Algebras of Modal Operators and Partial Correctness

Bernhard Möller [a,*] Georg Struth [b]

[a] *Institut für Informatik, Universität Augsburg, Universitätsstr. 14, D-86135 Augsburg, Germany*

[b] *Fakultät für Informatik, Universität der Bundeswehr München, D-85577 Neubiberg, Germany*

Abstract

Modal Kleene algebras are Kleene algebras enriched by forward and backward box and diamond operators. We formalise the symmetries of these operators as Galois connections, complemetarities and dualities. We study their properties in the associated operator algebras and show that the axioms of relation algebra are theorems at the operator level. Modal Kleene algebras provide a unifying semantics for various program calculi and enhances efficient cross-theory reasoning in this class, often in a very concise pointfree style. This claim is supported by novel algebraic soundness and completeness proofs for Hoare logic and by connecting this formalism with an algebraic decision procedure.

Key words: Semirings, Kleene algebra, modal operators, partial correctness, Hoare logic.

1 Introduction

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 fundamental structures of computer science with widespread applications. The model class contains languages, relations, formal power series, matrices, traces and paths. The development of Kleene algebra

* Corresponding author.
Email addresses: moeller@informatik.uni-augsburg.de (Bernhard Möller), struth@informatik.unibw-muenchen.de (Georg Struth).

has been decisively influenced by two seminal papers by Kozen, the first one providing a particularly useful and elegant axiomatization of KA as the algebra of regular events [15], the second one extending KA to Kleene algebra with tests (KAT) for modeling the usual constructs of sequential programming [16]. But although KAT subsumes propositional Hoare logic (PHL) [17], it is not rich enough to 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 [9]. This Kleene algebra with domain (KAD) is more expressive than KAT. It does not only allow relational reasoning about hardware and software [9], it also subsumes propositional dynamic logic and supplies it with a natural algebraic semantics [10]. The full potential of the modal operators that are definable in KAD via preimage and image operations, however, has not been sufficiently exploited so far. This concerns both the structure theory of modalities and applications beyond dynamic logic.

The present paper considers KAD as *modal Kleene algebras*. It studies the symmetries and dualities of modal operators and develops their algebra. As a sample application, it provides algebraic partial correctness semantics in the wlp style and encodings of the rules of Hoare logic. The connection to total correctness semantics in wp style is set up in the successor paper [22]. The relation to temporal logics, such as Hennessy-Milner logic, LTL, CTL and CTL* will be the subject of another paper(see [7] for preliminary results). Altogether, we show that modal Kleene algebras close the gap between algebras such as KAT and various modal and predicate transformer formalisms.

Our Contributions.

- Using the domain and codomain operations of KAD we define forward and backward box and diamond operators as modal operators à la Jónsson and Tarski [13]. We show that these operators are related by fundamental symmetries in the form of Galois connections and complementarities and by natural algebraic dualities. The Galois connections and complementarities serve as theorem generators, yielding a number of modal properties for free. The dualities serve as theorem transformers, passing properties of one modal operator automatically to its relatives. We also develop further natural algebraic properties, including complete additivity of domain and codomain and covariance and contravariance properties of forward and backward operators, most of which transfer to predicate transformer algebras.
- We study the algebra of modal operators in modal Kleene algebras, which form again certain Kleene algebras and certain lattice-ordered monoids. We also show that all axioms of relation algebra are theorems of modal Kleene algebra at the operator level, including the Schröder and Dedekind law. In particular, meet, complementation, conversion and residuals can be defined

at the operator level. The abstraction to the operator level thus introduces a very rich algebraic structure. It supports concise pointfree modal reasoning and leads to further structural insight. The Galois connections at the test level lift nicely to the operator level, where they admit, a.o., cancellation and shunting rules that are beyond the expressiveness of most modal formalisms.

- We apply modal Kleene algebra in the context of partial correctness by giving purely calculational proofs of soundness and relative completeness for (propositional) Hoare logic. We provide a faithful encoding of Hoare's syntax and model the standard weakest liberal precondition semantics. Our encoding and soundness proof — all inference rules of PHL are theorems in KAD — is simpler and more direct than a previous KAT-based one [17]. In particular, when abstracted to the algebra of modal operators, the Hoare rules immediately reflect natural algebraic properties. Our novel algebraic proof of relative completeness is much shorter and more abstract, thus applicable to more models, than the standard ones.
- We provide a novel algebraic decision procedure for propositional Hoare logic and, more generally, for the class of valid Hoare formulas. We also provide a decision procedure for that fragment of modal Kleene algebra that is most interesting for program analysis.

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 alternative approaches, for instance relational algebra [25] or temporal algebra [26], where some of our issues have also been treated. Finally, our results are of independent interest for the foundations of modalities. See [7] for a synopsis of related results on modal Kleene algebra and for further support for our claims. The present paper is an extension of [21] presented at AMAST 2004.

2 Kleene Algebra with Domain

A *semiring* is a structure $(S, +, \cdot, 0, 1)$ such that $(S, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid, multiplication distributes over addition from the left and right and $a0 = 0 = 0a$ holds for all $a \in S$. A semiring is *idempotent* if addition is, that is, $a + a = a$ holds for all $a \in S$.

Two properties are important here. First, every idempotent semiring admits a natural ordering defined by $a \leq b$ iff $a + b = b$, for all $a, b \in S$. It is, up to isomorphism, the only ordering with least element 0 for which addition and multiplication are isotone. The natural ordering turns $(S, +)$ into a semilattice.

Second, every semiring S induces an *opposite* semiring S^{op} in which the order of multiplication is swapped. For every statement about semirings there is a dual statement, obtained by opposition, that holds in its opposite.

The structure $(K, ^*)$ is a *left-inductive Kleene algebra* if K is an idempotent semiring and * is a unary operation that satisfies the following *star unfold* laws and *star induction* laws. For all $a, b, c \in K$,

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

It is *a right-inductive Kleene algebra* if it satisfies the unfold laws and the opposite induction laws. It is a *Kleene algebra* [15] if it is both left-inductive and right-inductive. The star is also isotone with respect to the natural ordering. Models of Kleene algebra are relations under union, relational composition and reflexive transitive closure, sets of regular languages (regular events) over some finite alphabet under the regular operations or programs under nondeterministic choice, sequential composition and finite iteration.

As usual, a *Boolean algebra* is a complemented distributive lattice. By overloading, we often 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 symbols $\neg$, $-$ and $\rightarrow$ denote complementation, relative complementation and Boolean implication. We will consistently use the letters $a, b, c \ldots$ for Kleenean elements and $p, q, r, \ldots$ for Boolean elements. We will freely use the standard laws of Boolean algebra. In particular, relative complementation and Boolean complementation satisfy the Galois connections (c.f. the following section)

$$p - q \leq r \Leftrightarrow p \leq q + r \qquad \text{and} \qquad pq \leq r \Leftrightarrow p \leq q \rightarrow r.$$

A *test semiring* is a two-sorted structure (S, B), where S is an idempotent semiring and B a Boolean algebra that is embedded into S such that zero is sent to zero, one to one, join to addition and meet to multiplication. The Boolean operations are the restrictions of the semiring operations to B. In general, B contains only a subset of the elements below 1 in S, since not all of these need be multiplicatively idempotent. We call elements of B *tests* and write $\mathsf{test}(S)$ instead of B. A test semiring is a *Kleene algebra with tests* [16] if the semiring is also a Kleene algebra. The class of Kleene algebras with tests is denoted by KAT. All tests p satisfy $p^* = 1$.

When a semiring 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 starting states. A *domain semiring* [9] is a structure

(S, δ), where S is a test semiring and the *domain operation* $\delta : S \to \mathsf{test}(S)$ satisfies for all $a, b \in S$ and $p \in \mathsf{test}(S)$

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

A domain semiring is a *Kleene algebra with domain* if it is also a Kleene algebra. In particular, no axioms for the interaction of domain and the star are required. The class of Kleene algebras with domain is denoted by KAD.

Let us explain these axioms. Axiom (d1) states that restricting an action to its domain is no restriction at all. Axiom (d2) means that the domain of an action that is restricted in its starting states respects this restriction. Axiom (d3), which is called *locality axiom*, states that the domain of ab is entirely determined by the restriction of a by $\delta(b)$ in its result states; information about the inner structure or the "far end" of b is not needed.

All three 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 usually explicitly mention where (d3) has to be used. Therefore we speak of *predomain semiring* and a*Kleene algebra with predomain* if only (d1) and (d2), but not necessarily (d3), hold.

3 Some Properties of Domain

It has been shown in [9] that (d1) is equivalent to the implication ($\Rightarrow$) in each of the properties

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

while (d2) is equivalent to the converse implication ($\Leftarrow$). These properties provide elimination laws for (pre)domain, but also characterize it in an intuitive way as least left preserver (llp), i.e., as the least element of the set $\{p : a \leq pa\}$, and its complement as greatest left annihilator (gla), i.e. as the greatest element of the set $\{p : pa \leq 0\}$. Since least and greatest elements are unique in a partial order, domain is uniquely defined when it exists. A necessary condition for existence of domain is that the set of left preservers has an infimum and the set of left annihilators has a supremum.

A standard example of a non-complete Boolean algebra is given as follows (c.f. [3], p.113). Let A be the powerset algebra of some countable set S and let I be the lattice-theoretic ideal of all finite subsets of S. The associated congruence identifies sets that differ only at finitely many elements. Then the epimorphic image A/I is a Boolean algebra that is not complete in the very

strong sense that *no* infinite joins exist, since sets in an infinite set cannot be made equal by adjoining finitely many elements. This algebra can be interpreted as a Kleene algebra with tests in which all elements are tests.

Lemma 3.1 *Some test semirings do not admit a domain operation.*

An interesting class of algebras where domain always exists are the *Boolean quantales*, where the carrier set S is a complete Boolean algebra and composition $\cdot$ is completely additive (see [6] for the proof). This covers, a.o., the case of relation and trace algebras.

Many natural properties of domain follow from the axioms. First, (d1) can be strengthened to the identity $a = \delta(a)a$. Second, (d2) is equivalent to the identity $\delta(pa) = p\delta(a)$. Third, the order dual of (d3) holds, that is, $\delta(ab) \leq \delta(a\delta(b))$ and therefore the identitiy $\delta(ab) = \delta(a\delta(b))$ in the presence of (d3). Fourth, domain is *strict* and *additive*, that is, $\delta(a) = 0 \Leftrightarrow a = 0$ and $\delta(a+b) = \delta(a) + \delta(b)$ and, as a consequence of additivity, it is also isotone: $a \leq b \Rightarrow \delta(a) \leq \delta(b)$. Fifth, domain preserves tests, that is, $\delta(p) = p$. Sixth, there is an interesting interaction of domain with star. We have $\delta(a^*) = 1$ for all a in the Kleene algebra. In presence of tests there are laws $p + \delta(aa^*p) = \delta(a^*p)$ and $p + \delta(a^*ap) = \delta(a^*p)$, which become test-level *star unfold* laws

$$p + \delta(a\delta(a^*p)) = \delta(a^*p) \qquad \text{and} \qquad p + \delta(a^*\delta(ap)) = \delta(a^*p)$$

in the presence of (d3). Moreover, there is a test-level *star induction* law

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

It is equivalent to $\delta(ap) \leq p \Rightarrow \delta(a^*p) \leq p$ and to the identity $\delta(a^*p) - p \leq \delta(a(\delta(p) - p)$. See [9] for further information and [14,20] for counterexamples to right induction.

Additivity of domain can be further strenghtened. We call a function f on a semi-lattice L *completely additive* if it preserves all existing suprema, that is, $f(\sup(A)) = \sup(f(a) : a \in A)$ whenever $\sup(A : A \subseteq L)$ exists.

Proposition 3.2 *The domain operation is completely additive.*

PROOF. Let S be a domain semiring. Let $b = \sup(a : a \in A)$ exist for some set $A \subseteq S$. 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) and the definition of b. Hence pb is an upper bound of A and therefore $b \leq pb$. By (llp) this is equivalent to $\delta(b) \leq p$. □

It follows that (pre)domain preserves all suprema when the test algebra is complete. This has interesting consequences that we exploit in further sections.

A codomain operation ρ can easily be axiomatized as a domain operation on the opposite semiring. Alternatively, one can use the operation $^\circ$ of conversion, which can be axiomatized for $K \in \mathsf{KA}$ as follows. For all $a, b, p \in K$ with $p \leq 1$,

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

Hence $p^\circ = p$ and $a \leq b \Leftrightarrow a^\circ \leq b^\circ$. Codomain is then defined as $\rho(a) = \delta(a^\circ)$. Hence the equational axioms for codomain are duals with respect to opposition of those for domain, so that duals of (llp) and (gla) hold for codomain.

4 Galois Connections and Conjugation

In this section we briefly review two algebraic concepts that will capture fundamental symmetries of modal operators: Galois connections and conjugation. Galois connections have been advocated in computer science by Cousot [5] and Backhouse [2]. Conjugation has already been investigated by Jónsson and Tarski [13] in their seminal paper on Boolean algebras with operators. A description of certain modal algebras in terms of Galois connections has been given before by von Karger [26]. The two approaches are essentially equivalent, but of different convenience in different situations. By using these concepts, many properties of modal operators can be derived in a generic way. This is in contrast to the logical approach where complex individual axiom systems must be used for formalizing different modal logics.

Two endofunctions f and g on some Boolean algebra B are called *conjugate* if, for all $x, y \in B$,

$$f(x)y = 0 \Leftrightarrow g(y)x = 0. \tag{1}$$

Conjugates uniquely determine each other whenever they exist, viz.

$$g(y) = \inf(\neg x : f(x)y = 0).$$

The notion of conjugation generalizes to a test semiring S with mappings f, g of type $S \to \mathsf{test}(S)$. We say that that g is a *left conjugate* of f and f a *right*

conjugate of g if, for all $a, b \in S$, $af(b) \leq 0 \Leftrightarrow g(a)b \leq 0$. This notion is no longer symmetric and lacks most of the properties presented below.

Lemma 4.1 *For every test semiring, the domain operation is a right conjugate of the codomain operation.*

PROOF. We calculate

$$a\delta(b) \leq 0 \Leftrightarrow \rho(a) \leq \neg\delta(b) \Leftrightarrow \delta(b) \leq \neg\rho(a) \Leftrightarrow \rho(a)b \leq 0.$$

The first step uses the dual of (gla) for codomain. The second step uses order duality. The third step uses (gla). □

It has been shown in [9] that (d3) is equivalent to $ab \leq 0 \Leftrightarrow a\delta(b) \leq 0$. By Lemma 4.1, locality of domain implies that of codomain and vice versa. More abstractly, this property is evident from duality with respect to opposition.

A *Galois connection* is a pair of mappings $(f^\flat, f^\sharp)$ between partial orders $(A, \leq_A)$ and $(B, \leq_B)$ such that $f^\flat : B \to A$ and $f^\sharp : A \to B$ satisfy

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

for all $a \in A$ and $b \in B$. Here, we restrict our attention to one single ordering $\leq$. $f^\flat$ is called the *lower adjoint* and $f^\sharp$ is called the *upper adjoint* of the Galois connection. It follows immediately that

$$f^\flat(x) = \inf(y : x \leq f^\sharp(y)) \qquad \text{and} \qquad f^\sharp(y) = \sup(x : f^\flat(x) \leq y).$$

The following fact about Galois connections and conjugates is well known.

Proposition 4.2 *Let f, g be endofunctions on a Boolean algebra B and let h be defined by $h(x) = \neg g(\neg x)$.*

(i) Let f and g be lower and upper adjoints of a Galois connection. Then f and h are conjugate.
(ii) Let f and g be conjugate. Then f and h are lower and upper adjoints of a Galois connection.

Mappings defined by Galois connections or by conjugation enjoy certain generic properties. All conjugate functions and all lower adjoints in Galois connections are, for instance, completely additive. By Proposition 4.2, upper adjoints are completely multiplicative, that is they preserve all existing infima.

Proposition 4.3 *A mapping f on a lattice L has an upper adjoint iff the following conditions are satisfied.*

(i) f *is completely additive,*
(ii) $\sup(x : f(x) \leq y)$ *exists for all* $y \in L$.

By our correspondence between Galois connections and conjugations, the same conditions guarantee the existence of conjugate functions.

We now present further properties of adjoints of Galois connections and conjugate functions that are interesting for our considerations.

First, upper and lower adjoints satisfy the following *cancellation properties*:

$$f^\flat \circ f^\sharp \leq 1 \qquad \text{and} \qquad 1 \leq f^\sharp \circ f^\flat.$$

Second, $f^\sharp \circ f^\flat \circ f^\sharp = f^\sharp$ and $f^\flat \circ f^\sharp \circ f^\flat = f^\flat$, that is $f^\sharp \circ f^\flat$ and $f^\flat \circ f^\sharp$ are dual isomorphisms.

Third, if f is an isotone endofunction, g an endofunction and $h^\flat$ the lower adjoint of a Galois connection on some set, then

$$f \circ h^\sharp \leq g \Rightarrow f \leq g \circ h^\flat. \tag{2}$$

Moreover, if f is a mapping and g is antitone, then

$$g \circ h^\flat \leq f \Rightarrow g \leq f \circ h^\sharp. \tag{3}$$

The following general property of additive functions over a Boolean algebra is needed for the fourth property.

$$f(x) - f(y) \leq f(x - y). \tag{4}$$

The following lemma is from Jónsson and Tarski [13].

Lemma 4.4 *Let* f *and* g *be endofunctions on a Boolean algebra* B*. Then the following conditions are equivalent.*

(i) f *and* g *are conjugate.*
(ii) f *and* g *are strict and* $f(x)y \leq f(xg(y))$ *and* $g(y)x \leq g(yf(x))$ *hold for all* $x, y \in B$.

This lemma is interesting because it provides an equational characterisation of conjugate functions. In a later section we will use the properties of Lemma 4.4(ii) to obtain a variant of the modular law of relation algebra, when f and g are interpreted as forward and backward diamond operators, respectively, over a modal semiring.

The domain and predomain operations are neither lower or upper adjoints of Galois connections, nor are they conjugates in the strict sense. This may

be surprising, since many properties of domain and codomain also arise from Galois connections or conjugation. We will see in the next section that Galois connections and conjunctions arise for preimage and image operations, which are special domain and codomain operations for actions restricted to propositions.

5 Modalities

We now define various modal operators in domain semirings. Their names are justified, since they induce strict and additive mappings on test algebras, whence Boolean algebras with operators or dual operators in the sense of Jónsson and Tarski. They can also be interpreted, respectively, as disjunctive or conjunctive predicate transformers. This links them with the syntax and semantics of Hoare logic.

Let S be a test semiring and let $a \in S$. The first definition introduces the forward diamond operator $|a\rangle$ on $\mathsf{test}(S)$ in the standard way via abstract preimage. For $p \in \mathsf{test}(S)$,

$$|a\rangle p = \delta(ap).$$

This operator is the same as $\langle a\rangle$ in dynamic logic. It satisfies the following properties that we will also denote as (llp) and (gla).

$$|a\rangle p \leq q \Leftrightarrow ap \leq qa \Leftrightarrow \neg qap \leq 0.$$

We now define a backward diamond operator by duality with respect to opposition, i.e., via abstract image as

$$\langle a|p = \rho(pa).$$

It follows that dual variants of (llp) and (gla) hold for backward diamonds. In presence of converse we have that $|a\rangle p = \langle a^\circ|p$. The following statement is immediate from (gla) and opposition.

Lemma 5.1 *The forward and backward diamonds are conjugate.*

As usual, we define for all $a \in S$ and $p \in \mathsf{test}(S)$ the box operators

$$|a]p = \neg|a\rangle\neg p \quad \text{and} \quad [a|p = \neg\langle a|\neg p.$$

We will see later that $|a]p$ corresponds to $\mathsf{wlp}(a, p)$; it is also the same as the monotype factor used in [2]. By Proposition 4.2, boxes and diamonds are upper and lower adjoints of Galois connections.

Lemma 5.2 *In a domain semiring S, for all $a \in S$ and $p, q \in \mathsf{test}(S)$,*

$$|a\rangle p \leq q \Leftrightarrow p \leq [a|q, \qquad \langle a|p \leq q \Leftrightarrow p \leq |a]q. \tag{5}$$

Duality with respect to complementation is the second one besides duality with respect to opposition. While the operation of conversion, which operates on actions, is an isomorphism onto the opposite semiring, negation is an isomorphism onto the lattice dual test algebra. In this sense, opposition is a temporal duality, since it inverts the flow of actions. Complementation is a spacial duality, since it operates on the test space.

Complementarity between forward and backward modalities and the Galois connection imply many useful properties in a generic way.

Proposition 5.3 *The diamonds of a domain semiring are completely additive; the boxes are completely multiplicative.*

It also follows immediately from the Galois connections that boxes and diamonds are unique whenever they exist. Moreover, it follows from duality with respect to opposition and the Galois connection that all modal operators are in bijective correspondence.

In the following sections, we will appeal to the dualities with respect to opposition and complementation as theorem transformers. We will prove statements for one operation and then obtain three others for free. We will appeal to the Galois connections and to conjugation as theorem generators.

We have seen in this section that the modal operators over a domain semirings satisfy symmetries and dualities that are far beyond those of domain. This is the case although domain and codomain can be defined from forward and backward diamonds by $\delta(a) = |a\rangle 1$ and $\rho(a) = \langle a|1$. We call a semiring with a domain and codomain operation that satisfies (d1), (d2) and (d3) as well as their duals with respect to opposition a *modal Kleene algebra* in order to emphasize this particular point of view.

6 Modal Operator Algebras

We now take up the correspondence between properties of operators over Boolean algebras and relational properties that has been pioneered by Jónsson and Tarski. Pure Kleene algebra, however, is not expressive enough for many relational properties, since it lacks the operations of meet, complementation and converse of actions that are available in relation algebra (cf. [25]). In this section we show that all the axioms of relation algebra are theorems in modal

operator semirings. Consequently, the calculus of functions and relations can be regained at the operator level for the more general class of modal algebras.

We introduce operator algebras by considering general endofunctions on the test algebra. We lift addition and meet point-wise by setting $(f + g)(x) = f(x) + f(x)$ and $(f \sqcap g)(x) = f(x) \cdot g(x)$. The associated natural order is the pointwise order on operators:

$$f \leq g \Leftrightarrow \forall x.f(x) \leq g(x).$$

A multiplication is given by $(fg)(x) = f(g(x))$. We also define $1 = |1\rangle = \langle 1|$ and $0 = |0\rangle = \langle 0|$. (Relative) complementation and Boolean implication can be lifted in a similar way.

The locality laws yield closure conditions for modal operators. $|ab\rangle = |a\rangle|b\rangle$ says that diamonds are closed under composition. While this law is covariant, we have the contravariant law $\langle ab| = \langle b|\langle a|$ for backward diamonds. Closure under addition follows from $|a + b\rangle = |a\rangle + |b\rangle$, which is immediate from additivity of domain.

Proposition 6.1 *The diamond operators on a domain semiring form an idempotent semiring.*

PROOF. Consider the mapping $\phi(x) = |x\rangle$. It follows from the closure conditions $|a + b\rangle = |a\rangle|b\rangle$ and $|ab\rangle = |a\rangle|b\rangle$ that ϕ is a semiring homomorphism. Since idempotent semirings are equational classes, the class is, by the HSP-theorem, closed under homomorphic images. Therefore the operators algebra is also an idempotent semiring. □

We will later encounter situations when ϕ is an isomorphism.

We now add further elements to the operator algebra. We will use the well-known fact from lattice theory that the space of endofunctions on a (distributive) lattice forms again a (distributive) lattice. Since (distributive) lattices are equational classes, they are, by the HSP-theorem, closed under subalgebras. The following statement takes the meet structure into account. Since diamonds are not closed under meet and complementation, a larger function space must be considered.

Let $\Omega_L(S)$, $\Omega_H(S)$ and $\Omega_B(S)$ be the closures of $\{|s\rangle : s \in S\}$ under addition and meet, addition, meet and relative complementation and addition, meet and complementation.

Proposition 6.2 *Let S be a domain semiring.*

(i) $\Omega_L(S)$ *is a distributive lattice.*
(ii) $\Omega_H(S)$ *is a Heyting algebra.*
(iii) $\Omega_B(S)$ *is a Boolean algebra with greatest element* $\top = 1 + \neg 1$.

PROOF. (i) $\Omega_L(S)$ with join and meet defined pointwise is a subalgebra of the endomorphism algebra on $\mathsf{test}(S)$ and thus a distributive lattice.

(ii) Define implication by $|a\rangle \to |b\rangle = \neg|a\rangle + |b\rangle$. By the same argument as in (i), $\Omega_H(S)$ is a lattice. It is easy to show that implication satisfies, for all diamonds f, g and h, the Galois connection $f \sqcap g \leq h \Leftrightarrow f \leq g \to h$, by reducing it to the pointwise Galois connection of Boolean complementation. Thus the algebra is a Heyting algebra.

(iii) Using (i) it remains to verify the properties of $\top$ and of complementation. It is easy to show that $\top$ maps all elements of the Boolean algebra to 1. Thus $\top$ is the greatest element of the operator algebra by definition of the ordering on operators. It remains to show that $|a\rangle + \neg|a\rangle = \top$ and $|a\rangle \sqcap \neg|a\rangle = 0$. But $(|a\rangle + \neg|a\rangle)(p) = |a\rangle p + (|a\rangle p)' = 1 = \top(p)$ and $(|a\rangle \sqcap \neg|a\rangle)(p) = (|a\rangle p)(|a\rangle p)' = 0 = 0(p)$. □

Note, however, that $\top$ conflicts with the semiring axioms. $\top(0) = 1$, that is top is not strict. Therefore, at the operator level, 0 is no longer a right annihilator.

Proposition 6.2 shows that Boolean algebra, converse and semirings are available at the operator level.

The addition of meets and complements leads, however, to conflicts with distributivity laws, since endofunctions f, g and h over a Boolean algebra satisfy a left distributivity law $f(g + h) = fg + fg$ only in case f is additive. Operator level meet and negation, of course, are not additive but multiplicative. In function spaces with non-additive elements we can therefore only expect weak variants of semirings without left distributivity.

A structure $(M, +, \sqcap, \cdot, 0, 1)$ is a *right-distributive lattice-ordered monoid* (a *rd-monoid*) if $(M, +, \sqcap)$ is a distributive lattice and $(M, +, \cdot, 0, 1)$ is a semiring that need not satisfy the left distributivity law. Similar structures have extensively been studied in [3]. Note that the semiring-retract of a d-monoid is idempotent.

Proposition 6.3 *Let* S *be a domain semiring and let* $\Omega(S)$ *be the closure of* $\{|s\rangle : s \in S\}$ *under addition, multiplication and meet. Then* $(\Omega(S), +, \sqcap, \cdot, \mathsf{0}, \mathsf{1})$ *is a rd-monoid.*

PROOF. Proposition 6.2(i) shows that $\Omega(S)$ is a distributive lattice. Right-distributivity and left annihilation ($Oa = 0$) hold for arbitrary endofunctions. Right annihilation holds for all strict endofunctions, but meets of diamonds are strict. By closure under subalgebras, $\Omega(S)$ is a rd-monoid. □

Closure of the operator algebra under complementation is even more problematic, since this is neither strict nor isotone. Therefore we now concentrate on showing that the axioms of relation algebra hold for diamonds.

First, we introduce an operation of conversion, setting $|.\rangle^\circ = \langle .|$ and $\langle .|^\circ = |.\rangle$. The required axioms are easily shown. E.g., for contravariance we calculate

$$|ab\rangle^\circ = \langle ab| = \langle b|\langle a| = |b\rangle^\circ |a\rangle^\circ.$$

Next, present some further consequences of the lifting.

Lemma 6.4 *Let S be a domain semiring. For all $a \in S$ and endofunctions f, g on $\mathsf{test}(S)$,*

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

The operator-level conjugation law is an analogue to the Schröder law from relation algebra, which is even one of its defining axioms. The operator-level Galois connections define residuals or factors on modal operators. Here, $g|a\rangle = [a|g$ is the *right residual* of g by $|a\rangle$. It follows from (3) that $f|a\rangle \leq g \Leftrightarrow f \leq g[a|$ if f and g are antitone. In that case, $g\backslash|a\rangle = g[a|$ is the *left residual* of g by $|a\rangle$. The following laws are further simple consequences of the Galois connection and Boolean algebra. They do not use any specific properties of modal semirings or modules. We have the *cancellation properties*

$$\langle a||a] \leq 1 \leq |a]\langle a|. \tag{6}$$

Second, for arbitrary endofunctions f, g on B we have the laws

$$|a\rangle f - |a\rangle g \leq |a\rangle(f - g), \tag{7}$$
$$|a](f \to g) \leq |a]f \to |a]g. \tag{8}$$

This follows from (4) and its dual. These laws are interesting for proving the following variant of the *modular laws* of relation algebra, which are operator-level variants of the general laws from Lemma 4.4(ii).

Lemma 6.5 *Let S be a domain semiring. For all $a \in S$ and endofunctions f, g on $\mathsf{test}(S)$, the conjunction of the modular laws*

$$|a\rangle f \sqcap g \leq |a\rangle(f \sqcap \langle a|g) \qquad \langle a|f \sqcap g \leq \langle a|(f \sqcap |a\rangle g) \tag{9}$$

is equivalent to the Schröder law.

An analogue of the following property is sometimes called co-difunctionality in relation algebra.

Lemma 6.6 *Let K be a modal Kleene algebra. Then for all $a \in K$,*

$$|a\rangle \leq |a\rangle\langle a||a\rangle. \tag{10}$$

PROOF. Let $f = |a\rangle$. Using the modular law, we calculate

$$f = f \sqcap f = f1 \sqcap f \leq f(1 \sqcap f^\circ f) = ff^\circ f.$$

□

The following difference to relation algebra is worth noting. In relation algebra, $\top 0 = 0$, whereas according to our definition, $\top$ is not strict. In relation algebra, $\top 0 = 0$ follows immediately from the Schröder law $a0 \leq 0 \Leftrightarrow a^\circ \top \leq \top$ and the facts that $\top$ is the complement of 0 and the greatest element. This is no contradiction, since in our case the Schröder laws hold only for diamonds (or dually for boxes), whereas $\top$ is not in this class. Consequently, since some closure properties are obviously violated, the algebra of modal operators over a domain semiring is not a relation algebra.

Proposition 6.7 *The diamonds over a domain semiring satisfy all axioms of relation algebra.*

PROOF. Here, we consider a relation algebra as a l-monoid that is also a Boolean algebra with an operation of conversion that satisfies the modal Schröder law. We have verified all these axioms in previous Propositions. □

It follows that the operator algebra is rich enough for formalizing the notions of a function and of determinacy and for developing the usual functional calculus of relation algebra.

We now consider the impact of the Kleenean structure on the operator algebra.

Proposition 6.8 *The (forward) diamond operators on a left inductive Kleene algebra with domain form a left inductive Kleene algebra, setting $|a\rangle^* = |a^*\rangle$.*

This holds since the operator level star unfold laws

$$1 + |a\rangle|a^*\rangle = |a^*\rangle, \qquad 1 + |a^*\rangle|a\rangle = |a^*\rangle$$

hold and since the operator level star induction law implies that $f + |a\rangle g \leq g \Rightarrow |a^*\rangle f \leq g$ holds for arbitrary endofunctions f, g on the Boolean algebra. Therefore the mapping ϕ defined above is also a homomorphism with respect to the star. Note that the class of Kleene algebras as a quasivariety is not closed under homomorphic images.

There is no similar law for box operators. Instead, by duality, it can be shown that for each a of some Kleene module, $|a^*]$ is the greatest postfixed point of the mapping $f(x) = p \sqcap |a]x$. It follows that the operator level laws $1 \sqcap |a]|a^*] = |a^*]$, its dual and $g \leq f \sqcap |a]g \Rightarrow g \leq |a^*]f$ hold.

Lemma 6.9 *Let $(S, B, |\ \rangle)$ be a Kleene module. Then the test-level induction law is equivalent to the following identity. For all $a \in S$,*

$$|a\rangle^* - 1 \leq |a\rangle^*(|a\rangle - 1). \tag{11}$$

(11) corresponds to the induction axiom of propositional dynamic logic. A proof of the equivalence can be found in [10]. It is again based on the Galois connection for relative complements. Therefore the quasi-variety of left star inductive operator Kleene algebra contains the variety of left operator Kleene algebras that satisfy (11), which is also a very interesting class.

Instead of calculating at the domain level, we can therefore calculate many modal properties more simply at this higher level of abstraction (see below).

7 Application: Propositional 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. To this end we assume a set Π of propositional variables and a set Γ of atomic commands such as assignments. The set Φ of *propositions* is defined by the grammar

$$\Phi ::= \Pi \mid \Phi \wedge \Phi \mid \neg\Phi,$$

with the abbreviations $\phi_1 \vee \phi_2$ and $\phi_1 \rightarrow \phi_2$ for $\phi_1, \phi_2 \in \Phi$ defined as usual. The set Σ of *statements* is defined by the grammar

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

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 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 $[\![\gamma]\!] \in K$. Then we inductively define the semantics $[\![\phi]\!]$ of every $\phi \in \Phi$ and $[\![\alpha]\!]$ of every $\alpha \in \Sigma$ as follows.

$$\begin{aligned}
[\![\phi \wedge \psi]\!] &= [\![\phi]\!][\![\psi]\!], \\
[\![\neg\phi]\!] &= \neg[\![\phi]\!], \\
[\![\mathsf{abort}]\!] &= 0, \\
[\![\mathsf{skip}]\!] &= 1, \\
[\![\alpha\,;\,\beta]\!] &= [\![\alpha]\!][\![\beta]\!], \\
[\![\ \mathsf{if}\ \phi\ \mathsf{then}\ \alpha\ \mathsf{else}\ \beta]\!] &= [\![\phi]\!][\![\alpha]\!] + \neg[\![\phi]\!][\![\beta]\!], \\
[\![\ \mathsf{while}\ \phi\ \mathsf{do}\ \alpha]\!] &= ([\![\phi]\!][\![\alpha]\!])^*\neg[\![\phi]\!].
\end{aligned}$$

We follow [17] in defining validity of formulas and PCAs. We call a proposition $\phi \in \Phi$ *valid*, in signs $\models \phi$, iff $[\![\phi]\!] = 1$. In particular,

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

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 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 Galois connection between boxes and diamonds, is consistent with the standard wlp-semantics (see also Section 10 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

$$\models \{p\}\ a\ \{q\} \Leftrightarrow \langle a|p \leq q. \tag{12}$$

The Hoare calculus for partial correctness of deterministic sequential programs

consists of the following inference rules.

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

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

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

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

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

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

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

A rule with premises $P_1, \cdots, P_n$ and conclusion P is *sound* if validity of all premises implies validity of the conclusion. Derivations are defined as usual.

Here, (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 Γ of atomic commands as a parameter in our approach. The requirement of sufficient expressiveness on Γ that ensures completeness of the calculus will be discussed in Section 10. Following [17], we call this abstract form of Hoare logic *propositional Hoare logic* (PHL).

8 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 [12] and KAT [17], 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 in that we may reason both at the test level and the operator level. 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 [1,19] and show that KAD provides a natural abstract algebraic semantics for PHL.

A first pointwise encoding of the soundness conditions for the Hoare rules is rather straightforward from (12). (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 contravariance of multiplication of backward diamonds. 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 the test-level induction law, 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. Compared with standard textbooks (cf. [1,19]), 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.

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. [17]). We can obtain this encoding also in KAD, using (llp).

We now head for another, pointfree, 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 8.1 *Let $K \in$ KAD. Then the soundness conditions for the inference rules of* PHL *are equivalent to the following pointfree encodings: for all*

$a, b \in K$ *and* $p \in \mathsf{test}(K)$ *and* $f, g, h, k : \mathsf{test}(K) \to \mathsf{test}(K)$,

(Abort)	$\langle 0 \mid \leq \langle q \mid,$
(Skip)	$\langle 1 \mid \leq \langle 1 \mid,$
(Composition)	$\langle ab \mid \leq \langle b \mid \langle a \mid,$
(Conditional)	$\langle pa + \neg pb \mid \leq \langle a \mid \langle p \mid + \langle b \mid \langle \neg p \mid,$
(While)	$\langle a \mid \langle p \mid f \leq f \Rightarrow \langle \neg p \mid \langle (pa)^* \mid f \leq \langle \neg p \mid f,$
(Weakening)	$f \leq g \wedge \langle a \mid g \leq h \wedge h \leq k \Rightarrow \langle a \mid f \leq k.$

PROOF. (Abort) and (Skip) are obvious. For the remaining ones we use the principle of *indirect inequality*:

$$p \leq q \Leftrightarrow (\forall r \,.\, q \leq r \Rightarrow p \leq r).$$

(Composition) By indirect inequality the claim is equivalent to

$$\forall p, r. \langle b \mid \langle a \mid p \leq r \Rightarrow \langle ab \mid p \leq r.$$

But this is follows from the pointwise encoding by setting $q = \langle a \mid p$.
Assume now the pointfree encoding and let $\langle a \mid p \leq q$ and $\langle b \mid q \leq r$. Then

$$\langle ab \mid p \leq (\langle b \mid \langle a \mid)(p) = \langle b \mid \langle a \mid p \leq \langle b \mid q \leq r.$$

(Conditional) Assume the pointwise encoding. Then the antecedent is equivalent to $\langle a \mid \langle p \mid q \leq r \wedge \langle b \mid (\langle \neg p \mid q) \leq r$, hence to $(\langle a \mid \langle p \mid + \langle b \mid \langle \neg p \mid)(q) \leq r$. Now the pointfree encoding follows by multiplicative contravariance and indirect inequality.
Assume the pointfree encoding and let $\langle a \mid (pq) \leq r$ and $\langle b \mid (\neg pq) \leq r$. Then

$$\begin{aligned} \langle (pa + \neg pb) \mid q &= \langle pa \mid q + \langle \neg pb \mid q \\ &= \langle a \mid (\langle p \mid q) + \langle b \mid (\langle \neg p \mid q) \\ &= \langle a \mid (pq) + \langle b \mid (\neg pq) \\ &\leq r + r \\ &= r. \end{aligned}$$

(While) Assume the pointwise encoding. Then the antecedent is equivalent to $(\langle a \mid \langle p \mid) q \leq q$, while the succedent is equivalent to $\langle (pa)^* \neg p \mid q \leq \langle \neg p \mid q$. Replacing q by $f(r)$ for suitable f and r yields the pointfree encoding.
Assume now the pointfree encoding. Then use the converse translation.
(Weakening) Similar to the (While) case. □

In this transformation, (While) and (Weakening) are the only rules where,

at first sight, nothing has been gained by the lifting. However, their correctness proofs can now be performed entirely in the operator algebra instead of expanding to properties of domain.

Theorem 8.2 *The pointfree encodings of the* PHL*-rules are theorems in* KAD*.*

PROOF. The pointfree variants of (Abort) and (Skip) are trivial. The pointfree variant of (Composition) is nothing but contravariance of multiplication for backward diamonds. The pointfree variant of (Conditional) is evident from the closure properties for addition and multiplication. The proof for (While) is essentially the pointwise one lifted to the operator level. (Weakening) holds by isotonicity of multiplication in i-semirings. □

Theorem 8.3 PHL *is sound with respect to the* KAD *semantics.*

PROOF. By induction on PHL derivations, using Theorem 8.2. □

As observed in [17], 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.

9 Soundness of Some Further Hoare Rules

To further support our claim of simplicity and flexibility, we now give calculational soundness proofs for some admissible rules of PHL in KAD. The examples are taken from [1].

Lemma 9.1 *The following axioms and inference rules are sound with respect to the semantics of* PHL*.*

(i) *If* $pa = ap$ *then* $\{p\}\ a\ \{p\}$.

(ii)
$$\frac{\{p\}\ a\ \{q\} \quad \{p\}\ b\ \{r\}}{\{p\}\ a+b\ \{q \vee r\}}.$$

(iii)
$$\frac{\{p\}\ a\ \{r\} \quad \{q\}\ a\ \{r\}}{\{p \vee q\}\ a\ \{r\}}.$$

(iv)
$$\frac{\{p_1\}\ a\ \{q_1\} \quad \{p_2\}\ a\ \{q_2\}}{\{p_1 \wedge p_2\}\ a\ \{q_1 \wedge q_2\}}.$$

(v) If $pa = ap$ *then*
$$\frac{\{q\}\ a\ \{r\}}{\{p \wedge q\}\ a\ \{p \wedge r\}}.$$

Note that the condition $pa = ap$ might for instance arise by abstraction from the fact that the free variables in p are not changed by a.

The proofs are entirely straightforward, each taking at most one line of calculus. We encourage the reader to show soundness of the rules using the standard set-theoretic semantics. This is by far more complex. As a conclusion, we can only support the observation in [17] that in Kleene algebra *the specialised syntax and deductive apparatus of Hoare logic are inessential and can be replaced by simple equational reasoning.*

10 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
$$\mathsf{wlp}(P, T) = \{s \in S : P(s) \subseteq T\},$$
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 connections (5) and (12) immediately imply
$$\models \{p\}\ \alpha\ \{q\} \ \Leftrightarrow\ p \leq |a]q.$$

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 dualising our results from Section 6.

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 ψ under α, i.e.,
$$[\![\phi]\!] = \mathsf{wlp}([\![\alpha]\!], [\![\psi]\!]). \tag{13}$$

Assuming (13) 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. Moreover, for every atomic command $\gamma \in \Gamma$ and test q we add an axiom

$$\{|g]q\}\ g\ \{q\}, \tag{14}$$

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

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

Proposition 10.1 *Let $K \in \mathsf{KAD}$. Let $a, b, c, w \in K$ and $p, q \in \mathsf{test}(K)$.*

(i) For $c =$ if p then a else b,

$$p\,(|c]q) = p\,(|a]q), \tag{15} \qquad \neg p\,(|c]q) = \neg p\,(|b]q). \tag{16}$$

(ii) For $w =$ while p do a,

$$p\,(|w]q) = p|a](|w]q), \tag{17} \qquad \neg p\,(|w]q) \leq q. \tag{18}$$

PROOF. (i) We only show (15), since (16) is similar. First, by additivity of addition and the simple property

$$|pa]q = \neg p + |a]q, \tag{19}$$

$|c]q = (|pa]q)(|\neg pb]q) = (\neg p + |a]q)(p + |b]q) = p(|a]q) + \neg p(|b]q) + (|a]q)(|b]q)$.
Hence, by $|b]q \leq 1$ and isotonicity,

$$p(|c]q) = p(|a]q) + p(|a]q)(|b]q) = p(|a]q).$$

(ii) For (17) we calculate

$$\begin{aligned} p(|w]q) &= p(|(pa)^*]|\neg p]q) \\ &= p(|(pa)^*](p+q)) \\ &= p(p+q)(|pa]|(pa)^*](p+q)) \\ &= p(\neg p + |a]|(pa)^*](p+q)) \\ &= p(|a]|(pa)^*]|\neg p]q) \\ &\leq |a]|w]q. \end{aligned}$$

The first step uses the definition of w and contravariance of box over multiplication, the second one (19), the third one operator level star unfold, the fourth one the absorption law for lattices and (19), the fifth one Boolean algebra and (19), the sixth one that $p \leq 1$ and the definition of w.

For (18), we calculate, using the first three steps from the proof of (17),

$$\neg p(|w]q) \leq \neg p(p+q)(|pa]|(pa)^*](p+q)) = \neg pq(|pa]|(pa)^*](p+q)) \leq q.$$

□

Now we can proceed, as for instance in [1].

Lemma 10.2 *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 $a = bc$. By the induction hypothesis,

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

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

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

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

Hence, by (Weakening), also

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

By (15) and (16) these statements are equivalent to

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

so that (Conditional) shows the claim.

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

$$\vdash \{|a]r\}\ a\ \{r\},$$

hence by (Weakening)

$$\vdash \{p|a]r\}\ a\ \{r\}.$$

By (17) this is equivalent to

$$\vdash \{pr\}\ a\ \{r\}.$$

(While) shows that $\vdash \{r\}\ w\ \{\neg pr\}$ and (18) and (Weakening) yield the required

$$\vdash \{|w]q\}\ w\ \{q\}.$$

□

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

Theorem 10.3 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 (10), Lemma 10.2 and (Weakening). □

11 Decidability

We now present a novel decidability result for PHL that follows from a decidability result for a natural subclass of KAD.

A *Hoare formula* in KAD is a universal Horn formula with literals of the form $s \leq p$ such that p is a Boolean KAT term and s is either a KAT term or a term $|a\rangle p$ or $\langle a|p$ where p and a are KAT terms. All encodings of PHL inference rules in KAD are Hoare formulas in KAD. A *Hoare formula* in KAT is a universal Horn formula whose literals are of the form $s \leq 0$ and s is a KAT term.

Proposition 11.1 *For every Hoare formula ϕ in* KAD *that is valid in* KAD *there is a Hoare formula in* KAT *that is equivalent to ϕ in* KAD *and that is valid in* KAT. *The translation from* KAD *to* KAT *is linear.*

PROOF. Use (llp) or (gla) to eliminate all modalities from a Hoare formula ϕ in KAD. This yields a Hoare formula ψ in KAT that is equivalent to ϕ in KAD. Since ψ does not contain any modal subterm, only KAT-axioms are applicable to ψ. Therefore ψ holds in KAD if and only it holds in KAT. □

It seems very promising to extend this "demodalisation" result to further classes of KAD formulas. In particular, a result from [11] yields an equivalence transformation from Hoare formulas in KAT to equations in KAT so that one can use a PSPACE automata-theoretic decision procedure.

Lemma 11.2 *Hoare formulas in* KAD *are decidable in PSPACE.*

We give a decidability result for another class of KAD expressions, where we couple actions and tests further. In modal semirings, properties of actions

can be measured via their effects on states, but these measurements need not completely determine the behaviour of actions. A modal semiring $(S, B, |\ \rangle)$ is *extensional* if $|a\rangle = |b\rangle$ implies $a = b$. This is equivalent to the extensionality law

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

By isotonicity of diamonds this can be strengthened to the equivalence $|a\rangle \leq |b\rangle \Leftrightarrow a \leq b$.

Lemma 11.3 *The relation $a \preceq b$ defined by $|a\rangle \leq |b\rangle$ is a pre-congruence on the Kleene algebra.*

PROOF. For addition, we calculate

$$a \preceq b \Leftrightarrow |a\rangle \leq |b\rangle \Rightarrow |a\rangle + |c\rangle \leq |b\rangle + |c\rangle \Leftrightarrow |a + c\rangle \leq |b + c\rangle \Leftrightarrow a + c \preceq b + c.$$

For left multiplication, we calculate

$$a \preceq b \Leftrightarrow |a\rangle \leq |b\rangle \Rightarrow |c\rangle|a\rangle \leq |c\rangle|b\rangle \Leftrightarrow |ca\rangle \leq |cb\rangle \Leftrightarrow ca \preceq cb.$$

The proof for right multiplication works by duality. For the star, we calculate

$$a \preceq b \Leftrightarrow |a\rangle \leq |b\rangle \Rightarrow |a\rangle^* \leq |b\rangle^* \Leftrightarrow |a^*\rangle \leq |b^*\rangle \Leftrightarrow a^* \preceq b^*.$$

□

The associated congruence $\approx$ is the kernel of the above homomorphism ϕ from the Kleene algebra onto the diamond algebra. In case of extensionality, ϕ is injective and therefore an isomorphism. Therefore, in the extensional case the operator semiring or Kleene algebra and the underlying semiring or Kleene algebra are isomorphic.

We now provide another result of the operator level in the spirit of our previous structure theorems. Consider the axioms of dynamic algebra, as e.g. given in [12].

$$\begin{aligned}
|a + b\rangle p &= |a\rangle p + |b\rangle p, \\
|ab\rangle p &= |a\rangle|b\rangle p, \\
|a\rangle(p + q) &= |a\rangle p + |a\rangle q, \\
|1\rangle p &= p, \\
|0\rangle p &= 0, \\
|a^*\rangle p &= p + |a\rangle|a^*\rangle p, \\
|a\rangle^* - 1 &\leq |a\rangle^*(|a\rangle - 1).
\end{aligned}$$

In addition, there are some suitable axioms for Boolean algebra. Note that the algebra of actions is only implicitly induced via $\approx$ by these axioms. Also note that $|a^*\rangle p = p + |a^*\rangle|a\rangle p$ follows from the other unfold and induction law.

Theorem 11.4 *Every dynamic algebra induces a left inductive Kleene algebra at the operator level. Every extensional dynamic algebra induces a left inductive Kleene algebra of actions.*

PROOF. It suffices to show the second part, the first one being induced by the congruence $\approx$. We only give three cases, the other ones being similar.

Left distributivity: $a(b+c) = ab + ac \Leftrightarrow |a(b+c)\rangle = |ab+ac\rangle$. But

$$|a(b+c)\rangle = |a\rangle(|b\rangle + |c\rangle) = |a\rangle|b\rangle + |a\rangle|c\rangle) = |ab+ac\rangle.$$

Left star unfold: $1 + aa^* = a^* \Leftrightarrow |1 + aa^*\rangle = |a^*\rangle$. This holds by the unfold law of dynamic algebra.

Left star induction: $b+ac \leq c \Rightarrow a^*b \leq c \Leftrightarrow \forall p.|b+ac\rangle p \leq |c\rangle p \Rightarrow \forall p.|a^*b\rangle p \leq |c\rangle p$. This follows from the operator level left induction law and Lemma 6.9. □

To define test algebras [24] the additional axiom $|p\rangle q = pq$ is used and tests are embedded into the algebra of actions. Using our previous result it is easy to show that extensional left inductive Kleene algebras with domain (and without codomain) and dynamic algebras define precisely the same classes. In particular, identities between actions can be transformed to equivalent modal expressions using extensionality. It follows from well-known results about test algebra [24] that extensional left inductive Kleene algebras with domain and propositional dynamic logic satisfy precisely the same identities.

Theorem 11.5 *Every identity in an extensional left inductive Kleene algebra with domain can be decided in EXPTIME.*

PROOF. Translate the identity to propositional dynamic logic and use a PDL decision procedure decision procedure, which is is EXPTIME. □

12 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 formalised 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 pointfree specifications and proofs of modal properties.

As an application we have provided algebraic soundness and completeness proofs for propositional Hoare logic that use modal Kleene algebra both at the syntactic and at the semantic side. In particular, the pointfree soundness proof and the completeness proof exhibit the natural algebraic properties that are implicit in the partial correctness assertions and Hoare rules.

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

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

The approach is, however, not limited to partial correctness. Program termination can be modelled in modal Kleene algebra, too [8]. Based on the concepts of that paper we present in [22] an algebraic semantics for total correctness similar to that of [23]. It turns out that the wp predicate transformer coincides with the wlp operator in a suitable semiring of commands. In particular, our generic proofs of soundness and completeness carry over to that setting, giving a non-trivial application of the results in the present paper.

As a further use of modal Kleene algebra we have shown that propositional dynamic logic can be embedded [10]. Currently we are considering temporal logics. An algebraic treatment of LTL along the lines of [26] is contained in [7]; a paper on full CTL^* is forthcoming.

Recently, the modal operators have also been incorporated into *Lazy Kleene Algebra* [20], a framework extending the work of Cohen [4] and von Wright [27] and is designed to deal with both terminating and non-terminating computations and hence also with reactive systems.

Further applications of modal Kleene algebra are surveyed in [7].

Altogether, these 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. The extension to full first order logics, based on Tarskian frames [18], is left for future work.

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

References

[1] K.-R. Apt and E.-R. Olderog. *Verification of Sequential and Concurrent Programs*. Springer, 2nd edition, 1997.

[2] R. Backhouse and J. van der Woude. Demonic operators and monotype factors. *Mathematical Structures in Computer Science*, 3(4):417–433, 1993.

[3] G. Birkhoff. *Lattice Theory*, volume 25 of *Colloquium Publications*. American Mathematical Society, 1984. Reprint.

[4] 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.

[5] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *6th POPL*, pages 269–282. ACM Press, 1979.

[6] J. Desharnais and B. Möller. Characterizing determinacy in Kleene algebras. *Information Sciences*, 139(3–4):253–273, 2001.

[7] J. Desharnais, B. Möller, and G. Struth. Applications of modal Kleene algebra — a survey. *JoRMiCS — Journal on Relational Methods in Computer Science*, 1:93–131, 2004.

[8] J. Desharnais, B. Möller, and G. Struth. Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, and J. Mitchell, editors, *Exploring new frontiers of theoretical informatics*, volume 155 of *IFIP International Federation for Information Processing Series*, pages 653–666. Kluwer, 2004.

[9] J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM Transaction on Computational Logic*, 2005. (to appear).

[10] T. Ehm, B. Möller, and G. Struth. Kleene modules. In R. Berghammer, B. Möller, and G. Struth, editors, *Relational and Kleene-Algebraic Methods in Computer Science*, volume 3051 of *LNCS*, pages 112–123. Springer, 2004.

[11] 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.

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

[13] B. Jónsson and A. Tarski. Boolean algebras with operators, Part I. *American Journal of Mathematics*, 73:891–939, 1951.

[14] D. Kozen. On Kleene algebras and closed semirings. In B. Rovan, editor, *Proc. of MFCS'90*, volume 452 of *LNCS*, pages 26–47. Springer, 1990.

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

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

[17] D. Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1(1):60–76, 2001.

[18] D. Kozen. Some results in dynamic model theory. *Science of Computer Programming*, 51(1–2):3–22, 2004.

[19] J. Loeckx and K. Sieber. *The Foundations of Program Verification*. Wiley Teubner, 2nd edition, 1987.

[20] B. Möller. Lazy Kleene algebra. In D. Kozen, editor, *Mathematics of Program Construction*, volume 3125 of *LNCS*, pages 252–273. Springer, 2004.

[21] B. Möller and G. Struth. Modal Kleene algebra and partial correctness. In C. Rattray, S. Maharaj, and C. Shankland, editors, *Algebraic methodology and software technology*, volume 3116 of *LNCS*, pages 379–393. Springer, 2004.

[22] B. Möller and G. Struth. WP is WLP. In *Participants' Proceedings of the 8th International Seminar on Relational Methods in Computer Science (RelMiCS 8) and 3rd International Workshop on Applications of Kleene Algebra, February 22-26, 2005, St. Catharines, Ontario, Canada*, 2005. (to appear).

[23] G. Nelson. A generalization of Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 11:517–561, 1989.

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

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

[26] B. von Karger. Temporal algebra. *Mathematical Structures in Computer Science*, 8(3):277–320, 1998.

[27] 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.