes complementation in $\mathsf{test}(K)$. We will also use relative complement $p - q = p\,\neg q$ and implication $p \to q = \neg p + q$ with their standard laws.

A *Kleene algebra with tests* [13] is a test semiring (K, B) such that K is a KA. For all $p \in \mathsf{test}(K)$ we have that $p^* = 1$.

Let now a semiring element a describe an action or abstract program and a test p a proposition or assertion. Then pa describes a restricted program that acts like a when the initial state satisfies p and aborts otherwise. Symmetrically, ap describes a restriction of a in its possible final states. We now introduce an abstract domain operator $\ulcorner$ that assigns to a the test that describes precisely its enabling states.

An *semiring with domain* [6] (a $\ulcorner$-semiring) is a structure $(K, \ulcorner)$, where K is an idempotent semiring and the *domain operation* $\ulcorner\colon K \to \mathsf{test}(K)$ satisfies for all $a, b \in K$ and $p \in \mathsf{test}(K)$

$$a \leq (\ulcorner a)a, \quad \text{(d1)} \qquad \ulcorner(pa) \leq p, \quad \text{(d2)} \qquad \ulcorner(a\,\ulcorner b) \leq \ulcorner(ab) \quad \text{(d3)}$$

If K is a KA, we speak of a *KA with domain*, briefly $\ulcorner$*-KA*. To explain (d1) and (d2) we note that their conjunction is equivalent to each of

$$\ulcorner a \leq p \Leftrightarrow a \leq pa, \quad \text{(llp)} \qquad \ulcorner a \leq p \Leftrightarrow \neg pa \leq 0, \quad \text{(gla)}$$

which constitute elimination laws for $\ulcorner$. (llp) and (gla) say that $\ulcorner a$ is the least left preserver and $\neg\ulcorner a$ is the greatest left annihilator of a, resp. Both properties obviously characterize domain for set-theoretic relations. (d3) states that the domain of ab is not determined by the inner structure of b or its codomain; information about $\ulcorner b$ in interaction with a suffices.

Many natural properties follow from the axioms. Domain is uniquely defined. It is strict ($\ulcorner a = 0 \Leftrightarrow a = 0$), additive ($\ulcorner(a + b) = \ulcorner a + \ulcorner b$), isotone ($a \leq b \Rightarrow \ulcorner a \leq \ulcorner b$), local ($\ulcorner(ab) = \ulcorner(a\,\ulcorner b)$) and stable on tests ($\ulcorner p = p$). Domain satisfies an import/export law ($\ulcorner(pa) = p\,\ulcorner a$), and an

induction law ($\ulcorner(ap) \leq p \Rightarrow \ulcorner(a^*p) \leq p$). Finally, domain commutes with all existing suprema. See [6] for further information.

A codomain operation $\urcorner$ is easily defined as a domain operation in the opposite semiring in which the order of multiplication is swapped. We call a semiring K with domain and codomain also a *modal semiring*; if K in addition is a KA, we call it a *modal KA (MKA)*.

Let K be a modal semiring. We introduce forward and backward diamond operators via abstract preimage and image.

$$|a\rangle p = \ulcorner(ap), \qquad (1) \qquad\qquad \langle a|p = (pa)\urcorner, \qquad (2)$$

for all $a \in K$ and $p \in \mathsf{test}(K)$. It follows that diamond operators are strict additive mappings (or *hemimorphisms*) on the algebra of tests.

Forward and backward diamonds satisfy the *exchange law*

$$|a\rangle p \leq \neg q \Leftrightarrow \langle a|q \leq \neg p \qquad (3)$$

for all $a \in K$ and $p, q \in \mathsf{test}(K)$. De Morgan duality transforms diamonds into boxes and vice versa, for instance $|a]p = \neg|a\rangle\neg p$ and $|a\rangle p = \neg|a]\neg p$. This yields Galois connections: for all $a \in K$ and $p, q \in \mathsf{test}(K)$,

$$|a\rangle p \leq q \Leftrightarrow p \leq [a|q, \qquad (4) \qquad\qquad \langle a|p \leq q \Leftrightarrow p \leq |a]q. \qquad (5)$$

Hence diamonds (boxes) commute with all existing suprema (infima) of the test algebra and thus are isotone.

In the sequel, when the direction of diamonds and boxes does not matter, we will use the notation $\langle a\rangle$ and $[a]$. For a test p we have $\langle p\rangle q = pq$ and $[p]q = p \rightarrow q$. Hence, $\langle 1\rangle = [1]$ is the identity function on tests. Moreover, $\langle 0\rangle p = 0$ and $[0]p = 1$.

We now study the modal operators as objects with their own algebra. We use the pointwise ordering $f \leq g \Leftrightarrow \forall p \,.\, fp \leq g\,p$ between functions $f, g : \mathsf{test}(K) \rightarrow \mathsf{test}(K)$, and the pointwise liftings of join and meet,

$$(f + g)(p) = f(p) + g(p), \quad (6) \qquad\qquad (f \sqcap g)(p) = f(p)g(p). \quad (7)$$

We also use the pointwise liftings of $-$ and $\rightarrow$ to the operator level.

Many properties of modal operators can now be presented much more succinctly in the respective algebra of operators. First, modalities distribute through the semiring operators as follows.

$$\begin{array}{rclrclrcl} \langle a + b\rangle & = & \langle a\rangle + \langle b\rangle, & |ab\rangle & = & |a\rangle|b\rangle, & \langle ab| & = & \langle b|\langle a|, \\ [a + b] & = & [a] \sqcap [b], & |ab] & = & |a]|b], & [ab| & = & [b|[a|. \end{array}$$

Note that the decomposition with respect to multiplication is covariant for forward modalities and contravariant for backward modalities. The decomposition can be used to transform expressions into normal form and to reason entirely at the level of modal o0perators. These laws imply that diamonds are isotone, i.e., $a \leq b$ implies $\langle a\rangle \leq \langle b\rangle$, and boxes are antitone, i.e., $a \leq b$ implies $[b] \leq [a]$.

Next, the test-level Galois connections can be lifted to operators $f, g : \mathsf{test}(K) \to \mathsf{test}(K)$ by setting, for all $a \in K$,

$$|a\rangle f \leq g \Leftrightarrow f \leq [a|g, \qquad \langle a|f \leq g \Leftrightarrow f \leq |a]g.$$

Finally, we obtain the following unfold and induction laws (cf. [6]):

$$|1\rangle + |a\rangle|a^*\rangle = |a^*\rangle, \qquad |1\rangle + |a^*\rangle|a\rangle = |a^*\rangle, \tag{8}$$

$$|b\rangle + |a\rangle|c\rangle \leq |c\rangle \Rightarrow |a^*\rangle|b\rangle \leq |c\rangle. \tag{9}$$

3. Termination in Modal Kleene Algebra

We now abstract a notion of termination from the theory of partial orders. A similar characterization has been used in [10].

According to the standard definition, a relation R on a set A is well-founded iff every non-empty subset of A has an R-minimal element. In a $^\ulcorner$- semiring K the minimal part of $p \in \mathsf{test}(K)$ w.r.t. some $a \in K$ can algebraically be characterized as $p - \langle a|p$, i.e., as the set of points that have no a-predecessor in p. So, by contraposition, the well-foundedness condition holds iff for all $p \in \mathsf{test}(K)$ one has $p - \langle a|p \leq 0 \Rightarrow p \leq 0$. Abstracting to a modal semiring K (and using Boolean algebra) we say that a is *well-founded* or *Noetherian*, resp., if for all $p \in \mathsf{test}(K)$,

$$p \leq \langle a|p \Rightarrow p \leq 0. \tag{10}$$

$$p \leq |a\rangle p \Rightarrow p \leq 0. \tag{11}$$

Note that by de Morgan duality a is Noetherian iff, for all $p \in \mathsf{test}(K)$,

$$|a]p \leq p \Rightarrow 1 \leq p. \tag{12}$$

The set of Noetherian elements in K is denoted by $\mathcal{N}(K)$.

We now state abstract algebraic variants of some simple and well-known properties of well-founded and Noetherian relations. Because of symmetry we only treat Noethericity; for algebraic proofs see [6].

LEMMA 1 *Let K be a $^\ulcorner$-semiring with $0 \neq 1$ and $a, b \in K$, $p \in \mathsf{test}(K)$.*

(i) $0 \in \mathcal{N}(K)$.
(ii) $p \notin \mathcal{N}(K)$, *if* $p \neq 0$ *and in particular* $1 \notin \mathcal{N}(K)$.
(iii) $b \in \mathcal{N}(K)$ *and* $a \leq b$ *imply* $a \in \mathcal{N}(K)$.
(iv) $a \in \mathcal{N}(K)$ *implies* $a \sqcap 1 \leq 0$, *i.e., a is irreflexive.*
(v) $a \not\leq 0$ *and* $a \in \mathcal{N}(K)$ *imply* $a \not\leq aa$, *that is a is not dense.*
(vi) $a \in \mathcal{N}(K)$ *iff* $a^+ \in \mathcal{N}(K)$, *for K a $^\ulcorner$-KA.*
(vii) $a^* \notin \mathcal{N}(K)$, *for K a KA with domain.*
(viii) $a + b \in \mathcal{N}(K)$ *implies* $a \in \mathcal{N}(K)$ *and* $b \in \mathcal{N}(K)$.

In general, $a \in \mathcal{N}(K)$ and $b \in \mathcal{N}(K)$ do not imply $a + b \in \mathcal{N}(K)$, so that $\mathcal{N}(K)$ is not a semilattice-ideal. A trivial counterexample is given by the relations $a = \{(0, 1)\}$ and $b = \{(1, 0)\}$. In Section 7 we will present commutativity conditions that enforce this implication.

4. Termination in Modal Logics

We now give two equational characterizations of Noethericity. The first one uses the star, the second one does not. It holds for the special case of a *transitive* Kleenean element a, i.e., when $aa \leq a$.

Let K be a $\ulcorner$-semiring or a $\ulcorner$-KA, resp. Consider the equations

$$|a\rangle \leq |a\rangle^+(|1\rangle - |a\rangle), \quad (13) \qquad\qquad |a\rangle \leq |a\rangle(|1\rangle - |a\rangle). \quad (14)$$

The equation (14) is a translation of Löb's formula from modal logic (cf. [3]) that expresses well-foundedness in Kripke structures. We say that a is *pre-Löbian* if it satisfies (13). We say that a is *Löbian* if it satisfies (14). The sets of pre-Löbian and Löbian elements of K are denoted by $p\mathcal{L}(K)$ and $\mathcal{L}(K)$, resp.

In the relational model, Löb's formula states that a is transitive and that there are no infinite a-chains. We will now relate Löb's formula and Noethericity.

THEOREM 2 *Let T be the set of transitive elements of a $\ulcorner$-KA K.*
(i) $\mathcal{L}(K) \subseteq \mathcal{N}(K)$.
(ii) $p\mathcal{L}(K) \subseteq \mathcal{N}(K)$.
(iii) $\mathcal{N}(K) \subseteq p\mathcal{L}(K)$.
(iv) $\mathcal{N}(T) \subseteq \mathcal{L}(T)$.

Properties (i) and (iv) already hold in $\ulcorner$-semirings. A calculational proof of (iii) based on [10] can be found in [6].

The calculational translation between the Löb-formula and our definition of Noethericity is quite interesting for the correspondence theory of modal logic. In this view, our property of Noethericity expresses a frame property, which is part of semantics, whereas the Löb formula stands for a modal formula, which is part of syntax. In modal semirings, we are able to express syntax and semantics in one and the same formalism. Moreover, 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 instance for mechanization.

5. Termination via Infinite Iteration

Cohen has extended KA with an $^\omega$ operator for modeling infinite iteration [4]; he has also shown applications in concurrency control. In [17], this algebra has been used for calculating proofs of theorems from abstract rewriting that use simple termination assumptions.

An *ω-algebra* is a structure (K, ω) where K is a KA and

$$a^\omega \leq aa^\omega, \qquad (15) \qquad\qquad c \leq ac + b \Rightarrow c \leq a^\omega + a^*b, \qquad (16)$$

for all $a, b, c \in K$. Hence a^ω is also the greatest fixpoint of $\lambda x \,.\, ax$.

Like in Section 2, for a $^\ulcorner$-KA K it seems interesting to lift (15) and (16) to operator algebras, similar to the laws (8), and (9) for the star. This is very simple for (15): for $a \in K$,

$$|a^\omega\rangle \leq |a\rangle|a^\omega\rangle. \tag{17}$$

However, as we will see below, there is no law corresponding to (9) and (16). The proof of (9) uses (llp) and works, since the star occurs at the left-hand sides of inequalities. There is no similar law that allows us to handle $^\omega$ which occurs at right-hand sides of inequalities.

Instead one can axiomatize the greatest fixpoint $\nu|a\rangle$ of $|a\rangle$ for $a \in K$:

$$\nu|a\rangle \leq |a\rangle\, \nu|a\rangle, \tag{18}$$

$$p \leq |a\rangle p + q \Rightarrow p \leq \nu|a\rangle + |a^*\rangle q. \tag{19}$$

For complete $\mathsf{test}(K)$, by the Knaster-Tarski theorem $\nu|a\rangle$ always exists, since $|a\rangle$ is isotone. Then one can use a weaker axiomatization (see [10]) from which (19) follows by greatest fixpoint fusion.

Since $|a\rangle p = \neg|a]\neg p$, existence of $\nu|a\rangle$ also implies existence of the least fixpoint $\mu|a]$ of $|a]$, since $\mu|a] = \neg\nu|a\rangle$. In the modal μ-calculus, $\mu|a]$ is known as the *halting predicate* (see, e.g., [11]). With the help of $\nu|a\rangle$ we can rephrase Noethericity more concisely as

$$a \in \mathcal{N}(K) \Leftrightarrow \nu|a\rangle = 0. \tag{20}$$

Corollary 3 *Define, for fixed $q \in \mathsf{test}(K)$ and $a \in K$, the function $f : \mathsf{test}(K) \to \mathsf{test}(K)$ by $fp = q + |a\rangle p$. If $\nu|a\rangle$ exists and $a \in \mathcal{N}(K)$ then f has the unique fixpoint $|a^*\rangle q$.*

Proof. The star axioms imply that that the least fixpoint of f is $|a^*\rangle q$. But by the assumption and (19) this is also the greatest fixpoint of f so that all fixpoints coincide with it. □

It turns out that $\nu|a\rangle$ is more suitable for termination analysis than a^ω. In ω-algebra one defines guaranteed termination as the absence of infinite iteration. We call a *ω-Noetherian* if $a^\omega \leq 0$, and denote by $\mathcal{N}_\omega(K)$ the set of all ω-Noetherian elements. To study the relation between $\mathcal{N}$ and $\mathcal{N}_\omega$, we call a $^\ulcorner$-KA K *extensional*, if $|a\rangle \leq |b\rangle \Rightarrow a \leq b$ for all $a, b \in K$. E.g., the language model is not extensional. The following lemma shows, somewhat surprisingly, that the connection between Noethericity and ω-Noethericity does not depend on extensionality, although the two notions coincide for the extensional relational model.

Lemma 4 *Let K be an ω-algebra with domain.*
(i) $\mathcal{N}(K) \subseteq \mathcal{N}_\omega(K)$.
(ii) $\mathcal{N}_\omega(K) \not\subseteq \mathcal{N}(K)$, *for K suitably chosen.*
(iii) $\mathcal{N}_\omega(K) \not\subseteq \mathcal{N}(K)$, *for extensional K suitably chosen.*
(iv) $\mathcal{N}_\omega(K) \subseteq \mathcal{N}(K)$, *for non-extensional K suitably chosen.*

Proof. (i) Let a be Noetherian. By isotonicity, for all $p \in \mathsf{test}(K)$,

$$|a^\omega\rangle p \leq |aa^\omega\rangle p = |a\rangle|a^\omega\rangle p.$$

Hence Noethericity of a implies that $|a^\omega\rangle p = 0$ for all $p \in \mathsf{test}(K)$. But, by strictness of domain, this is the case iff $a^\omega = 0$.

(ii) In the language model we have $a^\omega = 0$ if $1 \sqcap a = 0$, but also $a \neq 0 \Rightarrow \forall p \,.\, |a\rangle p = p$.

(iii) We use an *atomic* KA, in which every element is the sum of *atoms*, i.e., minimal nonzero elements. There are 4 atoms and hence 2^4 elements; it is order-isomorphic to the power set of the set of atoms under inclusion. The atoms of the test algebra are p and q, i.e., $1 = p + q$. The domain of an element x is the sum of all atomic tests t such that $tx \neq 0$. Composition is given by a table for the atoms only; it extends to the other elements through disjunctivity, thus satisfying this axiom by construction. E.g., for atoms w, x, y, z we set $(w+x)(y+z) = wy + wz + xy + xz$. The algebra is extensional. Moreover, it is easily checked that 0 is the only fixpoint of the function $\lambda x \,.\, (a + b)x$, so that $(a + b)^\omega = 0$. But $1 \leq |a + b\rangle 1$.

$\cdot$	p	q	a	b
p	p	0	a	0
q	0	q	0	b
a	0	a	0	0
b	b	0	0	0

(iv) Consider the KA K from [5], p. 101. It consists of elements $0 < 1 < a$; the ordering defines the addition table. The only non-trivial relation in the multiplication table is $aa = a$. The star is defined by $a^* = a$ and $0^* = 1^* = 1$. We extend K to an ω-algebra by setting $0^\omega = 0$ and $1^\omega = a^\omega = a$. Moreover, we define domain by $\ulcorner 0 = 0$ and $\ulcorner 1 = \ulcorner a = 1$. Since $x^\omega = 0 \Leftrightarrow x = 0$ holds in K, i.e., $\mathcal{N}_\omega(K) = \{0\}$, we have to verify $\mathcal{N}_\omega(K) \subseteq \mathcal{N}(K)$ only for the zero. But $0 \in \mathcal{N}(K)$ was already stated in Lemma 1(i). □

By the following corollary, (16) cannot in general be lifted to (19).

COROLLARY 5 *There exists a $\ulcorner$-KA K such that $\nu|a\rangle \leq 0$, but $a^\omega > 0$ for some $a \in K$.*

Thus ω-algebra does not entirely capture the notion of termination.

6. Termination of Exhaustive Iteration

We now study the exhaustive finite iteration of an element $a \in K$,

$$\mathsf{exh}\, a = \mathsf{while}\, \ulcorner a\, \mathsf{do}\, a = a^* \neg \ulcorner a \;.$$

Then the set of points from which a terminal point can be reached via a-steps is represented by

$$\ulcorner(\mathsf{exh}\, a) = \ulcorner(a^* \neg \ulcorner a) = |a^*\rangle \neg \ulcorner a. \tag{21}$$

PROPOSITION 6 *If $a \in \mathcal{N}(K)$ then $\ulcorner(\mathsf{exh}\, a) = 1$, i.e., from* every *starting point a terminal point can be reached.*

Proof. We calculate a recursion equation for $\ulcorner(\mathsf{exh}\, a)$ as follows:

$$\begin{aligned}\ulcorner(\mathsf{exh}\, a) &= |a^*\rangle\neg\ulcorner a = (|1\rangle + |a\rangle|a^*\rangle)\neg\ulcorner a\\ &= \neg\ulcorner a + |a\rangle|a^*\rangle\neg\ulcorner a = \neg\ulcorner a + |a\rangle\ulcorner(\mathsf{exh}\, a)\ .\end{aligned}$$

The first step uses (21), the second star unfold, the third distributivity and neutrality of 1, the fourth again (21).

So $\ulcorner(\mathsf{exh}\, a)$ has to be a fixpoint of $f(p) = \neg\ulcorner a + |a\rangle p$ which by Noetheric-ity of a and Corollary 3 is unique. Hence our claim is shown if 1 also is a fixpoint of f. This holds, since $f(1) = \neg\ulcorner a + |a\rangle 1 = \neg\ulcorner a + \ulcorner a = 1$. □

This theorem shows again that MKA is more adequate for termination analysis than ω-algebra. To see this, consider the algebra LAN of formal languages which is both an ω-algebra and a $\ulcorner$-KA with complete test algebra $\mathsf{test}(\mathrm{LAN}) = \{0, 1\}$. In LAN we have $|a\rangle 1 = \ulcorner a = 1 \neq 0$ when $a \neq 0$ and hence $\mathcal{N}(a) \Leftrightarrow a = 0$. Moreover, distinguishing the cases $a = 0$ and $a \neq 0$, easy calculations show that in LAN we have $\mathsf{exh}\, a = \neg\ulcorner a$. This mirrors the fact that by totality of concatenation a nonempty language can be iterated indefinitely without reaching a terminal element. But we also have $a^\omega = 0$ whenever $1 \sqcap a = 0$. Therefore, unlike in the relational model, $a^\omega = 0 \not\Rightarrow \ulcorner(\mathsf{exh}\, a) = 1$, while still $\nu|a\rangle = 0 \Rightarrow \ulcorner(\mathsf{exh}\, a) = 1$.

7. Additivity of Termination

Many statements of abstract rewriting that depend on termination assumptions can be proved in ω-algebra [17], among them an abstract variant of Bachmair's and Dershowitz's well-founded union theorem [2]. For comparison, we prove that here in MKA.

Consider a KA K and $a, b \in K$. We say that a *semi-commutes* over b, if $ba \leq a^+b^*$. a *quasi-commutes* over b, if $ba \leq a(a + b)^*$. We write $sc(a, b)$ if a semi-commutes over b and $qc(a, b)$, iff a quasi-commutes over b. Semi-commutation and quasi-commutation state conditions for permuting certain steps to the left of others. In general, sequences with 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 where both kinds of steps are mixed. The following lemma lifts semi-commutation and quasi-commutation to sequences of b-steps and states a separation law.

Lemma 7 *For a KA K and all $a, b \in K$,*

(i) $sc(a, b) \Leftrightarrow b^*a \leq a^+b^*$,
(ii) $qc(a, b) \Leftrightarrow b^+a \leq a(a + b)^*$,
(iii) $(a + b)^* = a^*b^* + a^*b^+a(a + b)^*$.

A proof of this lemma can be found in [17]. The following lemma compares quasi-commutation and semi-commutation.

LEMMA 8 *Consider a KA K and $a, b \in K$.*
(i) $sc(a,b) \Rightarrow qc(a,b)$.
(ii) *If K is extensional and $a \in \mathcal{N}(K)$ then* $qc(a,b) \Rightarrow sc(a,b)$.

Proof. (i) Let a semi-commute over b. By Kleene algebra,

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

(ii) Let a quasi-commute over b and let a be Noetherian. First,

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

The first step uses Lemma 7(iii), the second distributivity and the definition of a^+, the third Lemma 7 (ii), the fourth $x^*x^* = x^*$.

To apply Noethericity, we now pass to the modal operator level. To enhance readability, we write α for $|a\rangle$ and β for $|b\rangle$ and ζ for $|0\rangle$.

$$\begin{aligned} \alpha(\alpha+\beta)^* - \alpha^+\beta^* &\leq (\alpha^+\beta^* + \alpha^+\alpha(\alpha+\beta)^*) - \alpha^+\beta^* \\ &= (\alpha^+\beta^* - \alpha^+\beta^*) + (\alpha\alpha^+(\alpha+\beta)^* - \alpha^+\beta^*) \\ &\leq \alpha\alpha^+(\alpha+\beta)^* - \alpha^+\alpha^+\beta^* \\ &= \alpha^+(\alpha(\alpha+\beta)^* - \alpha^+\beta^*). \end{aligned}$$

The first step uses isotonicity of minus in its first argument. The second step uses $(p+q) - r = (p-r) + (q-r)$. The third step uses $p - p = 0$, $a^+a^+ \leq a^+$ and antitonicity of subtraction in its second argument. The fourth step uses $aa^+ = a^+a$ and distributivity.

By Lemma 1(vi) we know that a is Noetherian iff a^+ is. Therefore $\alpha^+(\alpha+\beta)^* - \alpha^+\beta^* \leq \zeta$, whence $\alpha^+(\alpha+\beta)^* \leq \alpha^+\beta^*$. The claim then follows from $\alpha \leq \alpha^+$ and extensionality. □

LEMMA 9 *Let K be a $^\ulcorner$-KA.*
(i) *For all $a \in \mathcal{N}(K)$ and $b \in K$, $qc(a,b) \Rightarrow b^*a \leq a^+b^*$.*
(ii) *For all $a, b \in K$, $qc(a,b)$ and $a \in \mathcal{N}(K)$ imply $b^*a \in \mathcal{N}(K)$.*
(iii) *For all $b, b^*a \in \mathcal{N}(K)$, $(a+b) \in \mathcal{N}(K)$.*

Proof. We use the same abbreviations as in the previous proof.

(i) Immediate from Lemma 8 and Lemma 7 (i).

(ii) Let $a \in \mathcal{N}(K)$ and $\alpha\beta \leq (\alpha+\beta)^*\alpha$. Then by (i), $\alpha\beta^* \leq \beta^*\alpha^+$. Now let $p \leq \beta^*\alpha p$, whence $p \leq \alpha^+\beta^*p$ and in particular $\beta^*p \leq \alpha^+\beta^*p$. Since by Lemma1 (vi) a is Noetherian iff a^+ is, we have that $\beta^*p \leq 0$ by assumption. This can only be the case if $p \leq 0$.

(iii) We calculate $(a+b)^+ = (b^*a)^*b^*(a+b) \leq (b^*a)^+ + b^+$. Now $a+b$ is Noetherian if $(a+b)^+$ is. Let $p \leq (\alpha+\beta)^+p$. Then $p \leq (\beta^*\alpha)^+p + \beta^+p$ and $p \leq 0$ follows from the assumptions. □

Lemma 9 (ii) and (iii) immediately imply the main theorem of this section. It generalizes the Bachmair-Dershowitz well-founded union theorem from relations to MKA.

THEOREM 10 *Let K be an extensional $^\ulcorner$-KA and $a, b \in K$ with $qc(a,b)$. Then $(a+b) \in \mathcal{N}(K)$ iff $a, b \in \mathcal{N}(K)$.*

These results show that MKA provides proofs for abstract rewriting that are as simple as those in ω-algebra. Note that the original proofs in [2] are rather informal, while also previous diagrammatic proofs (e.g. [9]) suppress many elementary steps. In contrast, our algebraic proofs are complete, formal and still simple. For an extensive discussion of the relation between the proofs in ω-algebra and their diagrammatic counterparts see [17]. In particular, the algebraic proofs mirror precisely the diagrammatic; this also holds for the modal proofs given here.

8. Newman's Lemma and Normal Forms

We now turn from semi-commutation to commutation and confluence. For their direct algebraic characterization one either has to use converse at the element level or a combination of forward and backward modalities at the operator level. Since converse is not available in MKA, we have to choose the second alternative.

We say that $a, b \in K$ *commute* if $\langle b^* || a^* \rangle \leq |a^*\rangle\langle b^*|$, and *commute locally* if $\langle b || a \rangle \leq |a^*\rangle\langle b^*|$. These definitions can be visualized as

Then $a \in K$ is *(locally) confluent* if it (locally) commutes with itself.

In the relational setting, the generalization from confluence to commutation has been used in [15] for a theory of term-rewriting with pre-congruences that extends the traditional equational case. This also yields generalizations of the Church-Rosser theorem and of Newman's lemma. While the former has already been proved in Kleene algebra in [16], it has been argued in [17] that a proof of Newman's lemma does not work in pure Kleene or ω-algebra.

For the equational case, [14] gives a calculational proof of Newman's lemma in relation algebra. But it cannot be adapted to our case, since it uses a notion of unique normal form that does not exist in the commutation-based setting. Moreover, conceptually it is nicer to completely uncouple confluence from normal forms.

We will faithfully reconstruct the diagrammatic proof using Noetherian induction [15]; it turns out that MKA is very well suited for this. A calculational proof that is close in spirit occurs in [8]. However, it is more complex in that it uses full residuation, whereas we can make do with the much weaker concept of modal operators. (The modal box operator corresponds to the monotype factor that is also used in [8].) Also, the theorem there is more restricted, since it only covers the relational

case, whereas our result also applies to e.g. the path algebra. Now we are ready for our generalization of Newman's lemma.

THEOREM 11 *Let K be a modal KA with complete test algebra. If $a+b \in \mathcal{N}(K)$ and a and b commute locally then a and b commute.*

Proof. The central idea of our proof is to use a generalized predicate that characterizes the set of all points on which a and b commute and to retrieve full commutation as a special case. If we can show that this predicate is contracted by $|a+b]$ then, by the second form (12) of Noethericity, we are done. So let us define (rc stands for "restricted commutation")

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

$rc(p,a,b)$ states that a and b commute on all points in p. The notation $\langle p\rangle$ enhances the symmetry of the formulation; it is justified, since $|p\rangle = \langle p|$ for all tests p. Clearly, a and b commute iff $rc(1,a,b)$. Moreover, rc is downward closed, i.e., $rc(p,a,b) \wedge q \leq p \Rightarrow rc(q,a,b)$. We now define $r = \sup\{p \mid rc(p,a,b)\}$ which exists by completeness of $\mathsf{test}(K)$. This represents the set of all points on which a and b commute. Completeness of $\mathsf{test}(K)$ implies that $\cdot$ distributes over all suprema in $\mathsf{test}(K)$, so that $|r\rangle = \sup\{|p\rangle \mid rc(p,a,b)\}$. Moreover, composition with diamonds is universally disjunctive in both arguments, so that we may infer $rc(r,a,b)$. Together with downward closure of rc we therefore obtain

$$p \leq r \Leftrightarrow rc(p,a,b) \ . \tag{22}$$

We now show that r is contracted by $|a+b]$, so that $a+b \in \mathcal{N}(K)$ implies $r = 1$. For this we first calculate

$$\begin{array}{rcl}
(|a+b]r \leq r) & \Leftrightarrow & (\forall\, p \,.\, p \leq |a+b]r \Rightarrow p \leq r) \\
& \Leftrightarrow & (\forall\, p \,.\, \langle a+b|p \leq r \Rightarrow p \leq r) \\
& \Leftrightarrow & (\forall\, p \,.\, \langle a|p \leq r \wedge \langle b|p \leq r \Rightarrow p \leq r) \\
& \Leftrightarrow & (\forall\, p \,.\, rc(p_a,a,b) \wedge rc(p_b,a,b) \Rightarrow rc(p,a,b)).
\end{array}$$

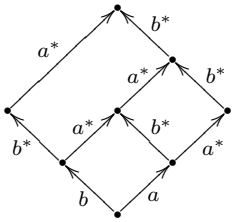
The first step uses order theory, the second the Galois connection (5), the third distributivity and Boolean algebra, the fourth (22) and the definition $p_x = \langle x|p$.

So assume $rc(p_a,a,b) \wedge rc(p_b,a,b)$. By the star fixpoint law (8) 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 isotonicity, $p \leq 1 \leq x^*$ and neutrality of $|1\rangle$. For the middle summand we first state

$$\langle p\rangle|x\rangle = \langle p\rangle|x\rangle\langle p_x\rangle \leq |x\rangle\langle p_x\rangle \ , \quad \langle x|\langle p\rangle = \langle p_x\rangle\langle x|\langle p\rangle \leq \langle p_x\rangle\langle x| \ . \tag{23}$$

This follows by isotonicity, since the definition of p_a and right neutrality of codomain imply $px = px(p_x) \leq x(p_x)$. Now we calculate, illustrating this by a 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, resp.

$$
\begin{array}{ll}
& \langle b^*|\langle b|\langle p\rangle|a\rangle|a^*\rangle \\
\leq & \langle b^*|\langle p_b\rangle\langle b||a\rangle\langle p_a\rangle|a^*\rangle \\
\leq & \langle b^*|\langle p_b\rangle|a^*\rangle\langle b^*|\langle p_a\rangle|a^*\rangle \\
\leq & |a^*\rangle\langle b^*|\langle b^*|\langle p_a\rangle|a^*\rangle \\
\leq & |a^*\rangle\langle b^*|\langle p_a\rangle|a^*\rangle \\
\leq & |a^*\rangle|a^*\rangle\langle b^*| \\
\leq & |a^*\rangle\langle b^*|.
\end{array}
$$



The first step uses idempotence of $\langle p\rangle$, codomain propagation (23) twice and compositionality, the second $\mathrm{LC}(a,b)$, the third the assumption $rc(p_a,a,b)$, the fourth idempotence of star and compositionality, the fifth the assumption $rc(p_b,a,b)$, the sixth idempotence of star and compositionality. □

We conclude this section by showing that confluence implies uniqueness of normal forms. As in Section 6, for $a \in K$ the element $\mathsf{exh}\, a = a^*\neg\ulcorner a$ describes the exhaustive iteration of a, the points in $(\mathsf{exh}\, a)^\urcorner$ being the *normal forms*. Now, a Kleene element b assigns to each point in its domain at most one point in its codomain iff b is *deterministic*, i.e., iff $\langle b||b\rangle \leq \langle 1\rangle$. This formula corresponds to the relational characterization $b^\smile b \leq 1$ of determinacy of b (where $^\smile$ is converse). Now we can show

LEMMA 12 *If a is confluent then* $\mathsf{exh}\, a$ *is deterministic.*
Proof. Plugging in the definition of $\mathsf{exh}\, a$ we calculate

$$
\begin{array}{rcl}
\langle a^*\neg\ulcorner a||a^*\neg\ulcorner a\rangle & = & \langle\neg\ulcorner a\rangle\langle a^*||a^*\rangle\langle\neg\ulcorner a\rangle \leq \langle\neg\ulcorner a\rangle|a^*\rangle\langle a^*|\langle\neg\ulcorner a\rangle \\
& = & |\neg\ulcorner aa^*\rangle\langle\neg\ulcorner aa^*| = |\neg\ulcorner a\rangle\langle\neg\ulcorner a| \leq \langle 1\rangle.
\end{array}
$$

The first step uses compositionality, the second confluence of a, the third compositionality again, the fourth the star fixpoint law, distributivity and (gla), the fifth isotonicity and idempotence of $\langle 1\rangle$. □

9. Conclusion

We have used modal KA for termination analysis, introducing and comparing different notions of termination that arise in this context and applying our techniques to two examples from abstract rewriting. All proofs are abstract, concise and entirely calculational. Together with previous work [16, 17] our case study in abstract rewriting shows that large parts of this theory can be reconstructed in MKA. By its simplicity, our approach has considerable potential for mechanization. There are strong connections with automata-theoretic decision procedures.

From the proof of Newman's lemma and the associated diagram it becomes clear that MKA allows one to perform induction in the middle of an expression. This is not possible in pure Kleene or ω-algebra due to the shape of the star and omega induction rules. Hence MKA allows

"context-free" induction, whereas pure Kleene or ω-algebra admit only "regular" induction. Therefore, in [8] residuals are used to move the point of induction from inside an expression to its ends and back.

The results of this paper contribute to establishing modal Kleene algebra as a formalism for safe cross-theory reasoning and therefore interoperability between different calculi for program analysis. We envision three main lines of further work. First, the integration of our results into Hoare-style reasoning and into Kleene algebras for the weakest precondition semantics, second, a further exploitation of the mentioned connection with the modal μ-calculus and third, further applications of our technique to the analysis of programs and protocols.

References

[1] F. Baader, T. Nipkow. *Term rewriting and all that*. Cambridge University Press 1998.

[2] L. Bachmair, N. Dershowitz. Commutation, transformation, and termination. In J.H. Siekmann (ed.), *8th International Conference on Automated Deduction*. LNCS 230. Springer 1986, 5–20.

[3] B.F. Chellas. *Modal Logic: An Introduction*. Cambridge University Press 1980.

[4] E. Cohen. Separation and reduction. In R. Backhouse, J.N. Oliveira (eds.), *Proc. Mathematics of Program Construction, 5th International Conference, MPC 2000*. LNCS 1887. Springer 2000, 45–59.

[5] J.H. Conway. *Regular Algebra and Finite State Machines*. Chapman & Hall 1971.

[6] J. Desharnais, B. Möller, G. Struth. Kleene algebra with domain. Technical Report 2003-07, Universität Augsburg, Institut für Informatik, June 2003.

[7] J. Desharnais, B. Möller, G. Struth. Termination in modal Kleene algebra. Technical Report 2004-04, Universität Augsburg, Institut für Informatik, January 2004.

[8] H. Doornbos, R. Backhouse, J. van der Woude. A calculational approach to mathematical induction. *Theoretical Computer Science*, 179:103–135 (1997).

[9] A. Geser. *Relative termination*. PhD thesis, Fakultät fur Mathematik und Informatik, Universität Passau 1990.

[10] R. Goldblatt., R. An algebraic study of well-foundedness. *Studia Logica*, 44(4):422–437 (1985).

[11] D. Harel, D. Kozen, J. Tiuryn. *Dynamic Logic*. MIT Press 2000.

[12] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390 (1994).

[13] D. Kozen. Kleene algebra with tests. *Trans. Programming Languages and Systems*, 19(3):427–443 (1997).

[14] G. Schmidt, T. Ströhlein. *Relations and Graphs*. EATCS Monographs in Computer Science. Springer 1993.

[15] G. Struth. Non-symmetric rewriting. Technical Report MPI-I-96-2-004, Max-Planck-Institut für Informatik Saarbrücken 1996.

[16] G. Struth. Calculating Church-Rosser proofs in Kleene algebra. In H.C.M. de Swart (ed.), *Relational Methods in Computer Science, 6th International Conference*. LNCS 2561. Springer 2002, 276–290.

[17] G. Struth. An algebraic study of commutation and termination. Technical Report 2003-18, Institut für Informatik, Universität Augsburg, December 2003.