# Modal Kleene Algebra and Partial Correctness

Bernhard Möller Georg Struth*

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

**Abstract** Modal Kleene algebra is Kleene algebra enriched by forward and backward box and diamond operators. We formalize the symmetries of these operators as Galois connections and dualities. We study their properties in the associated semirings of operators. Modal Kleene algebra provides a unifying semantics for various program calculi and enhances efficient cross-theory reasoning in this class, often in a very concise state-free style. This claim is supported by novel algebraic soundness and completeness proofs for Hoare logic.

## 1 Introduction

Complex hardware and software development usually depends on many different models and formalisms. This calls for a unifying semantics and for calculi that enhance safe cross-theory reasoning. During the last decade, variants of Kleene algebra (KA) have emerged as foundational structures with widespread applications in computer science ranging from program and protocol analysis [3,12,22], program development [2,18] and compiler optimization [14] to rewriting theory [20] and concurrency control [3]. The development has been initialized by two seminal papers by Kozen, the first one providing a particularly useful and elegant axiomatization of KA as the algebra of regular events [11], the second one extending KA to Kleene algebra with tests (KAT) for modeling the usual constructs of sequential programming [12]. But although KAT subsumes propositional Hoare logic (PHL) [13], it seems not appropriate as a unifying core calculus, since it does not admit an explicit definition of modalities as they occur in many popular methods.

KAT has recently been enriched by simple equational axioms for abstract domain and codomain operations [4]. This Kleene algebra with domain (KAD) is more expressive than KAT. It does not only allow relational reasoning about hardware and software [4], it also subsumes propositional dynamic logic and supplies it with a natural algebraic semantics [7].

This motivates the following question: Is KAD suitable as a calculus for cross-theory reasoning and as a unifying semantics? Answering this question, however, requires further consideration of the modal aspects of KAD in general and its semantical impact for Hoare logic in particular[1].

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

[1] The relation between KAD and temporal logics will be the subject of another paper.

**Our Contributions.** First, we use the abstract image and preimage operations of KAD for defining forward and backward box and diamond operators as modal operators à la Jónsson and Tarski [10]. We show that these operators are related by two fundamental symmetries: Galois connections and dualities. The former serve as theorem generators, yielding a number of modal properties for free. The latter serve as theorem transformers, passing properties of one modal operator automatically to its relatives. We also develop further natural and interesting algebraic properties, including continuity of domain and codomain. Most of them immediately transfer to predicate transformer algebras.

Second, we study the algebra of modal operators over KAD, which under suitable conditions is again a Kleene algebra. This abstraction supports even more concise state-free modal reasoning and leads to further structural insight.

Third, we apply modal Kleene algebra by giving purely calculational algebraic proofs of soundness and relative completeness for PHL. We use this formalism both for a faithful encoding of Hoare's syntax and for modeling the standard weakest liberal precondition semantics. Our encoding and soundness proof — all inference rules of PHL are theorems in KAD — is more direct and concise than previous KAT-based ones [13]. In particular, when abstracted to the algebra of modal operators, the Hoare rules immediately reflect natural properties. Our novel algebraic proof of relative completeness is much shorter and more abstract, thus applicable to more models, than the standard ones (e.g. [1]). It exploits a Galois connection between forward boxes and backward diamonds that is beyond the expressiveness of most related modal formalisms.

These technical results support our claim that KAD may serve both as a calculus for cross-theory reasoning with various calculi for imperative programs and state transition systems and as a unifying semantics for modal, relational and further algebraic approaches. The economy of concepts in Kleene algebra imposes a discipline of thought which usually leads to simpler and more perspicuous proofs and to a larger class of application models than with alternative approaches, for instance relational algebra (cf. [19]) or temporal algebra [21], where some of our issues have also been treated. This is also interesting from a pedagogical point of view, since taxonomic knowledge about various structures and complex axiomatizations can be replaced by systematic knowledge about a few simple operations together with symmetries and abstraction techniques, a particular advantage of the algebraic approach. Finally, our results are of independent interest for the foundations of modalities.

In this extended abstract, we can only describe the main ideas of our approach. See [17] for a full technical treatment and [5] for a synopsis of related results on modal Kleene algebra and for further support for our claims.

**Outline.** The remainder is organized as follows: Section 2 introduces KAD and its basic properties. Section 3 introduces modal operators and the associated algebras of modal operators. Section 4 develops the basic calculus of modal operators. The syntax and semantics of Hoare logic and its soundness and completeness proofs in KAD are the subject of Section 5, Section 6 and Section 7. Section 8 contains a summary, a discussion of further results and an outlook.

## 2 Kleene Algebra with Domain

A *Kleene algebra* [11] is a structure $(K, +, \cdot, ^*, 0, 1)$ such that $(K, +, \cdot, 0, 1)$ is an (additively) idempotent semiring (an i-semiring) and $^*$ is a unary operation axiomatized by the identities and quasi-identities

$$1 + aa^* \leq a^*, \quad (*\text{-}1) \qquad b + ac \leq c \Rightarrow a^*b \leq c, \quad (*\text{-}3)$$
$$1 + a^*a \leq a^*, \quad (*\text{-}2) \qquad b + ca \leq c \Rightarrow ba^* \leq c, \quad (*\text{-}4)$$

for all $a, b, c \in K$ (the operation $\cdot$ is omitted here and in the sequel). If the structure satisfies $(*\text{-}1)$, $(*\text{-}2)$ and $(*\text{-}3)$, but not necessarily $(*\text{-}4)$, we call it a *left Kleene algebra*. It is called a *right Kleene algebra*, if $(*\text{-}1)$, $(*\text{-}2)$ and $(*\text{-}4)$, but not necessarily $(*\text{-}3)$ holds. The natural ordering $\leq$ on $K$ is defined by $a \leq b$ iff $a + b = b$. Models of Kleene algebra are relations under set union, relational composition and reflexive transitive closure, sets of regular languages (regular events) over some finite alphabet under the regular operations or programs under non-deterministic choice, sequential composition and finite iteration.

A *Boolean algebra* is a complemented distributive lattice. By overloading, we usually 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. The symbol $\neg$ denotes the operation of complementation. We will consistently use the letters $a, b, c \ldots$ for Kleenean elements and $p, q, r, \ldots$ for Boolean elements.

A *Kleene algebra with tests* [12] is a two-sorted structure $(K, B)$, where $K$ is a Kleene algebra and $B \subseteq K$ is a Boolean algebra such that the $B$ operations coincide with the restrictions of the $K$ operations to $B$. In particular, $p \leq 1$ for all $p \in B$. 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 $B$. All $p \in \mathsf{test}(K)$ satisfy $p^* = 1$. The class of Kleene algebras with tests is denoted by $\mathsf{KAT}$.

When a Kleenean element $a$ describes an action or abstract program and a test $p$ a proposition or assertion, the product $pa$ describes a restricted program that executes $a$ when the starting state satisfies assertion $p$ and aborts otherwise. Dually, $ap$ describes a restriction of $a$ in its possible result states. We now introduce an abstract domain operator that assigns to $a$ the test that describes precisely its enabling states.

A *Kleene algebra with domain* [4] is a structure $(K, \delta)$, where $K \in \mathsf{KAT}$ and the *domain operation* $\delta : K \to \mathsf{test}(K)$ satisfies for all $a, b \in K$ and $p \in \mathsf{test}(K)$

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

$\mathsf{KAD}$ denotes the class of Kleene algebras with domain.

Let us explain these axioms. Since $\delta(a) \leq 1$ by $\delta(a) \in \mathsf{test}(K)$, isotonicity of multiplication shows that (d1) can be strengthened to an equality expressing that restriction to the full domain is no restriction at all. Axiom (d1) means that after restriction the remaining domain must satisfy the restricting test. (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. It also ensures that the modal operators introduced below distribute through multiplication.

Moreover, (d1) is equivalent to one implication in each of the statements

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

that constitute elimination laws for $\delta$, while (d2) is equivalent to the other implications. (llp) says that $\delta(a)$ is the least left preserver of $a$. (gla) says that $\neg\delta(a)$ is the greatest left annihilator of $a$.

All domain axioms hold in the relational model, but (d1) and (d2) suffice for many applications, such as, for instance, proving soundness of propositional Hoare logic. Our completeness proof, however, depends on (d3). We will always explicitly mention where (d3) has to be used.

Because of (llp), domain is uniquely characterised by the two domain axioms. Moreover, if $\mathsf{test}(K)$ is complete then a domain operation always exists. If $\mathsf{test}(K)$ is not complete, this need not be the case.

Many natural properties follow from the axioms. Domain is fully strict ($\delta(a) = 0 \Leftrightarrow a = 0$), stable on tests ($\delta(p) = p$) and satisfies the import/export law ($\delta(pa) = p\,\delta(a)$). See [4] for further information.

Moreover, the Galois-like characterization (llp) implies that the domain operation satisfies a continuity property.

**Proposition 2.1.** *Domain commutes with all existing suprema in* KAD*; in particular, it is additive ($\delta(a+b) = \delta(a)+\delta(b)$) and isotone ($a \leq b \Rightarrow \delta(a) \leq \delta(b)$).*

*Proof.* Let $b = \sup(a : a \in A)$ exist for some set $A \subseteq K$. We must show that $\delta(b) = \sup(\delta(a) : a \in A)$. First, by isotonicity of domain, $\delta(b)$ is an upper bound of the set $\delta(A) = \{\delta(a) : a \in A\}$, since $b$ is an upper bound of $A$.

To show that $\delta(b)$ is the least upper bound of $\delta(A)$, let $p$ be an arbitrary upper bound of $\delta(A)$. Then for all $a \in A$, $\delta(a) \leq p \Leftrightarrow a \leq pa \Rightarrow a \leq pb$, by (llp). Hence $pb$ is an upper bound of $A$ and therefore $b \leq pb$. But by (llp) this is equivalent to $\delta(b) \leq p$. □

A codomain operation $\rho$ can easily be axiomatized as a domain operation on the opposite semiring. As usual in algebra, opposition just swaps the order of multiplication. An alternative definition uses the operation of converse, which can be axiomatized for $K \in \mathsf{KA}$ as follows. For all $a, b, p \in K$ with $p \leq 1$,

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

Consequently, $p^\circ = p$ and $a \leq b \Leftrightarrow a^\circ \leq b^\circ$. Codomain is defined by $\rho(a) = \delta(a^\circ)$.

## 3 Modalities

We now define various modal operators in KAD. Their names are justified, since they induce mappings on test algebras that form Boolean algebras with operators in the sense of Jónsson and Tarski. They can also be interpreted, respectively,

as disjunctive or conjunctive predicate transformers. This links KAD with the syntax and semantics of Hoare logic.

The first definition introduces forward and backward diamond operators in the standard way via abstract preimage and image.

$$|a\rangle p = \delta(ap), \quad (1) \qquad \langle a|p = \rho(pa). \quad (2)$$

Conversely therefore, $\delta(a) = |a\rangle 1$ and $\rho(a) = \langle a|1$. Forward and backward diamonds are duals with respect to converse.

$$|a\rangle p = \langle a^\circ|p, \qquad \langle a|p = |a^\circ\rangle p. \tag{3}$$

They are also related by an *exchange law*.

**Lemma 3.1.** *Let $K \in \mathsf{KAD}$. For all $a \in K$ and $p, q \in \mathsf{test}(K)$,*

$$|a\rangle p \leq \neg q \Leftrightarrow \langle a|q \leq \neg p. \tag{4}$$

*Proof.* Expanding the definitions of forward and backward diamonds and using (gla) we calculate $|a\rangle p \leq \neg q \Leftrightarrow qap \leq 0 \Leftrightarrow \langle a|q \leq \neg p$. □

Therefore, even in absence of converse, forward and backward diamond are interdefinable. Moreover, both operators are unique. Duality with respect to complementation transforms diamonds into boxes:

$$|a]p = \neg|a\rangle\neg p, \qquad [a|p = \neg\langle a|\neg p. \tag{5}$$

By (4) and (5), this symmetry can also be expressed by Galois connections.

**Lemma 3.2.** *Let $K \in \mathsf{KAD}$. For all $a \in K$, the operators $|a\rangle$, $\langle a|$ and $\langle a|$, $|a]$ are lower and upper adjoints of Galois connections. For all $p, q \in \mathsf{test}(K)$,*

$$|a\rangle p \leq q \Leftrightarrow p \leq [a|q, \qquad \langle a|p \leq q \Leftrightarrow p \leq |a]q. \tag{6}$$

Exploiting the symmetries further yields the dualities $|a]p = [a^\circ|p$ and $[a|p = |a^\circ]p$ and the exchange law $|a]p \leq \neg q \Leftrightarrow [a|q \leq \neg p$. In later sections, we will use these Galois connections as theorem generators and the dualities as theorem transformers. We write $\langle a\rangle p$ and and $[a]p$ if the direction does not matter.

Many modal properties can be expressed and calculated more succinctly in a point-free style in the operator semirings induced by the modal operators. While such structure-preserving abstractions are standard in algebra, they have no immediate logical analogues. See [17] for more information.

**Proposition 3.3.** *Let $\langle K\rangle$ be the set of all mappings $\lambda x.\langle a\rangle x$ on some $K \in \mathsf{KAD}$, where $a \in K$. Defining addition and multiplication on $\langle K\rangle$ by*

$$(\langle a\rangle + \langle b\rangle)(p) = \langle a\rangle p + \langle b\rangle p, \quad (7) \qquad (\langle a\rangle \cdot \langle b\rangle)(p) = \langle a\rangle(\langle b\rangle p), \quad (8)$$

*the structure $(\langle K\rangle, +, \cdot, \langle 0\rangle, \langle 1\rangle)$ is an i-semiring. Depending on whether $\langle .\rangle$ is $|.\rangle$ or $\langle .|$, we call it the* forward diamond semiring *or* backward diamond semiring.

The natural ordering on $\langle K\rangle$ is defined by point-wise lifting as

$$\langle a\rangle \leq \langle b\rangle \Leftrightarrow \forall p.\langle a\rangle p \leq \langle b\rangle p. \tag{9}$$

By duality with respect to complementation, also the structures $([K], \sqcap, \cdot, [0], [1])$ are i-semirings, the *forward* and *backward box semiring*, respectively. Here, $\sqcap$ is the lower bound operation on box operators defined by

$$([a] \sqcap [b])(p) = ([a]p)([b]p); \tag{10}$$

the natural ordering is lifted as for diamonds. This yields an interesting correspondence with disjunctive and conjunctive predicate transformer algebras.

Using the point-wise lifting we can write formulas like $\langle a\rangle + \langle b\rangle = \langle a+b\rangle$ and $([a] \sqcap [b]) = \langle a+b\rangle$ in a point-free style. We will strongly use point-free resoning in the following sections. This will yield shorter specifications and simpler and more concise proofs.

## 4 The Algebra of Modalities

We now develop the basic laws of an algebra of modal operators in KAD. We further investigate their symmetries in terms of Galois connections and of duality in order to derive further properties. But since our modal operators are not completely characterized by the symmetries, we also present properties that are based directly on domain and codomain. See [17] for a more technical discussion.

Expanding the definitions, we can show the following simple properties of the units of the operator semirings.

**Lemma 4.1.** *Let $K \in$ KAD and $p \in \mathsf{test}(K)$. Then $\langle 0\rangle p = 0 = \neg[0]p$ and $[1] = \langle 1\rangle$.*

The Galois connections (6) give us the following two theorems for free.

**Lemma 4.2.** *Let $K \in$ KAD. For all $a \in K$, we have the* cancellation laws

$$|a\rangle[a| \leq \langle 1\rangle \leq [a||a\rangle, \qquad \langle a||a] \leq \langle 1\rangle \leq |a]\langle a|. \tag{11}$$

**Proposition 4.3.** *Let $K \in$ KAD and $a \in K$. Then $\langle a\rangle$ and $[a]$ commute with all existing suprema and infima, respectively. If $\mathsf{test}(K)$ is a complete Boolean lattice then $\langle a\rangle$ is universally disjunctive and $[a]$ is universally conjunctive, that is, the operators commute with all suprema and infima, respectively.*

*Proof.* By Lemma 3.2, boxes and diamonds of KAD are upper and lower adjoints of a Galois connection. Then the results follow from general properties. □

As special cases we obtain, for all $a \in K$ and $p, q \in \mathsf{test}(K)$,

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

Consequently, $(\mathsf{test}(K), \{\langle a\rangle : a \in K\})$ and $(\mathsf{test}(K), \{[a] : a \in K\})$ are *Boolean algebras with operators* in the sense of Jónsson and Tarski [10]. This justifies calling our boxes and diamonds *modal operators*.

We now collect some further natural algebraic properties of modal operators. We restrict our attention to diamonds. Corresponding statements for boxes can immediately be inferred by duality.

**Lemma 4.4.** *Let $K \in \mathsf{KAD}$. For all $a, b \in K$ and $p, q \in \mathsf{test}(K)$,*

$$\langle a + b\rangle = \langle a\rangle + \langle b\rangle, \qquad (12) \qquad\qquad a \leq b \Rightarrow \langle a\rangle \leq \langle b\rangle, \qquad (15)$$

$$|ab\rangle \leq |a\rangle|b\rangle, \qquad (13) \qquad\qquad |paq\rangle = |p\rangle|a\rangle|q\rangle, \qquad (16)$$

$$\langle ab| \leq \langle b|\langle a|, \qquad (14) \qquad\qquad \langle paq| = \langle q|\langle a|\langle p|. \qquad (17)$$

The properties (13) and (14) can be proved using (d1) and (d2) only; since we additionally have (d3), they even become equalities. Spelling out (12) for box yields, for instance, $[a + b] = [a] \sqcap [b]$, while (13) yields $|a]|b] \leq |ab]$. Moreover, boxes are antitonic: $a \leq b$ implies $[b] \leq [a]$.

The following statements show that a star operation can be defined on a semiring of modal operators.

**Proposition 4.5.** *Let $|K\rangle$ be the forward diamond semiring over $K \in \mathsf{KAD}$. Defining a star on $|K\rangle$ by*

$$|a\rangle^*(p) = |a^*\rangle p, \qquad (18)$$

*for all $a \in K$ and $p \in \mathsf{test}(K)$ turns $|K\rangle$ into a left Kleene algebra.*

To see that ($*$-1)-($*$-3) hold in the forward diamond semiring $|K\rangle$, we use that that the identities $|1\rangle + |aa^*\rangle = |a^*\rangle$ and $|1\rangle + |a\rangle|a^*\rangle \geq |a^*\rangle$ have been shown in [4], whereas $|1\rangle + |a\rangle|a^*\rangle = |a^*\rangle$ follows using (d3). Moreover, we have the quasi-identity $p + |a\rangle q \leq q \Rightarrow |a^*\rangle p \leq q$ (see again [4]) and therefore also

$$|b\rangle + |a\rangle|c\rangle \leq |c\rangle \Rightarrow |a^*\rangle|b\rangle \leq |c\rangle. \qquad (19)$$

For $\langle K|$, we obtain a right Kleene algebra by similar arguments.

In case of a complete test algebra, we obtain a full Kleene algebra.

**Lemma 4.6.** *Let $K \in \mathsf{KAT}$. Then $\lambda x.p + x$ on $\mathsf{test}(K)$ commutes with all existing suprema and $\lambda x.px$ on $\mathsf{test}(K)$ commutes with all existing infima.*

**Proposition 4.7.** *Let $K \in \mathsf{KAD}$ and let $\mathsf{test}(K)$ be a complete Boolean lattice. Then for all $a \in K$, the operators $\langle a\rangle^*$ and $[a]^*$ exist. Moreover,*

$$\langle a\rangle^* = \sup(\langle a\rangle^i : i \geq 0), \qquad [a]^* = \inf([a]^i : i \geq 0).$$

This follows from Proposition 4.3, Lemma 4.6 and Kleene's fixed-point theorem.

**Proposition 4.8.** *Let $K \in \mathsf{KAD}$ with $\mathsf{test}(K)$ a complete Boolean lattice. Then the i-semiring $|K\rangle$ can uniquely be extended to a Kleene algebra.*

Instead of calculating with domain and modal operator laws, we can therefore calculate many modal properties simply in Kleene algebra at this higher level of abstraction (see below).

## 5 Hoare Logic

We now apply our results to obtain completely calculational algebraic soundness and completeness proofs for propositional Hoare logic. We first present the syntax and semantics of Hoare logic.

Let $\Phi$ be a set of *propositions* built from a set $\Pi$ with the usual Boolean connectives. Let $\Sigma$ be a set of *statements* defined by the following grammar from a set $\Gamma$ of atomic commands.

$$\Sigma ::= \mathsf{abort} \mid \mathsf{skip} \mid \Gamma \mid \Sigma\,;\,\Sigma \mid \ \mathsf{if}\ \Phi\ \mathsf{then}\ \Sigma\ \mathsf{else}\ \Sigma \mid \ \mathsf{while}\ \Phi\ \mathsf{do}\ \Sigma\,.$$

The basic formulas of Hoare logic are *partial correctness assertions* (PCAs) of the form $\{\phi\}\ \alpha\ \{\psi\}$, with $\phi, \psi \in \Phi$ (the *pre-* and *postcondition*) and $\alpha \in \Sigma$.

To define a semantics with respect to $\mathsf{KAD}$, let $K \in \mathsf{KAD}$. We assign to each propositional variable $\pi \in \Pi$ a test $[\![\pi]\!] \in \mathsf{test}(K)$ and to each atomic command $\gamma \in \Gamma$ a Kleenean element $[\![\gamma]\!] \in K$. Moreover, we assign 0 to $[\![\mathsf{abort}]\!]$ and 1 to $[\![\mathsf{skip}]\!]$. The remainder is the usual homomorphic extension.

$$[\![\phi \wedge \psi]\!] = [\![\phi]\!][\![\psi]\!], \tag{20}$$
$$[\![\neg\phi]\!] = \neg[\![\phi]\!], \tag{21}$$
$$[\![\alpha\,;\,\beta]\!] = [\![\alpha]\!][\![\beta]\!], \tag{22}$$
$$[\![\ \mathsf{if}\ \phi\ \mathsf{then}\ \alpha\ \mathsf{else}\ \beta]\!] = [\![\phi]\!][\![\alpha]\!] + \neg[\![\phi]\!][\![\beta]\!], \tag{23}$$
$$[\![\ \mathsf{while}\ \phi\ \mathsf{do}\ \alpha]\!] = ([\![\phi]\!][\![\alpha]\!])^*\neg[\![\phi]\!]. \tag{24}$$

We follow [13] in defining validity of formulas and PCAs. $\models \phi \Leftrightarrow [\![\phi]\!] = 1$, for all $\phi \in \Phi$. In particular, $\models \phi \to \psi \Leftrightarrow [\![\phi]\!] \leq [\![\psi]\!]$. Moreover,

$$\models \{\phi\}\ \alpha\ \{\psi\} \Leftrightarrow [\![\phi]\!][\![\alpha]\!]\neg[\![\psi]\!] \leq 0.$$

Using (gla) and Boolean algebra, we rewrite this definition more intuitively as

$$\models \{\phi\}\ \alpha\ \{\psi\} \Leftrightarrow \langle [\![\alpha]\!] | [\![\phi]\!] \leq [\![\psi]\!].$$

In the relational model of $\mathsf{KAD}$, the expression $\langle [\![\alpha]\!] | [\![\phi]\!]$ denotes the set of all states that can be reached from states in $[\![\phi]\!]$ through $[\![\alpha]\!]$. Therefore, the formula $\langle [\![\phi]\!] | [\![\alpha]\!] \leq [\![\psi]\!]$ is indeed a faithful translation of $\{\phi\}\ \alpha\ \{\psi\}$ that, by the exchange law of Lemma 3.1, is consistent with the standard $\mathsf{wlp}$-semantics (see also Section 7 for further details).

To shorten notation, we will henceforth confuse syntax and semantics and use Kleene algebra notation everywhere. Thus we express validity of a PCA as

$$\models \{p\}\ a\ \{q\} \Leftrightarrow \langle a | p \leq q. \tag{25}$$

The Hoare calculus for partial correctness of deterministic sequential programs consists of the following inference rules.

(Abort) $$\{p\}\ \mathsf{abort}\ \{q\},$$

(Skip) $$\{p\}\ \mathsf{skip}\ \{p\},$$

(Assignment) $$\{p[e/x]\}\ x := e\ \{p\},$$

(Composition) $$\frac{\{p\}\ a\ \{q\} \quad \{q\}\ b\ \{r\}}{\{p\}\ a\,;\,b\ \{r\}},$$

(Conditional) $$\frac{\{p \wedge q\}\ a\ \{r\} \quad \{\neg p \wedge q\}\ b\ \{r\}}{\{q\}\ \ \mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b\ \{r\}},$$

(While) $$\frac{\{p \wedge q\}\ a\ \{q\}}{\{q\}\ \ \mathsf{while}\ p\ \mathsf{do}\ a\ \{\neg p \wedge q\}},$$

(Weakening) $$\frac{p_1 \to p \quad \{p\}\ a\ \{q\} \quad q \to q_1}{\{p_1\}\ a\ \{q_1\}}.$$

A rule with premises $P_1, \cdots, P_n$ and conclusion $P$ is *sound* if $P_1, \ldots, P_n \models P$. Derivations are defined in the standard way.

(Assignment) is a non-propositional inference rule that deals with the internal structure of states. We therefore do not encode it directly into our framework, but instead use the set $\Gamma$ of atomic commands as a parameter in our approach. The requirement of sufficient expressiveness on $\Gamma$ that ensures completeness of the calculus will be discussed in Section 7. Following [13], we call this abstract form of Hoare logic *propositional Hoare logic* (PHL).

## 6 Soundness of Propositional Hoare Logic

We now prove soundness of PHL with respect to the KAD-semantics. More precisely, we show that the encoded inference rules of PHL are theorems of KAD. This subsumption is a popular exercise for many logics and algebras of programs, among them propositional dynamic logic [8] and KAT [13], which are both subsumed by KAD. However our result is interesting for two reasons, a syntactic and a semantic one. First, our encoding of PHL is more simple, abstract and direct, and Hoare-style reasoning in KAD is more flexible than in previous approaches. However we do not sacrifice algorithmic power. Second, the properties of our modal operators defined in terms of abstract image and preimage operations reflect precisely those of the standard partial correctness semantics [1,15] and show that KAD provides a natural abstract algebraic semantics for PHL.

A first point-wise encoding of the soundness conditions for the Hoare rules is rather straightforward from (25). (Composition), for instance, becomes

$$\langle a|p \leq q \wedge \langle b|q \leq r \Rightarrow \langle ab|p \leq r.$$

This is a theorem of KAD, since

$$\langle ab|p \leq \langle b|\langle a|p \leq \langle b|q \leq r$$

by (decomposition). As a second example, (While) becomes

$$\langle a|(pq) \leq q \Rightarrow \langle (pa)^*\neg p|q \leq \neg pq.$$

This is also a theorem of KAD. Using (induction), we calculate

$$\langle a|(pq) \leq q \Rightarrow \langle (pa)^*|q \leq q \Rightarrow \neg p(\langle (pa)^*|q) \leq \neg pq \Leftrightarrow \langle (pa)^*\neg p|q \leq \neg pq.$$

Point-wise encodings and proofs for the remaining PHL-rules are similar. Consequently, soundness of PHL can be proved literally in one line per inference rule from natural properties of KAD. In KAT, (Composition), for instance, must be encoded quite indirectly as

$$pa \leq aq \wedge qb \leq br \Rightarrow pab \leq abr$$

and the proof of theoremhood is based on rather syntactic commutation properties (cf. [13]). We can obtain this encoding also in KAD, using (llp). More generally, (llp) and (gla) provide translations of all PHL-rules into KAT and, using a result from [9], connect validity with respect to PHL with PSPACE automata-theoretic decision procedures. See [17] for a deeper discussion.

Compared with standard textbooks (cf. [1,15]), our proof is about ten times shorter. In addition, the textbook proofs are only semi-formal, since many logical and set-theoretic assumptions are left implicit. A complete formalization would produce further overhead.

We now give another point-free soundness proof of PHL in KAD that is even more abstract and concise. In particular, the properties expressed by the Hoare rules now correspond to natural algebraic properties of the algebra of modal operators.

**Proposition 6.1.** *Let $K \in$ KAD. Then the soundness conditions for the inference rules of* PHL *can be encoded as follows. For all $a, b \in K$ and $p \in \mathsf{test}(K)$,*

| | |
|---|---|
| *(Abort)* | $\langle 0| \leq \langle q|,$ |
| *(Skip)* | $\langle 1| \leq \langle 1|,$ |
| *(Composition)* | $\langle ab| \leq \langle b|\langle a|,$ |
| *(Conditional)* | $\langle pa + \neg pb| \leq \langle a|\langle p| + \langle b|\langle \neg p|,$ |
| *(While)* | $\langle a|\langle p| \leq \langle 1| \Rightarrow \langle \neg p|\langle (pa)^*| \leq \langle \neg p|,$ |
| *(Weakening)* | $\langle p_1| \leq \langle p| \wedge \langle p|\langle a| \leq \langle q| \wedge \langle q| \leq \langle q_1| \Rightarrow \langle q_1|\langle a| \leq \langle q_1|.$ |

The point-free encoding is derived from the point-wise one using the *principle of indirect inequality*: $p \leq q$ iff $q \leq r$ implies $p \leq r$ for all $r$.

(Skip) and (Abort) now reflect natural or even trivial semiring properties. (Conditional) expresses (additivity) and (import/export) of the operator semiring, (While) expresses a variant of (induction). (Composition) expresses (decomposition); it becomes an equality when (d3) is assumed on the underlying KAD. (Weakening) is the only rule where at first sight, nothing has be gained by the lifting. However, its correctness proof can now be based entirely on semiring properties, instead of expanding to properties of domain. These facts are immediately reflected by the following subsumption result.

**Theorem 6.2.** *The point-free encodings of the* PHL*-rules are theorems in* KAD*.*

*Proof.* The point-free variants of (Abort) and (Skip) are trivial consequences of Lemma 4.1. The point-free variant of (Composition) is nothing but (14). The point-free variant of (Conditional) is evident from (12) and (14). (While) follows immediately from (19) and isotonicity. (Weakening) holds by isotonicity of multiplication in i-semirings. □

**Theorem 6.3.** PHL *is sound with respect to the* KAD *semantics.*

*Proof.* By induction on the structure of PHL derivations, using Theorem 6.2. □

As observed in [13], all Horn clauses built from PCAs in PHL that are valid with respect to the standard semantics are theorems of KAT; whence a fortiori of KAD. PHL is too weak to derive all such formulas. Consequently, KAT and KAD have not only the derivable, but also the admissible rules of PHL as theorems.

## 7 Completeness of Propositional Hoare Logic

In this section we provide a novel algebraic completeness proof for the inference rules of PHL, using modal Kleene algebra as a semantics. Conventional completeness proofs use the *weakest liberal precondition* semantics. For a set $S$ of program states, a relational program $P \subseteq S \times S$ and set $T \subseteq S$ of target states one defines

$$\mathsf{wlp}(P,T) = \{s \in S : P(s) \subseteq T\}, \tag{26}$$

where $P(s)$ is the image of $s$ under $P$. Equivalently, $\mathsf{wlp}(P,T)$ is the largest subset $U \subseteq S$ such that $P(U) \subseteq T$. In a modal setting the wlp-operator can then of course be identified with the forward box operator. Confusing again syntax and semantics, the Galois connection (6) and (25) immediately imply that

$$\models \{p\}\ \alpha\ \{q\} \ \Leftrightarrow\ p \leq |a]q. \tag{27}$$

On the one hand, this Galois connection connects PHL syntax and semantics in a very concise way. One the other hand, we get the entire wlp-calculus for free by dualizing our results from Section 4.

For the standard completeness proofs (see e.g. [1]) it is crucial that the underlying assertion language is sufficiently expressive. This implies that for all

statements $\alpha \in \Sigma$ and all postconditions $\psi \in \Phi$ there is an assertion $\phi \in \Phi$ that expresses the weakest liberal precondition for $\psi$ under $\alpha$, i.e.,

$$[\![\phi]\!] = \mathsf{wlp}([\![\alpha]\!], [\![\psi]\!]). \tag{28}$$

Using (28) we can continue working semantically in KAD. We extend the original calculus so that all predicates are denoted by propositional variables. Completeness of this extension will then imply completeness of the former calculus.

For every atomic command $\gamma \in \Gamma$ and test $q$ we add an axiom

$$\{|g]q\}\ g\ \{q\}, \tag{29}$$

where $g = [\![\gamma]\!]$. (Assignment) has precisely this form.

Before the completeness proof, we state some technical properties of boxes in connection with conditionals and loops. Logical variants appear in [1].

**Proposition 7.1.** *Let $K \in \mathsf{KAD}$. Let $a, b, c, w \in K$ and $p, q \in \mathsf{test}(K)$.*

*(i) For $c =$ $\mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b$,*

$$p\,(|c]q) = p\,(|a]q), \tag{30} \qquad \neg p\,(|c]q) = \neg p\,(|b]q). \tag{31}$$

*(ii) For $w =$ $\mathsf{while}\ q\ \mathsf{do}\ a$,*

$$p\,(|w]q) = p|a](|w]q), \tag{32} \qquad \neg p\,(|w]q) \leq q. \tag{33}$$

The proofs need a few lines of calculus using the properties from Section 4. Now we can proceed, as for instance in [1].

**Lemma 7.2.** *Let $K \in \mathsf{KAD}$. For all $a \in K$ that are denotable by* PHL *commands and all $q \in \mathsf{test}(K)$, the PCA $\{|a]q\}\ a\ \{q\}$ is derivable in* PHL.

*Proof.* Let $\vdash \{p\}\ a\ \{q\}$ denote that $\{p\}\ a\ \{q\}$ is derivable in PHL. The proof is by induction on the structure of command $a$.

(i) $a$ is either skip or abort or denotes an atomic command. Then the claim is trivial, since PHL contains the respective PCA as an axiom.

(ii) Let $a = b$ and $c = bc$. By the induction hypothesis,

$$\vdash \{|b](|c]q)\}\ b\ \{|c]q\}, \qquad \vdash \{|c]q\}\ c\ \{q\}.$$

Now (Composition) shows $\vdash \{|b](|c]q)\}\ bc\ \{q\}$, which by the additional assumption of (d3) and the dual of (13) is equivalent to $\vdash \{|bc]q\}\ bc\ \{q\}$. Note that this is the only part of the proof where (d3) is used.

(iii) Let $a =$ $\mathsf{if}\ p\ \mathsf{then}\ b\ \mathsf{else}\ c$. By the induction hypothesis,

$$\vdash \{|b]q\}\ b\ \{q\}, \qquad \vdash \{|c]q\}\ c\ \{q\}.$$

Hence, by (Weakening), also

$$\vdash \{p(|b]q)\}\ b\ \{q\}, \qquad \vdash \{\neg p(|b]q)\}\ b\ \{q\}.$$

By (30) and (31) these statements are equivalent to

$$\vdash \{p(|a]q)\}\ b\ \{q\}, \qquad \vdash \{\neg p(|a]q)\}\ c\ \{q\},$$

so that (Conditional) shows the claim.

(iv) Let $a =$ while $p$ do $b$. Let $c = |a]q$. By the induction hypothesis,

$$\vdash \{|a]c\}\ b\ \{c\}.$$

By (32) this is equivalent to $\vdash \{pc\}\ b\ \{c\}$. (While) shows that $\vdash \{c\}\ a\ \{\neg pc\}$ and (33) and (Weakening) yield $\vdash \{|a]q\}\ a\ \{q\}$, as required, □

We are now prepared for the main theorem of this section.

**Theorem 7.3.** PHL *is relatively complete for the partial correctness semantics of deterministic programs in* KAD.

*Proof.* We must show that $\models \{p\}\ a\ \{q\}$ implies $\vdash \{p\}\ a\ \{q\}$. This follows from (27), Lemma 7.2 and (Weakening). □

Alternatively, we could also use our encodings of PCAs in KAD in the completeness proof. We could write $\langle a|_{\vdash} p \leq q$ instead of $\vdash \{p\}\ a\ \{q\}$ to further stress the fact that our proof is entirely in Kleene algebra and to denote that only the encodings of PHL-rules are allowed for transforming the indexed diamonds. Using this encoding, the statement $\langle a|_{\vdash}(|a]p) \leq p$, or even $\langle a|_{\vdash}|a] \leq |1]$, looks very much like a cancellation property of a Galois connection. This fact certainly deserves further consideration.

## 8 Conclusion and Outlook

We have investigated Kleene algebra with domain as a modal Kleene algebra. Modal operators have been defined as abstractions of relational image and preimage operations. Their symmetries have been formalized in terms of Galois connections and dualities. We have also studied the semirings induced by the modal operators. This additional level of abstraction yields very concise state-free specifications and proofs of modal properties.

Our results show the usefulness of modal Kleene algebra both as a calculus for cross-theoretic reasoning with various calculi for imperative programs and state transition systems, and as a unifying semantics for modal, relational and further algebraic approaches. While an analogous claim has already been verified for relational approaches [4] and for propositional dynamic logic [7], we provide algebraic soundness and completeness proofs for Hoare logic that use modal Kleene algebra both at the syntactic and at the semantic side. In particular the state-free soundness proof and the completeness proof exhibit very nicely the natural algebraic properties that are implicit in the partial correctness assertions and Hoare rules.

Compared with other formalisms, modal Kleene algebra is also very flexible. E.g., in [17], we show that several inference rules that are derivable in PHL are theorems of modal Kleene algebra. There, it is not always preferable to reason entirely using the modalities. Especially when the rules encode commutativity conditions, the subtheory KAT may provide more direct proofs.

It is also interesting to investigate in how far modalities can be eliminated from KAD formulas. In combination with hypothesis elimination techniques, we obtain a linear translation of certain KAD-expression into identities over KAT, whose validity can be decided by automata in PSPACE [17].

Modal Kleene algebra also subsumes Hoare logic for programs with bounded nondeterminism. Guarded commands, for instance, can be encoded as

$$\mathsf{if}\ p_1 \to a_1 \,[]\, \cdots \,[]\, p_n \to a_n\ \mathsf{fi}\ = \sup(p_i a_i : 1 \leq i \leq n),$$
$$\mathsf{do}\, p_1 \to a_1 \,[]\, \cdots \,[]\, p_n \to a_n\, \mathsf{od} = (\sup(p_i a_i : 1 \leq i \leq n))^* \inf(\neg p_i : 1 \leq i \leq n).$$

Program termination can also be modelled in modal Kleene algebra [4,6]. This suggests extending our approach to Hoare logics for total correctness. Moreover, since modal Kleene algebra allows the specification of syntax and relational semantics of modal calculi in one single formalism, one can use it to develop a calculational modal correspondence theory; see [4,5,18] for first results. To further establish modal Kleene algebra as a unifying framework, we also plan to consider temporal logics like LTL or CTL; for LTL an account of this along the lines of [21] is contained in [5]. Recently, the modal operators have also been incorporated into *Lazy Kleene Algebra* [16], a framework that extends the work of Cohen [3] and von Wright [22] and is designed to deal with both terminating and non-terminating computations and hence also with reactive systems. It is a challenging task to apply the framework of modal Kleene algebra to other problems and structures for further extending its practical relevance.

**Acknowledgment:** We would like to thank Jules Desharnais, Thorsten Ehm and Joakim von Wright for valuable discussions and comments.

## References

1. K.-R. Apt and E.-R. Olderog. *Verification of Sequential and Concurrent Programs.* Springer, 2nd edition, 1997.
2. K. Clenaghan. Calculational graph algorithmics: Reconciling two approaches with dynamic algebra. Technical Report CS-R9518, CWI, Amsterdam, 1994.
3. E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *Proc. of Mathematics of Program Construction, 5th International Conference, MPC 2000*, volume 1837 of *LNCS*, pages 45–59. Springer, 2000.
4. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. Technical Report 2003-07, Universität Augsburg, Institut für Informatik, 2003.
5. J. Desharnais, B. Möller, and G. Struth. Applications of modal Kleene algebra — a survey. Technical Report DIUL-RR-0401, Département d'informatique et de génie logiciel, Université Laval, Québec, 2004.

6. J. Desharnais, B. Möller, and G. Struth. Termination in modal Kleene algebra. Technical Report 2004-04, Universität Augsburg, Institut für Informatik, 2004.
7. T. Ehm, B. Möller, and G. Struth. Kleene modules. In R. Berghammer and B. Möller, editors, *Proc. 7th Seminar on Relational Methods in Computer Science and 2nd International Workshop on Applications of Kleene Algebra*, volume 3051 of *LNCS*. Springer, 2004. (to appear).
8. J. M. Fischer and R. F. Ladner. Propositional dynamic logic of regular programs. *J. Comput. System Sci.*, 18(2):194–211, 1979.
9. C. Hardin and D. Kozen. On the elimination of hypotheses in Kleene algebra with tests. Technical Report 2002-1879, Computer Science Department, Cornell University, October 2002.
10. B. Jónsson and A. Tarski. Boolean algebras with operators, Part I. *American Journal of Mathematics*, 73:891–939, 1951.
11. D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.
12. D. Kozen. Kleene algebra with tests. *Trans. Programming Languages and Systems*, 19(3):427–443, 1997.
13. D. Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1(1):60–76, 2001.
14. D. Kozen and M.-C. Patron. Certification of compiler optimizations using Kleene algebra with tests. In J. Lloyd, editor, *1st International Conference on Computational Logic*, volume 1861 of *LNCS*, pages 568–582. Springer, 2000.
15. J. Loeckx and K. Sieber. *The Foundations of Program Verification.* Wiley Teubner, 2nd edition, 1987.
16. B. Möller. Lazy Kleene algebra. In D. Kozen, editor, *Proc. of Mathematics of Program Construction, 7th International Conference, MPC 2004*, LNCS. Springer, 2004. (to appear). Preliminary version: Report No. 2003-17, Institut für Informatik, Universität Augsburg, December 2003.
17. B. Möller and G. Struth. Modal Kleene algebra and partial correctness. Technical Report 2003-08, Universität Augsburg, Institut für Informatik, 2003.
18. B. Möller and G. Struth. Greedy-like algorithms in modal Kleene algebra. In R. Berghammer and B. Möller, editors, *Proc. 7th Seminar on Relational Methods in Computer Science and 2nd International Workshop on Applications of Kleene Algebra*, volume 3051 of *LNCS*. Springer, 2004. (to appear).
19. G. W. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists.* EATCS Monographs on Theoretical Computer Science. Springer, 1993.
20. 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 *LNCS*, pages 276–290. Springer, 2002.
21. B. von Karger. Temporal algebra. *Mathematical Structures in Computer Science*, 8(3):277–320, 1998.
22. J. von Wright. From Kleene algebra to refinement algebra. In B. Möller and E. Boiten, editors, *Mathematics of Program Construction, 6th International Conference, MPC 2002*, volume 2386 of *LNCS*, pages 233–262. Springer, 2002.