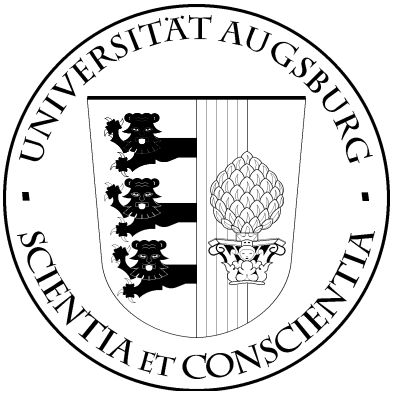
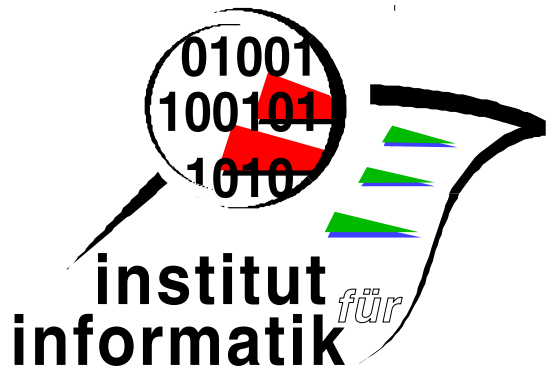
Universität Augsburg



Modal Kleene Algebra and Partial Correctness

Bernhard Möller and Georg Struth

Report 2003-08 Mai 2003



Institut für Informatik
D-86135 Augsburg

Copyright © Bernhard Möller and Georg Struth
Institut für Informatik
Universität Augsburg
D–86135 Augsburg, Germany
http://www.Informatik.Uni-Augsburg.DE
— all rights reserved —

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 We enrich Kleene algebra by domain and codomain operators. These abstractions of relational notions give rise to four modal operators. The boxes and diamonds enjoy various symmetries via Galois connections and dualities. Lifting modal statements to modal operator semirings yields a further abstraction and thus a more elegant and concise "statefree" reasoning about modalities.
We use this modal Kleene algebra for calculating soundness and completeness proofs for propositional Hoare logic. While our soundness proof is more direct than related ones, our algebraic completeness proof seems entirely novel. It uses a modal symmetry that relates the wlp predicate transformer with partial correctness assertions and that is beyond the expressibility of formalisms like propositional dynamic logic.

1 Introduction

Hoare's calculus for partial correctness has been around now for almost 25 years, with numerous offsprings and applications. So how can we hope to say something about it that is new as well as interesting? One of our aims is to use a generic semantic model in an enrichment of Kleene algebra and to show, on its basis, both soundness and completeness of propositional Hoare logic (PHL) in a in a purely calculational algebraic fashion.

Our enrichment is *Kleene algebra with domain* (KAD) [2] which takes a significant step beyond Kozen's *Kleene algebra with tests* (KAT) [8]. The specific difference is a simple equational axiomatization of domain and codomain operators as abstract counterparts of the respective notions for relations. This modest expansion leads to a considerable increase in expressiveness and structural insight. In KAD we can define image and preimage, and hence forward and backward modal box and diamond operators. These are related by two kinds of symmetries: Galois connections and dualities. The former yield a number of modal properties for free. The latter allow us to transfer properties of one modal operator automatically to its relatives. Further structural insights are provided by the modal operator semirings over KAD. This additional layer of abstraction supports even more elegant and concise "statefree" reasoning about modalities.

* This research was partially sponsored by DFG Project InopSys — Interoperability of Calculi for System Modelling

PHL has already been embedded into KAT [9] and its soundness has been proven on that basis. We provide an alternative but equivalent semantic model in KAD that, however, allows a more direct embedding and proof. A second proof in modal operator semirings is even more abstract and concise. Moreover, our main application is a purely calculational algebraic proof of relative completeness that is much shorter and, by the underlying abstract axiomatization, applicable to a much wider class of models than the usual ones (such as e.g. in [1]). To our knowledge, a completeness proof in terms of Kleene algebra has not been given before. We model (the semantics of) partial correctness assertions in terms of backward diamonds and wlp in terms of forward boxes; this gives a purely algebraic wlp-calculus. In this, we can exploit the Galois connection between boxes and diamonds that is beyond the expressiveness of formalisms like propositional dynamic logic.

Another aim of the study is to show the ease of use and the wide applicability of the new framework of KAD and its modal offsprings. Its closest relative is relational algebra, in which many of the issues discussed above have already been treated (see e.g. [12]). Why should KAD offer an alternative? At first sight the absence of certain operations, such as converse, residuals, arbitrary complement or general fixpoint operators may even seem a drawback. Our experience, however, suggests the opposite. The economy of concepts in Kleene algebra imposes a discipline of thought which frequently leads to simpler and more perspicuous proofs. Also, KAD in fact *does* provide lean forms of converse, residuals and complement which suffice for many applications (see also [2,3,11]). Moreover, KAD admits trace-like models, which is beyond the treatment of pure input/output behaviour of relational models. Finally, both the sequential calculus [6] and the relational calculus define subclasses of KAD. Therefore we can carry out formal derivations at various, but coherent, levels of abstraction.

The remainder of this paper is organized as follows: Section 2 introduces KAD and its basic properties. Section 3 formalizes PHL within KAD. Section 4 defines the modal operators box and diamond in terms of domain and codomain and gives basic properties. The diamond operator is used in Section 5 to give a more convenient formalization of validity for a very concise algebraic soundness proof for PHL. In Sections 6, 7 and 8 we provide further properties of the modal operators, investigate their symmetries and consider them in a pointfree manner in operator semirings over KAD. This admits an even more concise treatment of the soundness of PHL in Section 10. The technical part of the paper is concluded with Section 11 that provides an abstract algebraic completeness proof for PHL over KAD. Section 12 gives a conclusion as well as a brief outlook.

2 Kleene Algebra with Domain

A *Kleene algebra* [7] 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

defined by the equations

$$1 + aa^* \leq a^*, \tag{$*$-1}$$
$$1 + a^*a \leq a^*, \tag{$*$-2}$$

and the Horn sentences

$$b + ac \leq c \Rightarrow a^*b \leq c, \tag{$*$-3}$$
$$b + ca \leq c \Rightarrow ba^* \leq c, \tag{$*$-4}$$

for all $a, b, c \in K$ (the operation $\cdot$ is omitted here and in the sequel). The relation $\leq$ is the natural ordering on K defined by $a \leq b$ iff $a + b = b$. Models of Kleene algebra are for instance the set-theoretic relations under set union, relational composition and reflexive transitive closure, and the sets of regular languages (regular events) over some finite alphabet.

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. $\neg$ 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* [8] is a two-sorted structure (K, B), where K is a Kleene algebra and $B \subseteq K$ is a Boolean algebra such that $0_K = 0_B$ and $1_K = 1_B$. 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. For all $p \in \mathsf{test}(K)$ we have that $p^* = 1$. The class of Kleene algebras with tests is denoted by KAT.

An element $a \in K$ with $K \in \mathsf{KAT}$ might describe an abstract program and a test $p \in \mathsf{test}(K)$ an assertion. Then pa describes a restricted program that acts like a when the starting state satisfies assertion p and aborts otherwise. Symmetrically, ap describes a restriction of a in its possible result states. We now introduce an operator δ that assigns to a its *domain*, that is, the test that describes precisely the starting states of a.

A *Kleene algebra with domain* [2] is a structure (K, δ), where $K \in \mathsf{KAT}$ and the *domain operation* $\delta : K \to \mathsf{test}(K)$ satisfies for all $a, b \in K$ and $p \in \mathsf{test}(K)$

$$a \leq \delta(a)a, \tag{d1}$$
$$\delta(pa) \leq p. \tag{d2}$$

Let us explain these axioms. First, since $\delta(a) \leq 1$ by $\delta(a) \in \mathsf{test}(K)$, monotonicity of multiplication shows that (d1) can be strengthened to an equality expressing that restriction to *all* possible starting states is no restriction at all. (d2) means that after restriction the remaining starting states must be contained in the restricting set. So these two axioms are quite reasonable. Despite their simplicity, they lead to a host of interesting and useful properties, among them uniqueness of the domain operation.

The class of Kleene algebras with domain is denoted by KAD. The impact of (d1) and (d2) can also be motivated as follows. (d1) and (d2) together are

equivalent to each of the statements

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

which constitute elimination laws for δ. (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. Both properties obviously characterize domain in set-theoretic relations.

Some applications require the additional domain axiom

$$\delta(a\delta(b)) \leq \delta(ab). \tag{d3}$$

Its significance will be discussed below. We will always explicitly mention its use and avoid it as long as possible.

The following properties of domain follow from the axioms (d1) and (d2):

$\delta(a) = 0 \Leftrightarrow a = 0,$	(strictness)
$\delta(a + b) = \delta(a) + \delta(b),$	(additivity)
$a \leq b \Rightarrow \delta(a) \leq \delta(b),$	(monotonicity)
$\delta(ab) \leq \delta(a\delta(b)),$	(decomposition)
$\delta(pa) = p\delta(a),$	(import/export)
$\delta(p) = p,$	(stability)
$\delta(ap) \leq p \Rightarrow \delta(a^*p) \leq p.$	(induction)

See [2] for proofs. (decomposition) is of particular interest. Its converse (d3) is independent of the axioms (d1) and (d2), but it holds, for instance, in the relational model. It ensures that the modal operators box and diamond to be introduced below distribute through multiplication. Interestingly, (decomposition) is sufficient to show soundness of propositional Hoare logic, whereas its converse (d3) is needed in the completeness proof.

It turns out that by the Galois-like characterization (llp) the domain and codomain operators are even fully additive, they are continuous, when the underlying test algebra is complete.

Proposition 2.1. *In* KAD*, domain commutes with all existing suprema.*

Proof. Let $A \subseteq K$ be some set such that $b = \sup(a : a \in A)$ exists. We show that

$$\delta(b) = \sup(\delta(a) : a \in A).$$

First, by monotonicity 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 $a \in A$, by (llp),

$$\delta(a) \leq p \Leftrightarrow a \leq pa \Rightarrow a \leq pb\ .$$

Hence pb is an upper bound of A and therefore $b \leq pb$. But by (llp) this is equivalent to $\delta(b) \leq p$. □

Given domain, it is easy to define a codomain operator ρ as domain operator in the opposite semiring. As usual in algebra, the *opposite* of a Kleene algebra $(K, +, \cdot, 0, 1, ^*)$ is the structure $(K, +, \breve{\cdot}, 0, 1, ^*)$ where $a \breve{\cdot} b = b \cdot a$.

Another possibility is offered by Kleene algebras with a converse operator. A *Kleene algebra with weak converse* is a structure $(K, ^\circ)$ such that K is a Kleene algebra and $^\circ : K \to K$ is an operation that satisfies the following axioms for all $a, b, p \in K$ with $p \leq 1$.

$$a^{\circ\circ} = a, \tag{c1}$$
$$(a + b)^\circ = a^\circ + b^\circ, \tag{c2}$$
$$(ab)^\circ = b^\circ a^\circ, \tag{c3}$$
$$(a^*)^\circ = (a^\circ)^* \tag{c5}$$
$$p^\circ \leq p. \tag{c5}$$

It follows that $p^\circ = p$ and $a \leq b \Leftrightarrow a^\circ \leq b^\circ$. Then the codomain operation can be defined as $\rho(a) = \delta(a^\circ)$.

3 Propositional Hoare Logic

In this section, we 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 $\phi_1 \to \phi_2$ for $\phi_1, \phi_2 \in \Phi$ defined as usual.

The set Σ of *statements* is defined by the grammar

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

To define a semantics, let $K \in \mathsf{KAD}$ and assign to each 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:

$$[\![\phi \wedge \psi]\!] = [\![\phi]\!][\![\psi]\!], \tag{1}$$
$$[\![\neg\phi]\!] = \neg[\![\phi]\!], \tag{2}$$
$$[\![\mathsf{abort}]\!] = 0, \tag{3}$$
$$[\![\mathsf{skip}]\!] = 1, \tag{4}$$
$$[\![\alpha\,;\,\beta]\!] = ab \tag{5}$$
$$[\![\ \mathsf{if}\ \phi\ \mathsf{then}\ \alpha\ \mathsf{else}\ \beta]\!] = [\![\phi]\!][\![\alpha]\!] + \neg[\![\phi]\!][\![\beta]\!], \tag{6}$$
$$[\![\ \mathsf{while}\ \phi\ \mathsf{do}\ \alpha]\!] = ([\![\phi]\!][\![\alpha]\!])^*\neg[\![\phi]\!]. \tag{7}$$

We call a proposition $\phi \in \Phi$ *valid*, in signs $\models \phi$, iff $[\![\phi]\!] = 1$. In particular,

$$\models \phi \to \psi \Leftrightarrow [\![\phi]\!] \leq [\![\psi]\!] \tag{8}$$

The basic formulas of Hoare logic are *partial correctness assertions* (PCAs) of the form $\{\phi\}\alpha\{\psi\}$, where ϕ and ψ (the *precondition* and the *postcondition*) are propositions and α is a statement. Following [9], a PCA $\{\phi\}\ \alpha\ \{\psi\}$ is *valid*, in signs $\models \{\phi\}\ \alpha\ \{\psi\}$ iff $pa\neg q \leq 0$, where $p = [\![\phi]\!]$, $a = [\![\alpha]\!]$ and $q = [\![\psi]\!]$. Using (llp) and Boolean algebra, we can rewrite this definition more intuitively as

$$\models \{\phi\}\ \alpha\ \{\psi\} \Leftrightarrow \rho(pa) \leq q. \tag{9}$$

Since $\rho(pa)$ denotes the set of all states that can be reached from states in p through a, the formula $\rho(pa) \leq q$ is indeed a faithful translation of the corresponding PCA. In the sequel we will always use the above abbreviations p, q, a etc. and liberally confuse syntax and semantics to shorten the notation.

Traditionally, the Hoare calculus consists of the following inference rules for reasoning about programs.

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

An inference rule with premises $P_1, \cdots, P_n$ and conclusion P is *sound*, if

$$\{P_1, \ldots, P_n\} \models P.$$

(Assignment) is a non-propositional inference rule that deals with the internal structure of states. Therefore we do not encode it directly into our framework. We rather use the set Γ of atomic commands as a parameter in the whole treatment. The requirement on Γ that ensures completeness of the calculus will be given in Section 11. Following [9], we call our abstract form of Hoare logic *propositional Hoare logic* (PHL).

4 Modal Operators

Before proving soundness and completeness of PHL, we present some more useful tools within KAD. In particular, using the domain and codomain operators we define various modal operators to set up the link to propositional dynamic logic. In the relational model, these operators are connected to preimage and image operators. The term *modal operator* is justified, since, as we will see, they can be interpreted as strict additive mappings on the test algebra of a Kleene algebra. They thus give rise to a Boolean algebra with operators in the sense of Jónsson and Tarski, thus an algebraic variant of a modal logic. Alternatively, these operators can be interpreted, respectively, as disjunctive or conjunctive predicate transformers (viewing tests as predicates that hold in a program state). This will give the connection to the syntax and semantics of Hoare logic. Our modal operators enjoy various symmetries. These are symmetries of two kinds. First, symmetries arising from dualities and second, symmetries arising from Galois connections. These will be discussed in Section 8.

The first definition introduces, as usual, the forward and backward diamond operators using preimage and image.

$$\langle a\rangle\!\rangle p = \delta(ap), \tag{10}$$

$$\langle\!\langle a\rangle p = \rho(pa). \tag{11}$$

Consequently, $\delta(a) = \langle a\rangle\!\rangle 1$ and $\rho a = \langle\!\langle a\rangle 1$. If the direction doesn't matter, we just write $\langle a\rangle p$ for both values.

Forward and backward diamond are related by duality with respect to converse:

$$\langle a\rangle\!\rangle p = \langle\!\langle a^\circ\rangle p = (\langle\!\langle a^\circ\rangle p)^\circ, \qquad \langle\!\langle a\rangle p = \langle a^\circ\rangle\!\rangle p = (\langle a^\circ\rangle\!\rangle p)^\circ. \tag{12}$$

Even if converse is not explicit in the language, image and preimage are related by an exchange law.

Lemma 4.1. *Let $K \in$ KAD. The following* exchange law *holds. For all $a \in K$ and $p, q \in \mathsf{test}(K)$,*

$$\langle a\rangle\!\rangle p \leq \neg q \Leftrightarrow \langle\!\langle a\rangle q \leq \neg p. \tag{13}$$

Proof. Expanding the definitions of forward and backward diamond to domain and codomain and using (gla) we obtain

$$\langle a\rangle\!\rangle p \leq \neg q \Leftrightarrow qap \leq 0 \Leftrightarrow \langle\!\langle a\rangle q \leq \neg p.$$

□

Consequently, we can always define a backward diamond in presence of a forward one and vice versa, even in absence of converse. Both operators are unique. Duality with respect to complementation transforms diamonds into boxes:

$$[a]\!]p = \neg\langle\!\langle a\rangle\neg p, \qquad [\![a]p = \neg\langle a\rangle\!\rangle\neg p. \tag{14}$$

The symmetry between boxes and diamonds is then expressed by the following Galois connections.

Lemma 4.2. *Let $K \in \mathsf{KAD}$. For all $a \in K$, the operators $\langle a\rangle\!\rangle$ and $[\![a]$ as well as $\langle\!\langle a\rangle$ and $[a]\!]$ are the lower and upper adjoints of a Galois connection. That is, for all $p, q \in \mathsf{test}(K)$,*

$$\langle a\rangle\!\rangle p \leq q \Leftrightarrow p \leq [\![a]q, \qquad \langle\!\langle a\rangle p \leq q \Leftrightarrow p \leq [a]\!]q. \tag{15}$$

Proof. Immediate from (13) and (14). □

Exploiting the symmetries further immediately yields the dualities

$$[a]\!]p = ([\![a^\circ]p)^\circ, \qquad [\![a]p = ([a^\circ]\!]p)^\circ \tag{16}$$

and the exchange law

$$[a]\!]p \leq \neg q \Leftrightarrow [\![a]q \leq \neg p. \tag{17}$$

In later sections, we will use these Galois connections as theorem generators and the dualities as theorem transformers.

5 Soundness of Propositional Hoare Logic

In this section we present a first proof for the fact that PHL is subsumed by KAD. This subsumption is a popular exercise for many logics and algebras for imperative programming languages. PHL, for instance, has already been embedded into propositional dynamic logic [4] and KAT [9]. Since KAD is an extension of KAT, our subsumption result is no surprise. However we believe that it is interesting for two reasons. First, in KAD, an encoding of the inference rules of PHL is much more crisp and clear and so are the soundness proofs. Moreover, Hoare-style reasoning about programs can be done in a more flexible way in KAD. Second, the properties used in the standard partial correctness semantics [10,1] for Hoare logic are precisely mirrored by those of the domain operator, so that KAD may be considered a natural abstract algebraic semantics for PHL.

We have defined validity of a PCA $\{\phi\}\ \alpha\ \{\psi\}$ with respect to codomain in (9). Using the backward diamond this can be expressed equivalently as

$$\models \{\phi\}\ \alpha\ \{\psi\} \Leftrightarrow \langle\!\langle a\rangle p \leq q. \tag{18}$$

Thus we can encode the soundness conditions for the PHL rules quite succinctly:

$$\left.\begin{array}{ll}
\text{(Abort)} & \langle\!\langle 0\rangle p \leq q, \\
\text{(Skip)} & \langle\!\langle 1\rangle p \leq p, \\
\text{(Composition)} & \langle\!\langle a\rangle p \leq q \wedge \langle\!\langle b\rangle q \leq r \Rightarrow \langle\!\langle ab\rangle p \leq r, \\
\text{(Conditional)} & \langle\!\langle a\rangle(pq) \leq r \wedge \langle\!\langle b\rangle(\neg pq) \leq r \Rightarrow \langle\!\langle pa + \neg pb\rangle q \leq r, \\
\text{(While)} & \langle\!\langle a\rangle(pq) \leq q \Rightarrow \langle\!\langle (pa)^*\neg p\rangle q \leq \neg pq, \\
\text{(Weakening)} & p_1 \leq p \wedge \langle\!\langle a\rangle p \leq q \wedge q \leq q_1 \Rightarrow \langle\!\langle a\rangle p_1 \leq q_1.
\end{array}\right\} \tag{19}$$

Based on this encoding, we obtain a first simple calculational soundness proof for PHL. The encoding and proof will be further abstracted in Section 10. We present this first proof for two reasons. First, it allows a direct comparison with Kozen's KAT-based approach [9]. Second, it illustrates the gain of the further abstraction.

Theorem 5.1. PHL *is sound in* KAD*; the encoded rules of* PHL *are theorems of* KAD*.*

Proof. All parts of the proof follow immediately from lifting the properties of domain in Section 2 to modal backward diamonds. Corresponding properties for modal operators are collected in Section 9.

(Abort) is trivial by (strictness).

(Skip) is trivial by (stability).

(Composition) $\langle\!\langle ab\rangle\!\rangle p \leq \langle\!\langle b\rangle\!\rangle(\langle\!\langle a\rangle\!\rangle p) \leq \langle\!\langle b\rangle\!\rangle p \leq r$, by (decomposition).

(Conditional) $\langle\!\langle pa + \neg pb\rangle\!\rangle q = \langle\!\langle pa\rangle\!\rangle q + \langle\!\langle \neg pb\rangle\!\rangle q \leq r + r = r$, by (additivity).

(While) Using (induction), we calculate

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

(Weakening) $\langle\!\langle a\rangle\!\rangle p_1 \leq \langle\!\langle a\rangle\!\rangle p \leq q \leq q_1$, by (monotonicity). □

Thus, given our calculus for modal operators, soundness of PHL can be proved literally in one line per inference rule from natural properties of KAD. Comparing with KAT, we believe that our encodings and proofs in KAD are more direct, elegant and intuitive. Compared to standard set-theoretic textbook proofs (c.f [10,1]), our proof is about ten times shorter, without taking into account the fact that many logical and set-theoretic assumptions are left implicit in the textbook proofs and the proofs are only semi-formal.

We now compare our embedding in KAD with the KAT-based approach in [9]. E.g., (Composition) of PHL must now be encoded more indirectly as

$$pa \leq aq \wedge qb \leq br \Rightarrow pab \leq abr. \tag{20}$$

We can obtain this encoding also in KAD, using (llp). We can also obtain the equivalent encoding (in KAD and KAT)

$$pa\neg q \leq 0 \wedge qb\neg r \leq 0 \Rightarrow pab\neg r \leq 0, \tag{21}$$

using (gla). For computational purposes, (21) is quite convenient, since hypotheses of this form can be eliminated [5], whence Hoare-style reasoning in KAT becomes purely equational. This result is of general interest for KAD, since a reduction via (llp) or (gla) from KAD to equational KAT can lead to efficient automata-based decision procedures. Moreover, we obtain a simple characterization of a fragment of KAD that is in PSPACE.

A *Hoare formula* in KAD is a universal Horn formula whose literals are of the form $s \leq p$ such that p is a KAT term of Boolean sort and s is either a KAT

term or a term $\langle a\rangle p$ where p and a are KAT terms. Note that 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 5.2. *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 KAD ϕ 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 "demodalization" result to further classes of KAD formulas.

6 Soundness of Some Derived Hoare Rules

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

Lemma 6.1. *The following axioms and inference rules are sound with respect to the semantics of* PHL*.*

(i) Let $pa = ap$. 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) Let $pa = ap$. Then

$$\frac{\{q\}\ a\ \{r\}}{\{p\wedge q\}\ a\ \{p\wedge r\}}.$$

Proof. (i) Trivial.

(ii) We must show that $\langle\!\langle a\rangle p \leq q$ and $\langle\!\langle b\rangle p \leq r$ imply $\langle\!\langle a+b\rangle p \leq q+r$. By (additivity),

$$\langle\!\langle a+b\rangle p = \langle\!\langle a\rangle p + \langle\!\langle b\rangle p \leq q+r.$$

(iii) We must show that $\langle\!\langle a\rangle p \leq r$ and $\langle\!\langle a\rangle q \leq r$ imply $\langle\!\langle a\rangle(p+q) \leq r$. By (additivity),

$$\langle\!\langle a\rangle(p+q) = \langle\!\langle a\rangle p + \langle\!\langle a\rangle q \leq r+r = r.$$

(iv) We must show that $\langle\!\langle a\rangle p_1 \leq q_1$ and $\langle\!\langle a\rangle p_2 \leq q_2$ imply $\langle\!\langle a\rangle(p_1p_2) \leq q_1q_2$. In this case it seems that reasoning without diamonds yields a simpler proof. By (llp) and Boolean algebra, the assumptions are equivalent to $p_1a \leq aq_1$ and $p_2a \leq aq_2$. Then

$$p_1p_2a \leq p_1aq_2 \leq aq_1q_2.$$

Thus $\langle\!\langle a\rangle p_1p_2 \leq q_1q_2$.

(v) Assume that $pa = ap$. We must show that $\langle\!\langle a\rangle q \leq r$ implies $\langle\!\langle a\rangle(pq) \leq pr$. By (llp), the assumption is equivalent to $qa \leq ar$ and hence

$$pqa = qpa = qap \leq rp.$$

□

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.

We encourage the reader to try proofs using domain, where we did proofs without and vice versa. This will show that the flexibility of switching between KAD and KAT pays. We also 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 [9] that in Kleene algebra *the specialized syntax and deductive apparatus of Hoare logic are inessential and can be replaced by simple equational reasoning.* Hence KAD offers an elegant formal calculus and a simple algebraic semantics for reasoning in and about Hoare logic. We also believe that KAD offers even further advantages. It allows us to combine the intuitiveness and readability of specifications in Hoare logic and imperative program semantics with the computational power of KAT.

7 Modal Operator Semirings

Many properties of KAD can be expressed and calculated more succinctly in a pointfree style in the operator semirings induced by the modal operators.

Proposition 7.1. *Let $\langle K\rangle$ be the set of all mappings $\lambda x.\langle a\rangle x$ with $a \in K$ on some i-semiring K. Defining addition and multiplication on $\langle K\rangle$ by*

$$(\langle a\rangle + \langle b\rangle)(p) = \langle\!\langle a\rangle p + \langle\!\langle b\rangle p, \tag{22}$$

$$(\langle a\rangle \cdot \langle b\rangle)(p) = \langle\!\langle a\rangle(\langle\!\langle b\rangle p), \tag{23}$$

the structure $(\langle K\rangle\!\rangle, +, \cdot, \langle 0\rangle\!\rangle, \langle 1\rangle\!\rangle)$ *is an i-semiring, the* forward diamond semiring.

Dually, the structure $(\langle\!\langle K\rangle, +, \cdot, \langle\!\langle 0\rangle, \langle\!\langle 1\rangle)$ *with addition and multiplication defined in the obvious way is an i-semiring, the* backward diamond semiring.

Proposition 7.2. *Let* $[K]\!]$ *be the set of all mappings* $\lambda x.[a]\!]x$ *with* $a \in K$ *on some i-semiring* K*. Defining addition and multiplication on* $[K]\!]$ *by*

$$([a]\!] + [b]\!])(p) = ([a]\!]p)([b]\!]p), \tag{24}$$

$$([a]\!] \cdot [b]\!])(p) = [a]\!]([b]\!]p), \tag{25}$$

the structure $([K]\!], +, \cdot, [0]\!], [1]\!])$ *is an i-semiring, the* forward box semiring.

Dually, the structure $([\![K], +, \cdot, [\![0], [\![1])$ *with addition and multiplication defined in the obvious way is an i-semiring, the* backward box semiring.

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

Lemma 7.3. *Let* $K \in \mathsf{KAD}$*.*

(i) For all $p \in \mathsf{test}(K)$*,* $\langle 0\rangle\!\rangle p = 0 = \neg[0]\!]p$ *.*
(ii) $\langle 1\rangle\!\rangle = [1]\!]$*.*

We see that from box to diamond semirings, the Boolean lattice is turned upside down. We will henceforth use the operators semirings for lifting KAD expressions and write $f = g$ instead of $\forall p \,.\, fp = gp$, where f and g denote arbitrary combinations of boxes and diamonds.

8 Symmetries of Modal Operators

We now investigate the symmetries between the modal operators that arise from the Galois connections and from the dualities of converse and complementation. The Galois connections (15) give us theorems for free. The following two statements are immediate.

Lemma 8.1. *Let* $K \in \mathsf{KAD}$*. For all* $a \in K$*, the following* cancellation laws *hold.*

$$\langle a\rangle\!\rangle[a]\!] \leq \langle 1\rangle\!\rangle \leq [a]\!]\langle a\rangle\!\rangle. \tag{26}$$

Proposition 8.2. *Let* $K \in \mathsf{KAD}$*.*

(i) The operators $\langle a\rangle\!\rangle$ *and* $[a]\!]$ *commute with all existing suprema and infima, respectively.*
(ii) If $\mathsf{test}(K)$ *is a complete Boolean lattice then* $\langle a\rangle\!\rangle$ *is universally disjunctive and* $[a]\!]$ *is universally conjunctive, that is, they commute with all suprema and infima, respectively.*

Proof. Since in KAD boxes and diamonds are upper and lower adjoints of a Galois connection (see Lemma 4.2), the results follow from general properties of Galois connections. □

Lemma 8.3. *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.*

Proof. We only consider the proof for addition, the one for multiplication being dual. Let $Q \subseteq \mathsf{test}(K)$ We show that $\sup(q + p : q \in Q) = \sup(q : q \in Q) + p$. First, $\sup(q : q \in Q) + p$ is an upper bound of the $p + q$ by monotonicity of $+$. We now show that $\sup(q : q \in Q) + p$ is a least upper bound. So let r be another upper bound, that is $p + q \leq r$ for all $q \in Q$. Then

$$q + p \leq r \Leftrightarrow q \leq r\neg p \Leftrightarrow \sup(q : q \in Q) \leq r\neg p \Leftrightarrow \sup(q : q \in Q) + p \leq r.$$

□

As a consequence, we obtain the following proposition from Proposition 8.2, Lemma 8.3 and Kleene's fixed-point theorem.

Proposition 8.4. *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,*

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

In order to transform theorems, we introduce two duality operators on the space of box and diamond operators over a Boolean algebra. In general, we set $\partial^\pi f = \pi f \pi$, where f is a modal operator and π one of $\neg$ or $\circ$. $\partial^\neg$ is a bijection between $\langle\!\langle K\rangle$ and $[\![K]$ as well as $\langle K\rangle\!\rangle$ and $[K]\!]$, whereas ∂° is a bijection between $\langle K\rangle\!\rangle$ and $\langle\!\langle K\rangle$ and $[K]\!]$ and $[\![K]$, respectively. This yields

$$\partial^\neg : \langle a\rangle \mapsto [a], [a] \mapsto \langle a\rangle, \tag{27}$$

$$\partial^\circ : \langle a\rangle\!\rangle \mapsto \langle\!\langle a\rangle, \langle\!\langle a\rangle \mapsto [a]\!], [a]\!] \mapsto [\![a], [\![a] \mapsto [a]\!]. \tag{28}$$

$\partial^\neg$ and ∂° can be extended to Boolean elements in the standard way, using the de Morgan laws and the defining laws of converse, respectively. It is easy to see that $\partial^\neg$ and ∂° are involutory, that is, $\partial^\neg\partial^\neg = \partial^\circ\partial^\circ = id$, and that $\partial^\neg\partial^\circ = \partial^\circ\partial^\neg$. We will strongly use both dualities for translating theorems.

9 Properties of Modal Operators

In this section, we collect some properties of boxes and diamonds that follow either from the definition of domain or from the Galois connections. Here, we only present statements for forward diamond and box. Corresponding statements for the remaining modal operators can immediately be inferred by dualization.

Lemma 9.1. *Let $K \in \mathsf{KAD}$. For all $a, b \in K$ and $p, q \in \mathsf{test}(K)$,*

$$\langle a + b\rangle\!\rangle = \langle a\rangle\!\rangle + \langle b\rangle\!\rangle, \tag{29}$$

$$\langle ab\rangle\!\rangle \leq \langle a\rangle\!\rangle\langle b\rangle\!\rangle, \tag{30}$$

$$a \leq b \Rightarrow \langle a\rangle\!\rangle \leq \langle b\rangle\!\rangle, \tag{31}$$

$$\langle paq\rangle\!\rangle = \langle p\rangle\!\rangle\langle a\rangle\!\rangle\langle q\rangle\!\rangle. \tag{32}$$

In the presence of (d3) property (30) can be strengthened to an equality.

See [2] for proofs. From this lemma we immediately obtain the following rules for box by dualization with respect to $\partial^\neg$.

Lemma 9.2. *Let $K \in \mathsf{KAD}$. For all $a, b \in K$ and $p, q \in \mathsf{test}(K)$,*

$$[a+b]q = ([a]q)([b]q), \tag{33}$$
$$[ab] \geq [a][b], \tag{34}$$
$$a \leq b \Rightarrow [a] \geq [b], \tag{35}$$
$$[paq] = [p][a][q], \tag{36}$$
$$[pa]q = \neg p + [a]q. \tag{37}$$

In the presence of (d3) property (34) can be strengthened to an equality.

Further point-wise properties follow immediately from the definition and properties of domain in Section 2 and Galois connection (15).

Lemma 9.3. *Let $K \in \mathsf{KAD}$. Then for all $a \in K$, $\langle a\rangle$ is a strict, additive and monotonic mapping, that is, for all $p, q \in \mathsf{test}(K)$,*

$$\langle a\rangle 0 = 0, \tag{38}$$
$$\langle a\rangle(p+q) = \langle a\rangle p + \langle a\rangle q, \tag{39}$$
$$p \leq q \Rightarrow \langle a\rangle p \leq \langle a\rangle q. \tag{40}$$

Again, $\partial^\neg$-dualization yields the following pointwise properties of boxes.

Lemma 9.4. *Let $K \in \mathsf{KAD}$. Then for all $a \in K$, $[a]$ is a costrict, multiplicative and monotonic mapping, that is, for all $p, q \in \mathsf{test}(K)$,*

$$[a]1 = 1, \tag{41}$$
$$[a](pq) = ([a]p)([a]q), \tag{42}$$
$$p \leq q \Rightarrow [a]p \leq [a]q. \tag{43}$$

As a consequence of strictness and additivity and of costrictness and multiplicativity, respectively, the structures $(\mathsf{test}K, \{\langle a\rangle : a \in K\})$ and $(\mathsf{test}K, \{[a] : a \in K\})$ are *Boolean algebras with operators* in the sense of Jónsson and Tarski. This also justifies calling our boxes and diamonds *modal operators*.

We now investigate the relation between $\langle a\rangle^*$ and $\langle a^*\rangle$.

Lemma 9.5. *Let $K \in \mathsf{KAD}$. For all $a \in K$,*

(i) $\langle 1\rangle + \langle aa^*\rangle = \langle a^*\rangle$,
(ii) $\langle 1\rangle + \langle a\rangle\langle a^*\rangle \geq \langle a^*\rangle$,
(iii) $\langle 1\rangle + \langle a\rangle\langle a^*\rangle = \langle a^*\rangle$, *if (d3) holds.*

Lemma 9.6. *Let $K \in \mathsf{KAD}$. For all $a, b, c \in K$,*

$$\langle a\rangle \leq \langle 1\rangle \Rightarrow \langle a^*\rangle \leq \langle 1\rangle, \tag{44}$$
$$\langle b\rangle + \langle a^*\rangle\langle c\rangle \leq \langle c\rangle \Rightarrow \langle a^*\rangle\langle b\rangle \leq \langle c\rangle. \tag{45}$$

Proofs can be found in [2]. Thus we have the following theorems.

Proposition 9.7. *Let $K \in \mathsf{KAD}$ and let $\mathsf{test}(K)$ be a complete Boolean lattice. Then for all $a \in K$,*

$$\langle a^* \rangle = \langle a \rangle^*. \tag{46}$$

Thus for the case of complete Boolean lattices, we can expand our modal operators semirings to modal operator Kleene algebras.

Proposition 9.8. *Let $K \in \mathsf{KAD}$ and let $\mathsf{test}(K)$ be a complete Boolean lattice. Then the i-semiring $\langle K \rangle$ can be uniquely extended to a (left-handed) Kleene algebra.*

As a consequence, when test algebras in KAD are complete, the modal operators form again 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 new layer of abstraction. A more thorough investigation of this perspective is, however, beyond the scope of this text.

10 Soundness of Propositional Hoare Logic Revisited

We now show that the abstraction from KAD to operator semirings admits an even more concise treatment of soundness of PHL than that in Section 5. We first lift the encoding (19) of the inference rules, using the *principle of indirect inequality*, which says that $p \leq q$ iff $q \leq r$ implies $p \leq r$ for all r.

Proposition 10.1. *Let $K \in \mathsf{KAD}$. Then the soundness conditions for the inference rules of PHL can be encoded as follows.*

(Abort)	$\langle\!\langle 0 \rangle\!\rangle \leq \langle\!\langle q \rangle\!\rangle$,
(Skip)	$\langle\!\langle 1 \rangle\!\rangle \leq \langle\!\langle 1 \rangle\!\rangle$,
(Composition)	$\langle\!\langle ab \rangle\!\rangle \leq \langle\!\langle b \rangle\!\rangle \langle\!\langle a \rangle\!\rangle$,
(Conditional)	$\langle\!\langle pa + \neg pb \rangle\!\rangle \leq \langle\!\langle p \rangle\!\rangle \langle\!\langle a \rangle\!\rangle + \langle\!\langle \neg p \rangle\!\rangle \langle\!\langle b \rangle\!\rangle$,
(While)	$\langle\!\langle p \rangle\!\rangle \langle\!\langle a \rangle\!\rangle \leq \langle\!\langle 1 \rangle\!\rangle \Rightarrow \langle\!\langle (pa)^* \rangle\!\rangle \langle\!\langle \neg p \rangle\!\rangle \leq \langle\!\langle \neg p \rangle\!\rangle$,

Proof. We show that the pointwise and pointfree encodings are equivalent.

(Abort) Let $\langle 0 \rangle \leq \langle q \rangle$. Then $\langle\!\langle 0 \rangle\!\rangle p \leq \langle\!\langle q \rangle\!\rangle p = qp \leq q$.

Let $\langle\!\langle 0 \rangle\!\rangle p \leq q$. In particular, we also have $\langle\!\langle 0 \rangle\!\rangle p \leq p$ and therefore $\langle\!\langle 0 \rangle\!\rangle p \leq pq = \langle\!\langle q \rangle\!\rangle p$, whence $\langle 0 \rangle \leq \langle q \rangle$.

(Skip) Obvious.

(Composition) Assume the pointwise encoding. The antecedent and monotonicity imply that

$$\langle\!\langle b \rangle\!\rangle (\langle\!\langle a \rangle\!\rangle p) \leq r \Rightarrow \langle\!\langle ab \rangle\!\rangle p \leq r,$$

whence $\langle\!\langle ab\rangle q \leq \langle a\rangle(\langle\!\langle b\rangle p)$ and $\langle\!\langle ab\rangle \leq \langle b\rangle\langle\!\langle a\rangle$ by multiplication in $\langle\!\langle K\rangle$.

Assume the pointfree encoding and let $\langle\!\langle a\rangle p \leq q$ and $\langle\!\langle b\rangle q \leq r$. Then

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

(Conditional) Assume the pointwise encoding. Then the antecedent is equivalent to $\langle\!\langle a\rangle(\langle\!\langle p\rangle q) \leq r \wedge \langle\!\langle b\rangle(\langle\!\langle \neg p\rangle q) \leq r$, hence to $(\langle\!\langle p\rangle\langle\!\langle a\rangle + \langle\!\langle \neg p\rangle\langle\!\langle b\rangle)(q) \leq r$. Then the pointfree encoding follows with the principle of indirect inequality.

Assume the pointfree encoding and let $\langle\!\langle a\rangle(pq) \leq r$ and $\langle\!\langle b\rangle(\neg pq) \leq r$. Then

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

(While) Assume the pointwise encoding. Then the antecedent is equivalent to $(\langle\!\langle p\rangle\langle\!\langle a\rangle)q \leq q$, while the succedent is equivalent to $(\langle\!\langle (pa)^*\rangle\langle \neg p\rangle)q \leq \langle\!\langle \neg p\rangle q$. This yields the pointfree encoding.

Assume the pointfree encoding. Then use the converse translation. □

Note that the encoding in Proposition 10.1 reflects the operational content of the PHL-rules much better than that in (19). (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.

Note also that for each inference rule, the proof from pointfree to pointwise is essentially just one line. We did not present a pointfree variant of (Weakening), since that rule deals with points in an essential way. As a consequence of the direction from pointfree to pointwise in Proposition 10.1, we obtain the following alternative soundness proof for PHL.

Theorem 10.2. *The pointfree versions of the* PHL *rules are theorems in* KAD.

Proof. The pointfree variants of (Abort) and (Skip) are trivial consequences of Lemma 7.3. The pointfree variant of (Composition) is nothing but (30). The pointfree variant of (Conditional) is evident from (29), (30), (32) together with the definition of multiplication in $[\![K]\!]$. (While) follows immediately from (44) and monotonicity. (Weakening) follows immediately from monotonicity. □

Moreover, it has already been observed in [9] that all Horn clauses built from partial correctness assertions in Hoare logic that are valid with respect to the standard semantics are theorems of KAT. This result holds a fortiori for KAD. PHL is too weak to derive all such formulas [9]. Thus Kleene algebra has not only the derivable, but also the admissible inference rules of PHL as theorems.

11 Completeness of Propositional Hoare Logic

Completeness of the inference rules of PHL is usually proved with respect to 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

$$\mathsf{wlp}(P,T) = \{s \in S : P(s) \subseteq T\}, \tag{47}$$

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 one can therefore identify the wlp-operator with the forward box operator, as is well-known. In particular, using (18),(15) and (8), for $p = [\![\phi]\!]$, $a = [\![\alpha]\!]$ and $q = [\![\psi]\!]$

$$\models \{\phi\}\ \alpha\ \{\psi\} \ \Leftrightarrow\ p \leq [a]q \ \Leftrightarrow\ p \to [a]q. \tag{48}$$

Therefore, we get the complete wlp-calculus for free by dualizing our results from Sections 8 and 9 using $\partial^\neg$ and ∂°. Examples have been given in Section 9.

For the standard completeness proofs (see e.g. [1]) it is crucial that the underlying assertion language is strong enough. We therefore assume that the language Φ is *sufficiently rich*, i.e., 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.,

$$[\![\phi]\!] = \mathsf{wlp}([\![\alpha]\!], [\![\psi]\!]). \tag{49}$$

This assumption allows us to continue working at the semantical level in the following way. We embed the original calculus into one where all predicates are denoted by propositional variables and show completeness of this extended calculus. This will finally imply completeness of the original calculus.

To achieve this, we must add an axiom for the atomic commands $\gamma \in \Gamma$, viz., for $g = [\![\gamma]\!]$ and arbitrary test q,

$$\{[g]q\}\ g\ \{q\}. \tag{50}$$

(Assignment) has precisely that form.

Before giving the completeness proof, we show some technical properties of boxes. Logical variants appear in [1].

Proposition 11.1. *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,

$$p([c]q) = p([a]q), \tag{51}$$
$$\neg p([c]q) = \neg p([b]q). \tag{52}$$

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

$$p([w]q) = [a]([w]q), \tag{53}$$
$$\neg p([w]q) \leq q. \tag{54}$$

Proof. (i) For (51), first note that, by (33) and (37),

$$[c]q = ([pa]q)([\neg pb]q) = (\neg p + [a]q)(p + [b]q) = p([a]q) + \neg p([b]q) + ([a]q)([b]q).$$

Hence

$$p([w]q) = p([a]q) + p([a]q)([b]q) = p([a]q)$$

by $[b]q \leq 1$ and monotonicity. The proof of (52) is similar.

(ii) For (53), we calculate using Lemma 9.2

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

For (54), we calculate, using the first three steps from the proof of (53),

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

□

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

Lemma 11.2. *Let $K \in \mathsf{KAD}$ satisfy (d3). 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. As usual, we write $\vdash \{q\}\ a\ \{q\}$ to state that $\{q\}\ a\ \{q\}$ is derivable in PHL. We now prove the claim 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) $a = b\,;\, c = bc$. 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 Lemma 9.2 is the same as $\vdash \{[bc]q\}\ bc\ \{q\}$.

(iii) $a =$ if p then b 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 (51) and (52) 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) $a =$ $\mathsf{while}\ p\ \mathsf{do}\ b$. Let $c = [a]q$. By the induction hypothesis,

$$\vdash \{[a]c\}\ a\ \{c\}.$$

By (53) this is equivalent to $\vdash \{pc\}\ b\ \{c\}$. (While) shows that $\vdash \{c\}\ a\ \{\neg pc\}$ and (54) and (Weakening) yield $\vdash \{[a]q\}\ a\ \{q\}$, as required, □

We are now prepared for our main theorem.

Theorem 11.3. PHL *is relatively complete for partial correctness of deterministic programs in* KAD *with (d3).*

Proof. We must show that $\models \{p\}\ a\ \{q\}$ implies $\vdash \{p\}\ a\ \{q\}$. This follows by (48), Lemma 11.2 and (Weakening). □

Alternatively, we could also use our codings of PCAs in KAD in the completeness proof. We could write $\langle a\rangle_{\vdash} p \leq q$ 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 $\langle a\rangle_{\vdash}([a]p) \leq p$, or even $\langle a\rangle_{\vdash}[a] \leq \langle 1\rangle$, looks very much like a cancellation property of a Galois connection. This fact certainly deserves further consideration.

12 Conclusion and Outlook

We have presented the algebraic framework KAD of Kleene algebra with domain. We have derived and investigated the structure of various modal operators that arise in KAD. We have used the abstract propositional Hoare logic PHL as our running example for the use of that framework. We hope to have convinced the reader that KAD is a simple but powerful, flexible and convenient tool for treating modal operators and investigating properties of sequential programs and state transition systems in a calculational algebraic way. It should be clear that KAD also admits a straightforward treatment of programs with bounded nondeterminacy. We obtain, for instance, the following encoding of guarded commands.

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

There are several issues that we could not treat in this paper.

First, we believe that our result on demodalization in Section 5 deserves further investigation, in order to identify subclasses of PHL for which polynomial or exponential reductions to equational KAT exist.

Second, the modal operator semirings and Kleene algebras from Section 8 seem very interesting as a means of abstraction. Since our modal operators are also predicate transformers, these structures are essentially predicate transformer

algebras that allow us to derive properties of predicate transformers in a very succinct and abstract way.

Third, since KAD allows us to specify both the syntax and relational semantics of modal operators in one single formalism, it seems very promising to develop a calculational modal correspondence theory in KAD. First steps have been taken in [2,11].

Finally, we would like to mention that further applications of KAD and the associated modal operators are given in [2,11]. It is a challenging task to apply the framework of KAD to other problems in order to further evaluate its practical applicability.

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. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. Technical Report 2003-07, Universität Augsburg, Institut für Informatik, June 2003.
3. T. Ehm, B. Möller, and G. Struth. Kleene modules. In R. Berghammer and B. Möller, editors, *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 21–27. Universität Kiel, Germany, 2003.
4. J. M. Fischer and R. F. Ladner. Propositional dynamic logic of regular programs. *J. Comput. System Sci.*, 18(2):194–211, 1979.
5. 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.
6. C. A. R. Hoare and B. von Karger. Sequential calculus. *Information Processing Letters*, 53(3):123–130, 1995.
7. D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.
8. D. Kozen. Kleene algebra with tests. *Trans. Programming Languages and Systems*, 19(3):427–443, 1997.
9. D. Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1(1):60–76, 2001.
10. J. Loeckx and K. Sieber. *The Foundations of Program Verification.* Wiley Teubner, 2nd edition, 1987.
11. B. Möller and G. Struth. Greedy-like algorithms in Kleene algebra. In R. Berghammer and B. Möller, editors, *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 173–180. Universität Kiel, Germany, 2003.
12. G. W. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists.* EATCS Monographs on Theoretical Computer Science. Springer, 1993.