Kleene Modules

Thorsten Ehm Bernhard Möller Georg Struth

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

Abstract We propose axioms for Kleene modules (KM). These structures have a Kleene algebra and a Boolean algebra as sorts. The scalar products are mappings from the Kleene algebra and the Boolean algebra into the Boolean algebra that arise as algebraic abstractions of relational image and preimage operations. KM is the basis of algebraic variants of dynamic logics. We develop a calculus for KM and discuss its relation to Kleene algebra with domain and to dynamic and test algebras. As an example, we apply KM to the reachability analysis in digraphs.

1 Introduction

Programs and state transition systems can be described in a bipartite world in which propositions model their static properties and actions or events their dynamics. Propositions live in a Boolean algebra and actions in a Kleene algebra with the regular operations of sequential composition, non-deterministic choice and reflexive transitive closure. Propositions and actions cooperate via modal operators that view actions as mappings on propositions in order to describe state-change and via test operators that embed propositions into actions in order to describe measurements on states and to model the usual program constructs.

Most previous approaches show an asymmetric treatment of propositions and actions. On the one hand, propositional dynamic logic (PDL) [9] and its algebraic relatives dynamic algebras (DA) [12,17,19] and test algebras (TA) [17,19,22] are proposition-based. DA has only modalities, TA has also tests. Most axiomatizations do not even contain explicit axioms for actions: their algebra is only implicitly imposed via the definition of modalities. On the other hand, Kleene algebra with tests (KAT) [14]—Kleene algebra with an embedded Boolean algebra—is action-based and has only tests, complementarily to DA. Therefore, action-based reasoning in DA and TA and proposition-based reasoning in KAT is indirect and restricted. In order to overcome these rather artificial asymmetries and limitations, KAT has recently been extended to Kleene algebra with domain (KAD) with equational axioms for abstract domain and codomain operations [6]. This alternative to PDL supports both proposition- and action-based reasoning and admits both tests and modalities. The defining axioms of KAD, however, are quite different from those of DA and TA. Therefore, what is the precise relation between KAD and PDL and its algebraic relatives? Moreover, is the asymmetry and the implicitness of the algebra of actions in DA and TA substantial?

We answer these two questions by extending the above picture with a further intermediate structure (c.f. Figure 1). As already observed by Pratt [19], the definition of DA resembles that of a module in algebra, up to implicitness of the algebra of actions, in which the scalar products define the modalities. When DA was presented, this was reasonable, since there was no satisfactory axiomatization of Kleene algebra. So Pratt could only conjecture that a *Kleene module* (KM) with a Kleene algebra as scalar sort and a Boolean algebra as the other would yield a more natural and convenient axiomatization of DA. Depending on more recent developments in Kleene algebra, our axiomatization of KM verifies Pratt's conjecture and shows that the implicitness of Kleene algebra in DA is in fact unnecessary. KM is also used as a key for answering the first question and establishing KAD as a natural extension of previous approaches.

Our contributions. First, we axiomatize and motivate the class KM as a straightforward adaptation of the usual modules from algebra [11]. We show that the scalar products abstractly characterize relational image and preimage operations. We outline a calculus for KM, including a duality between left and right scalar products in terms of a converse operation and a discussion of separability, that is, when actions are completely determined by their effects on states. We provide several examples of KM. We also relate our approach to a previous one based on a second-order axiomatization of the star [12].

Second, we relate KM and DA. We show that KM subsumes DA and, using a result of [19], that the equational classes of separable KM and separable DA coincide. This answers Pratt's conjecture. Consequently, the axioms of separable KM are complete with respect to the equational theory of finite Kripke structures.

Third, we relate KAD with KM and TA. We identify KAD with a subclass of TA, but obtain a considerably more economic axiomatization of that class. We show that the equational classes of separable KAD and separable TA coincide, improving a previous related result [10]. Consequently, the axioms of separable KAD are complete for the equational theory of finite Kripke (test) structures; the equational theory of separable KAD is EXPTIME-complete.

Fourth, we present extensions of KM that subsume TA, its above-mentioned subclass and KAD. This clarifies a related axiomatization [10].

Fifth, we demonstrate the expressiveness gap between KM and KAD by defining a basic toolkit for dynamic reachability analysis in directed graphs with interesting applications in the development and analysis of (graph) algorithms.

More generally, our technical comparison establishes KAD as a versatile alternative to PDL. Its uniform treatment of modal, scalar product and domain operators supports the interoperability of different traditional approaches to program analysis and development, an integration of action- and proposition-based views and a unification of techniques and results from these approaches.

Related Work. We can only briefly mention some closely related work. Our semiring-based variants of Kleene algebra and KAT are due to Kozen [13,14]. DA has been proposed by Pratt [19] and Kozen [12] and further investigated, for instance, in [17,18]. TA has been proposed by Pratt [19] and further investigated in [17,22]. With the exception of [12], these approaches implicitly axiomatize the algebra of actions, the explicit Kleene algebra axioms for DA in [12] contain a second-order axiom for the star. More recently, Hollenberg [10] has proposed TA with explicit Kleene algebra axioms. This approach is similar, but less economic than ours. The related class of Kleenean semimodules has recently been introduced by Leiß [15] in applications to formal language theory, with our Boolean algebra weakened to a semilattice. Earlier on, Brink [2] has presented Boolean modules, using a relation algebra instead of a Kleene algebra. A particular matrix-model of KM has been implicitly used by Clenaghan [4] for calculating path algorithms. In the context of reachability analysis, concrete models of Kleene algebras or relational approaches have also be used, for instance, by Backhouse, van den Eijnde and van Gasteren [1], by Brunn, Möller and Russling [3], by Ravelo [21] and by Berghammer, von Karger and Wolf [20]. Ehm [7] uses an extension of KM for analyzing pointer structures.

In this extended abstract we can only informally present selected technical results. More details and in particular complete proofs of all statements in this text can be found in [8].

2 Kleene Algebra

A *Kleene algebra* [13] is a structure $(K, +, \cdot, ^*, 0, 1)$ such that $(K, +, \cdot, 0, 1)$ is an (additively) idempotent semiring and *, the *star*, is a unary operation defined by the identities and quasi-identities

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

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

for all $a, b, c \in K$. The natural ordering $\leq$ on K is defined by $a \leq b$ iff $a + b = b$. We call $(*\text{-}1)$, $(*\text{-}2)$ the *star unfold* and $(*\text{-}3)$, $(*\text{-}4)$ the *star induction* laws.

KA denotes the class of Kleene algebras. It includes, for instance, the set-theoretic relations under set union, relational composition and reflexive transitive closure (the *relational Kleene algebra*), and the sets of regular languages (regular events) over some finite alphabet (the *language Kleene algebra*).

The additive submonoid of a Kleene algebra is also an upper semilattice with respect to $\leq$. Moreover, the operations of addition, multiplication and star are monotonic with respect to $\leq$. The equational theory of regular events is the free Kleene algebra generated by the alphabet [13]. We will freely use the well-known theorems of KA (c.f. [8] for a list of theorems needed). In particular, the star unfold laws can be strengthened to equations.

Kleene algebra provides an algebra of actions with operations of non-deterministic choice, sequential composition and iteration. It can be enriched by a Boolean algebra to incorporate also propositions.

A *Boolean algebra* is a complemented distributive lattice. By overloading, we write $+$ and $\cdot$ also for the Boolean join and meet operation and use 0 and 1 for the least and greatest elements of the lattice. $'$ denotes the operation of complementation. BA denotes the class of Boolean algebras. We will consistently use the letters $a, b, c\dots$ for Kleenean elements and $p, q, r, \dots$ for Boolean elements. We will freely use the theorems of Boolean algebra in calculations.

A first integration of actions and proposition is Kleene algebra with tests. A *Kleene algebra with tests* [14] is a two-sorted structure (K, B), where $K \in \mathsf{KA}$ and $B \in \mathsf{BA}$ satisfies $B \subseteq K$ and has minimal element 0 and maximal element 1. In general, B is only a subalgebra of the subalgebra of all elements below 1 in K, since elements of the latter need not be multiplicatively idempotent. We call elements of B *tests* and write $\mathsf{test}(K)$ instead of B. For all $p \in \mathsf{test}(K)$ we have that $p^* = 1$. The class of Kleene algebras with tests is denoted by KAT.

3 Definition of Kleene Modules

In this section we define the class of Kleene modules. These are natural variants of the usual modules from algebra [11]. We replace the ring by a Kleene algebra and the Abelian group by a Boolean algebra.

Definition 1. *A* Kleene left-module *is a two-sorted algebra* $(K, B, :)$*, where* $K \in \mathsf{KA}$ *and* $B \in \mathsf{BA}$ *and where the* left scalar product $:$ *is a mapping* $K \times B \to B$ *such that for all* $a, b \in K$ *and* $p, q \in B$*,*

$$a : (p + q) = a : p + a : q, \qquad \text{(km1)} \qquad\qquad 1 : p = p, \qquad \text{(km4)}$$

$$(a + b) : p = a : p + b : p, \qquad \text{(km2)} \qquad\qquad 0 : p = 0, \qquad \text{(km5)}$$

$$(ab) : p = a : (b : p), \qquad \text{(km3)} \qquad\qquad q + a : p \leq p \Rightarrow a^* : q \leq p. \qquad \text{(km6)}$$

We do not distinguish between the Boolean and Kleenean zeroes and ones. KM_l denotes the class of Kleene left-modules. In accordance with the relation-algebraic tradition, we call scalar products of KM_l also *Peirce products*. We assign priorities $'$ higher than $:$ higher than $+$ and $-$.

Axioms of the form (km1)–(km4) also occur in algebra. For rings, an analog of (km5) is redundant, whereas for semirings—in absence of inverses—it is independent. Axiom (km6) is of course beyond ring theory. It is the star induction rule ($*$-3) with the semiring product replaced by the Peirce product and the sorts of elements adjusted, that is b and c replaced by Boolean elements. We call such a transformation of a KA-expression to a KM_l-expression a *peircing*.

We define *Kleene right-modules* as Kleene left-modules on the opposite semiring in the standard way (c.f [11]) by switching the order of multiplications. We write $p : a$ for right scalar products. A *Kleene bimodule* is a Kleene left-module that is also a Kleene right-module. Left and right scalar products can be uniquely determined by bracketing. We will henceforth consider only Kleene left-modules.

4 Example Structures

We now discuss the two models of Kleene modules that are most important for our purposes, namely relational Kleene modules and Kripke structures. Further example structures can be found in [6].

Example 1. (**Relational Kleene modules**) Consider the relational Kleene algebra $\mathsf{REL}(A) = (2^{A\times A}, \cup, \circ, \emptyset, \Delta, {}^*)$, on a set A with $2^{A\times A}$ denoting the set of binary relations over A and $\cup$, $\circ$, $\emptyset$ and Δ denoting set-union, relational composition, the empty relation and the identity relation, respectively. Finally, for all $R \in \mathsf{REL}(A)$ the expression R^* denotes the reflexive transitive closure of R.

Of course also $\mathsf{REL}(A) \in \mathsf{KAT}$ with $\mathsf{test}(\mathsf{REL}(A))$ being the set of all subrelations of Δ. This holds, since $\mathsf{test}(\mathsf{REL}(A))$ is a field of sets, whence a Boolean algebra, with $P \cap Q = P \circ Q$ and $P' = \Delta - P$, the minus denoting set difference. $\mathsf{test}(\mathsf{REL}(A))$ is isomorphic with the field of sets 2^A under the homomorphic extension of the mapping sending B to $\{(b, b) \mid b \in B\}$ for all $B \subseteq A$.

The *preimage* of a set $B \subseteq A$ under a relation $R \subseteq A \times A$ is defined as

$$R : B = \{x \in A \mid \exists y \in B.(x, y) \in R\}, \tag{1}$$

The definition of image is similar. We extend this definition to $\mathsf{REL}(A)$ via the above isomorphism. Then $(\mathsf{REL}(A), \mathsf{test}(\mathsf{REL}(A)), :)$, with : given by (1), is in KM_l. Therefore the KM_l axioms abstractly model binary relations with a preimage operation. □

Example 2. (**Kripke Structure**) By Example 1, there is an isomorphism between the subsets of a set A and the set of subrelations of the identity relation $\Delta \subseteq A \times A$. A *Kripke structure* on a set A is a pair (K, B), where B is a field of sets on A and K is an algebra of binary relations on A under the operations of union, relational composition and reflexive transitive closure. Finally, a preimage operation on (B, K) is defined by (1).

Every Kripke structure contains the identity relation, since it is presumed in the definition of the reflexive transitive closure operation. However, it need not contain the empty relation. Therefore, not every Kripke structure is a Kleene left-module, but every Kripke structure with the empty relation is.

A *Kripke test structure* on A is a Kripke structure with the additional operation

$$?p = \{(x, x) \mid x \in p\},$$

for all $p \in B$. Kri and Krit denote the class of Kripke structures and Kripke test structures, respectively. The Kripke structure $(2^A, 2^{A\times A})$ is called the *full* Kripke structure on A; it is isomorphic with $\mathsf{REL}(A)$ and has all Kripke structures on A as subalgebras. □

The fact that KM_l contains relational structures and Kripke structures yields a natural correspondence with the semantics of modal logics. More example structures can be found in [6]. These examples are based on Kleene algebra with domain. But by the subsumption result in Proposition 3 below, they can easily be transfered to Kleene modules.

5 Calculus of Kleene Modules

In this section, we list some properties of Kleene modules that are helpful in an elementary calculus. These properties are also needed in the syntactic comparison of KM_l with other structures in Section 8.

The first lemma provides some properties that do not mention the star.

Lemma 1. *Let $(K, B, :) \in \mathsf{KM}_l$. For all $a \in K$ and $p, q \in B$, the scalar product has the following properties.*

(i) *It is right-strict, that is $a : 0 = 0$.*
(ii) *It is left- and right-monotonic.*
(iii) $p \leq 0 \Rightarrow a : p \leq 0$.
(iv) $a : (pq) \leq (a : p)(a : q)$.
(v) $a : p - a : q \leq a : (p - q)$.

Here, $p - q = pq'$. Remember that Peirce products are left-strict by (km4).

The following statements deal with peircing the star. The first lemma explains why KM_l has no peirced variants of ($*$-1) and ($*$-2) as axioms.

Proposition 1. *Let $(K, B, :) \in \mathsf{KM}_l$. Let $a \in K$ and $p \in B$.*

(i) $p + a : (a^* : p) = a^* : p$,
(ii) $p + a^* : (a : p) = a^* : p$.

The following statement shows that quasi-identity (km6), although quite natural as a peirced variant of ($*$-3), can be replaced as an axiom by an identity.

Proposition 2. *Let $(K, B, :) \in \mathsf{KM}_l$ Then the quasi-identity (km6) and the following identity are equivalent.*

$$a^* : p \leq p + a^* : (a : p - p). \tag{2}$$

Proof. The Galois connection $p - q \leq r \Leftrightarrow p \leq q + r$ implies that $p \leq q \Leftrightarrow p - q \leq 0$ and that the cancellation law $p \leq q + (p - q)$ holds.

(km6) implies (2). Let $p = q$. Then $a : p + p = p$ and $a^* : (a : p + p) \leq p$. Adding $p + a^* : (a : p - p)$ to both sides of this last inequality yields

$$\begin{aligned} p + a^* : (a : p - p) &\geq p + a^* : (a : p - p) + a^* : (a : p + p) \\ &= p + a^* : ((a : p - p) + a : p + p) \\ &\geq p + a^* : (a : p) \\ &= (1 + a^* a) : p \\ &= a^* : p. \end{aligned}$$

The second step uses (km1). The third step uses the cancellation law and Kleene algebra. The fourth step uses (km4) and (km2). The fifth step uses again Kleene algebra.

(2) implies (km6). Let $a : p + q \leq p$, whence $a : p \leq p$ and $q \leq p$ and therefore $a : p - p \leq 0$. Using right-monotonicity and (km5), we calculate

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

□

In [8], we present various additional properties. We show, for instance, that (km6) is also equivalent to $a : p \leq p \Rightarrow a^* : p \leq p$, which reflects an unpeirced theorem of KA, and that (2) can be strengthened to an equality. All these properties can easily be translated to theorems of propositional dynamic logic (c.f [9]), using our consideration in Section 8. In particular, (2) translates to an axiom.

6 Extensionality

In Kleene modules, the algebras of actions and propositions are only weakly coupled. The finer the algebra of propositions, the more precisely can we measure properties of actions. In general, actions are *intensional*; their behavior is not completely determined by measurements on states. Set-theoretic relations, however, are *extensional*, since they are sets. Set-theoretic extensionality can be lifted to Kleene modules to enforce relational models. In analogy to dynamic algebra [12,19], we call $(K, B, :) \in \mathsf{KM}$ *(left)-separable*, if for all $a, b \in K$

$$\forall p \in B.(a : p \leq b : p) \Rightarrow a \leq b. \tag{3}$$

SV denotes the separable subclass of an algebraic class V with appropriate signature.

An adaptation of a three-element Kleene Algebra from [5] shows that separability is independent in KM_l. (3) is equivalent to $\forall p \in B.(a : p = b : p) \Rightarrow a = b$. Moreover, converse implications also hold by monotonicity. The term *separability* can be explained as follows: Assume (3) and let $a \neq b$ for some $a, b \in K$. Then $a : p \neq b : p$ for some $p \in B$; the witness p separates action a from action b.

Besides this relational motivation, separability can also be introduced algebraically. In [8], we show that the relation $\preceq$ on $(K, A, :) \in \mathsf{KM}_l$ defined by

$$a \preceq b \Leftrightarrow \forall p \in B.(a : p \leq b : p),$$

for all $a, b \in K$ is a precongruence on KM_l, that is, the operation of addition, left and right multiplication and star are monotonic with respect to $\preceq$. Moreover, the relation $\sim\, = \,\preceq \cap \succeq$ is a congruence on KM_l. Therefore, a Kleene module is separable, iff $\sim$ is the identity relation.

The relation $\sim$ introduces a natural notion of *observational equivalence*. For a set A, the preimage $R : \{p\}$ of a singleton set $\{p\} \subseteq A$ under a relation $R \subseteq A \times A$ is the set of all $q \in A$ with $(q, p) \in R$. Intuitively, $R : \{p\}$ scans R point-wise for its input-output behavior. Since relations are extensional, they are completely determined by this scanning. In intensional models, one can distinguish between observable and hidden intrinsic behavior. The congruence $\sim$ then identifies two relations up to intrinsic behavior and therefore via observational equivalence. The freedom of choosing the algebra of propositions in KM with arbitrary coarseness fits very well with this idea of measuring and identifying actions in a more or less precise way.

7 Relatives of Kleene Modules

We now situate the class KM_l within the context of Kleene algebra with domain and algebraic variants of propositional dynamic logic. To this end, we define the classes of dynamic algebras, test algebras à la Hollenberg, test algebras à la Pratt and Kleene algebra with domain.

We obtain the class DA [19] of *dynamic algebras* from Definition 1 by requiring an absolutely free algebra of Kleenean signature K (without 0 and 1) instead of a Kleene algebra, by removing (km4) and (km5), by adding right-strictness (Lemma 1 (i)) and the peirced star unfold law of Proposition 1 and by replacing (km6) by (2). Therefore, the algebra of actions is implicitly axiomatized in DA.

A *test algebra* à la Hollenberg [10] is a structure $(K, B, :, ?)$, where $K \in \mathsf{KA}$ and $B \in \mathsf{BA}$ and the operations $:$ of Peirce product type and $?$ of type $B \to K$ satisfies the axioms (km2), (km3), (km6) and

$$p? : q = pq, \qquad (4) \qquad\qquad (pq)? = (p?)(q?), \qquad (7)$$

$$0? = 0, \qquad (5) \qquad\qquad (a : 1)?a = a. \qquad (8)$$

$$(p + q)? = p? + q?, \qquad (6)$$

TA_H denotes the corresponding class. We show in [8] that $?$ is an embedding from B into K. In analogy to KAT, the symbol $?$ can therefore be made implicit; the axioms (5)–(7) and the $?$ symbol in the axioms (4) and (8) can be discarded. TA_H then reduces to KAT with the remaining axioms. Note that the algebra of actions is explicitly axiomatized in TA_H.

We obtain the class TA_P of *test algebras* à la Pratt [19] from DA by extending the signature with $?$ and by adding the axiom (4). Therefore, the algebra of actions is again implicitly axiomatized in TA_P.

A *Kleene algebra with domain* [6] is a structure (K, δ), where $K \in \mathsf{KAT}$ and the *domain operation* $\delta : K \to \mathsf{test}(K)$ satisfies, for all $a, b \in K$ and $p \in \mathsf{test}(K)$,

$$a \leq \delta(a)a, \quad (\mathrm{d1}) \qquad \delta(pa) \leq p, \quad (\mathrm{d2}) \qquad \delta(a\delta(b)) \leq \delta(ab). \quad (\mathrm{d3})$$

KAD denotes the class of Kleene algebras with domain. The impact of (d1), (d2) and (d3) can be motivated as follows. (d1) is equivalent to one implication in each of the statements

$$\delta(a) \leq p \Leftrightarrow a \leq pa, \qquad (\mathrm{llp}) \qquad\qquad \delta(a) \leq p \Leftrightarrow p'a \leq 0. \qquad (\mathrm{gla})$$

which constitute elimination laws for δ. (d2) is equivalent to the other implications. (llp) says that $\delta(a)$ is the least left preserver of a. (gla) says that $\delta(a)'$ is the greatest left annihilator of a. Both properties obviously characterize domain in set-theoretic relations. (d3) states that the domain of ab is not determined by the inner structure of b or its codomain; information about $\delta(b)$ in interaction with a suffices. All three axioms hold in relational Kleene algebra. Note that in contrast to KM_l, there is no particular axiom for the star. As Lemma 2 (vi) below shows, a variant of the star induction law is a theorem of KAD.

As for Kleene modules, a codomain operation can be defined on the opposite Kleene algebra. Moreover, domain has the following properties.

Lemma 2 ([6]). *Let $K \in \mathsf{KAD}$. For all $a \in K$ and $p \in \mathsf{test}(A)$,*

(i) Strictness, $\delta(a) = 0 \Leftrightarrow a = 0$.
(ii) Additivity, $\delta(a + b) = \delta(a) + \delta(b)$.
(iii) Monotonicity, $a \leq b \Rightarrow \delta(a) \leq \delta(b)$.
(iv) Locality, $\delta(ab) = \delta(a\delta(b))$.
(v) Stability, $\delta(p) = p$.

(vi) Induction, $q + \delta(ap) \leq p \Rightarrow \delta(a^*q) \leq p$.

Of course, the preimage of a relation R under a set P can also be defined via domain as $\delta(RP)$. We use

$$a : p = \delta(ap), \quad (9) \qquad\qquad \delta(a) = a : 1, \quad (10)$$

for defining abstract preimage in KAD and abstract domain in KM_l.

8 Main Results

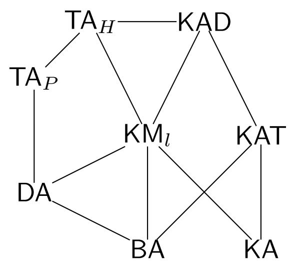

Figure 1.

Our main interest are subsumption relations between the classes introduced in Section 7. Here, we show only the most important ones. A more complete picture can be found in Figure 1. More relations and complete proofs can be found in [8]. We proceed purely calculationally by deriving the axioms in the subsumed class as theorems in the subsuming class. In particular, we use the properties of Peirce products from Section 5, the properties of domain from Section 7 and the translations (10), (9) between Peirce products and domain.

Proposition 3. $\mathsf{TA}_H = \mathsf{KAD} \subseteq \mathsf{KM}_l \subseteq \mathsf{DA}$.

Proof. We first show that $\mathsf{KAD} \subseteq \mathsf{TA}_H$. It follows from the remaining inclusions that all TA_H axioms but (8) are theorems of KAD. Since ? is an embedding, (8) can be written in the form $(a : 1)a = a$. Translating with (9), we see that one inequality is (d1) while the other one holds, since $\delta(a) \leq 1$.

We now show that $\mathsf{TA}_H \subseteq \mathsf{KAD}$, using (10) for translation. By the previous part of the proof it remains to show that axioms (d2) and (d3) are theorems of TA_H. For (d2), we must show that $(pa) : 1 \leq p$ by (10). Using (km3) and (4), which are axioms of TA_H, and Boolean algebra, we calculate

$$(pa) : 1 = p : (a : 1) = p(a : 1) \leq p.$$

For (d3), we must show that $(a(b : 1)) : 1 = (ab) : 1$. We calculate

$$(a(b : 1)) : 1 = a : ((b : 1) : 1) = a : ((b : 1)1) = a : (b : 1) = (ab) : 1.$$

The first step uses (km3). The second step uses (4), the third step uses Boolean algebra, the fourth step uses again (km3).

We now briefly discuss the remaining inclusions. $\mathsf{DA} \subseteq \mathsf{KM}_l$ is immediate from the definition of DA via theorems of KM_l. $\mathsf{KAD} \subseteq \mathsf{KM}_l$ follows from (9) and the results of Lemma 2. □

Proposition 3 shows that the axioms (km2) and (km6) are redundant in TA_H. The axioms (5)–(7) can be made implicit, using KAT for axiomatizing TA_H. Our axiomatization of KAD therefore reduces the number of axioms from eight to three compared to [10]. The reduction to KAT leads to additional economy of expression. Moreover, the axioms of KAD have a natural motivation as abstractions of set-theoretic domain operations, whereas the axiom (8), which does not appear in the traditional axiomatizations of test algebra, is not motivated in [10].

The following consequences of Proposition 3 are not entirely syntactic. They rely on previous semantic considerations [17,19,22]. As usual, we write $HSP(\mathsf{V})$ for the equational class or variety generated by a class V of algebras. This is the class of homomorphic images of subalgebras of products of algebras in V, according to Birkhoff's theorem. The left equality of the following semantic result is due to Pratt (Theorem 6.4. of [19]); the right equality is an adaptation by Hollenberg of a semantic result by Trnková and Reiterman (Corollary 1 of [22]).

Theorem 1. $HSP(\mathsf{SDA}) = HSP(\mathsf{Kri}) \supseteq HSP(\mathsf{Krit}) = HSP(\mathsf{STA}_H)$.

Based on the left equality of Theorem 1, Pratt conjectures that $HSP(\mathsf{SDA})$ *may be defined axiomatically by the dynamic algebra axioms [...] together with an appropriate set of axioms for binary relations.* At the time of writing, Kozen's axiomatization of KA did not yet exist. Hollenberg's axiomatization of TA_H verifies Pratt's conjecture with respect to TA_P. We can show that KM_l verifies it with respect to DA. More interestingly, KAD also verifies it with respect to TA_P. But axiomatically, KAD is a considerable improvement over TA_H.

Corollary 1. $HSP(\mathsf{SKM}_l) = HSP(\mathsf{Kri}) \supseteq HSP(\mathsf{Krit}) = HSP(\mathsf{SKAD})$.

9 Reachability Analysis in Directed Graphs

To demonstrate the applicability of KM and KAD, we present an abstract toolkit based on Kleene algebra for reachability analysis in digraphs. More details and proofs can again be found in [8]. Our toolkit has interesting applications in the development and analysis of graph algorithms, in the analysis of pointer and object structures and in garbage collection algorithms. Here, elements of K denote graphs and elements of $\mathsf{test}(K)$ denote sets of nodes.

The following concepts, for instance, can be defined in KM.

- $\mathsf{reach}(p,a) = p : a^*$ and $\mathsf{nreach}(p,a) = \mathsf{reach}(p,a)'$ denote the set of nodes that is reachable, respectably not reachable, from set p in a.
- $\mathsf{reach\text{-}p}(p,a,q) \Leftrightarrow q \leq \mathsf{reach}(p,a)$ and $\mathsf{nreach\text{-}p}(p,a,q) \Leftrightarrow q \leq \mathsf{nreach}(p,a)$ denote that set q is reachable, respectably non-reachable, from set p in a.

– $\mathsf{final}(p, a) = \mathsf{reach}(p, a)\delta(a)'$ denotes the final nodes with respect to reachability via a from p. When a is a program and p a set of initial states, then $\mathsf{final}(p, a)$ represents the solutions of a.

Note that $\mathsf{nreach\text{-}p}(q, a, p)$ reduces to $paq \leq 0$ in KAD. The following concepts must, however, be defined in KAD.

– $\mathsf{del}(a, b) = \delta(a)'b$ and $\mathsf{ins}(a, b) = a + \mathsf{del}(a, b)$ can be used to model deletions and insertions of edges in a graph.
– $\mathsf{span}(p, a) = \mathsf{reach}(p, a)a$ denotes the subgraph of a that is spanned from p via reachability.

All these definitions can easily be abstracted from the relational model. We can use them for calculating many interesting graph properties in KM or KAD. For instance, we can optimize reachability in KAD.

$$\mathsf{reach}(p, a) = p + \mathsf{reach}(p : a, p'a). \tag{11}$$

Another example are optimization rules for reach and span.

$$\mathsf{nreach\text{-}p}(p, a, \delta(b)) \Rightarrow \mathsf{reach}(p, a + b) = \mathsf{reach}(p, a), \tag{12}$$
$$\mathsf{nreach\text{-}p}(p, a, \delta(b)) \Rightarrow \mathsf{span}(p, a + b) = \mathsf{span}(p, a), \tag{13}$$
$$\mathsf{nreach\text{-}p}(p, a, \delta(b)) \Rightarrow \mathsf{reach}(p, \mathsf{ins}(b, a)) = \mathsf{reach}(p, a), \tag{14}$$
$$\mathsf{nreach\text{-}p}(p, a, \delta(b)) \Rightarrow \mathsf{span}(p, \mathsf{ins}(b, a)) = \mathsf{span}(p, a). \tag{15}$$

These results are applied to pointer analysis in [7]. Also a reconsideration of the previous approaches cited in the introduction seems promising.

10 Conclusion

We have presented an axiomatization of Kleene modules as a complementation to Kleene algebra with domain. This allows a fine-grained comparison with algebras related to propositional dynamic logic. Our results support a transfer between concepts and techniques from set- and relation-based program development methods and those based on modal logics. Although the striking correspondence between scalar products, relational preimage operations and modal operators is not entirely new, we find it still surprising.

In [8], we prove a series of further results. First, we relate KM_l with Kleenean semimodules [15], Boolean modules [2], the dynamic algebras of [12], monotonic predicate transformer algebras and Boolean algebras with operators. In particular, subsumption of the latter shows that Peirce products induce modal (diamond) operators. Second, we establish another duality between left- and right-modules via the operation of converse. Third, we show that separable Kleene bi-modules subsume SKAD. Fourth, our subsumption results allow a translation of previous results for TA to KAD. In particular, the SKAD axioms are complete with respect to the valid equations in Krit. Moreover $\mathit{HSP}(\mathsf{SKAD})$ is EXPTIME-complete. A similar transfer between DA and KM_l is also possible.

At the theoretic side, our results are only first steps of the representation theory for KM_l and KAD. A deeper investigation of these semantic issues is beyond the syntactic analysis of this paper. At the practical side, we have already started considering applications in the development of algorithms (cf. [16]).

References

1. R. C. Backhouse, J. P. H. W. van den Eijnde, and A. J. M. van Gasteren. Calculating path algorithms. *Science of Computer Programming*, 22(1-2):3–19, 1994.
2. C. Brink. Boolean modules. *Journal of Algebra*, 71:291–313, 1981.
3. T. Brunn, B. Möller, and M. Russling. Layered graph traversals and hamiltonian path problems–an algebraic approach. In J. Jeuring, editor, *Mathematics of Program Construction*, volume 1422 of *LNCS*, pages 96–121. Springer-Verlag, 1998.
4. K. Clenaghan. Calculational graph algorithmics: Reconciling two approaches with dynamic algebra. Technical Report CS-R9518, CWI, Amsterdam, 1994.
5. J. H. Conway. *Regular Algebra and Finite State Machines.* Chapman&Hall, 1971.
6. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. Technical Report 2003-07, Institut für Informatik, Universität Augsburg, 2003.
7. T. Ehm. Pointer Kleene algebra. Technical Report 2003-13, Institut für Informatik, Universität Augsburg, 2003.
8. T. Ehm, B. Möller, and G. Struth. Kleene modules. Technical Report 2003-10, Institut für Informatik, Universität Augsburg, 2003.
9. D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic.* MIT Press, 2000.
10. M. Hollenberg. Equational axioms of test algebra. In M. Nielsen and W. Thomas, editors, *Computer Science Logic, 11th International Workshop, CSL '97*, volume 1414 of *LNCS*, pages 295–310. Springer, 1997.
11. N. Jacobson. *Basic Algebra*, volume I,II. Freeman, New York, 1985.
12. D. Kozen. A representation theorem for $*$-free PDL. Technical Report RC7864, IBM, 1979.
13. D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.
14. D. Kozen. Kleene algebra with tests. *Trans. Programming Languages and Systems*, 19(3):427–443, 1997.
15. Hans Leiß. Kleenean semimodules and linear languages. In Zoltán Ésik and Anna Ingólfsdóttir, editors, *FICS'02 Preliminary Proceedings*, number NS-02-2 in BRICS Notes Series, pages 51–53. Univ. of Aarhus, 2002.
16. B. Möller and G. Struth. Greedy-like algorithms in Kleene algebra. This volume.
17. I. Németi. Dynamic algebras of programs. In *Proc. FCT'81 — Fundamentals of Computation Theory*, volume 117 of *LNCS*, pages 281–291. Springer, 1981.
18. V. Pratt. Dynamic logic as a well-behaved fragment of relation algebras. In D. Pigozzi, editor, *Conference on Algebra and Computer Science*, volume 425 of *LNCS*, pages 77–110. Springer, 1988.
19. V. Pratt. Dynamic algebras: Examples, constructions, applications. *Studia Logica*, 50:571–605, 1991.
20. B. von Karger R. Berghammer and A. Wolf. Relation-algebraic derivation of spanning tree algorithms. In J. Jeuring, editor, *Mathematics of Program Construction*, volume 1422 of *LNCS*, pages 23–43. Springer, 1998.
21. J. N. Ravelo. Two graph algorithms derived. *Acta Informatica*, 36:489–510, 1999.
22. V. Trnkova and J. Reiterman. Dynamic algebras with tests. *J. Comput. System Sci.*, 35:229–242, 1987.