On the Representation of Kleene Algebras with Tests

Dexter Kozen
Department of Computer Science
Cornell University
Ithaca, New York 14853-7501, USA
kozen@cs.cornell.edu

September 18, 2003

Abstract

We investigate conditions under which a given Kleene algebra with tests is isomorphic to an algebra of binary relations. Two simple separation properties are identified that, along with star-continuity, are sufficient for nonstandard relational representation. An algebraic condition is identified that is necessary and sufficient for the construction to produce a standard representation.

1 Introduction

Kleene algebra with tests (KAT) is an equational system for program verification that combines Kleene algebra (KA), or the algebra of regular expressions, with Boolean algebra. One can model basic programming language constructs such as conditionals and while loops, verification conditions, and partial correctness assertions. KAT has been applied successfully in verification tasks involving communication protocols, source-to-source program transformation, concurrency control, compiler optimization, and dataflow analysis [1, 2, 4, 5, 20, 23]. The system subsumes Hoare logic and is deductively complete for partial correctness over relational models [21].

There are many interesting and useful models of KAT: language-theoretic, relational, trace-based, matrix. In programming language semantics and verification, the relational models are of primary importance, because correctness conditions are often expressed as input/output conditions on the start and final state of the computation.

In relational models, actions and tests are represented as binary relations on some universal set of states. The class of all relational KATs is denoted REL. Because of the prominence of relational models in programming language semantics and verification, it is of interest to characterize them axiomatically or otherwise. It is known that REL satisfies no more equations than those satisfied by KATs in general, and the equational theory is *PSPACE*-complete [6]. This result extends to the *Hoare theory*, universal Horn formulas in which all premises are of the form $\mathsf{p} = 0$ [6, 24]. However, the full

Horn theories of REL and KAT diverge: the relationally valid Horn formula $\mathsf{p} \le 1 \to \mathsf{p}^2 = \mathsf{p}$ is not true in all KATs or even in all star-continuous KATs. For example, it fails in the min,+ algebra or *tropical semiring* used in shortest path algorithms.

In this paper we explore conditions under which a Kleene algebra with tests can be represented isomorphically as a relational KAT. Not all algebras are so representable, even star-continuous ones; as observed above, the min,+ algebra is not. We have identified two basic first-order properties, Properties 3.1 and 3.2 below, that are sufficient for relational representation of idempotent semirings with tests, or Kleene algebras without *. In the presence of *, these properties plus the infinitary star-continuity condition are sufficient for representation by a *nonstandard* relational model—one in which p^* is the least reflexive transitive relation containing p *in the algebra*, although not necessarily the set-theoretic reflexive transitive closure. We also identify a property that is equivalent to the assertion that the construction yields a standard model.

The two properties 3.1 and 3.2 can be viewed as *separation properties*. Essentially, they assert the existence of enough tests to allow binary relations to be characterized by their observable behavior, where the tests of the algebra are the observations. The two conditions are relatively weak, although for trivial reasons neither is a necessary condition for representation. We discuss the significance of Properties 3.1 and 3.2 further in Section 3 below.

The Stone representation theorem (see e.g. [3, 11]) asserts that every Boolean algebra is isomorphic to a Boolean algebra of sets. After McKinsey's [28] and Tarski's [33] axiomatization of relation algebras, several authors [9, 13, 29] searched for a similar representation result for relation algebras but with only partial success. This work culminated in a counterexample of Lyndon [27]. In his conclusion, Lyndon discussed the possibility of a positive representation result in weaker systems. He mentioned specifically *relational rings*, which are essentially idempotent semirings or Kleene algebras without *. Work on the relational representation of dynamic algebra [16, 15, 17, 18, 32, 31] built on this work and is analogous to the present results in the stronger setting in which all weakest preconditions are assumed to exist. The main result of this paper strengthens the representation results of [16, 18] in that respect.

2 Preliminary Definitions

2.1 Kleene Algebra

Kleene algebra (KA) is the algebra of regular expressions [14, 7]. The axiomatization used here is from [19]. A *Kleene algebra* is an algebraic structure $(K, +, \cdot, ^*, 0, 1)$ that is an idempotent semiring under $+, \cdot, 0, 1$ such that $\mathsf{p}^*\mathsf{q}$ is the $\le$-least solution to $\mathsf{q} + \mathsf{px} \le \mathsf{x}$ and qp^* is the $\le$-least solution to $\mathsf{q} + \mathsf{xp} \le \mathsf{x}$. Here $\le$ refers to the natural partial order on K: $\mathsf{p} \le \mathsf{q} \stackrel{\text{def}}{\iff} \mathsf{p} + \mathsf{q} = \mathsf{q}$. This is a universal Horn axiomatization. A Kleene algebra is *star-continuous* if it satisfies the stronger infinitary property

$$\mathsf{pq}^*\mathsf{r} \quad = \quad \sup_n \mathsf{pq}^n\mathsf{r}. \tag{1}$$

The family of star-continuous Kleene algebras is denoted KA^*. It is a proper subclass of the Kleene algebras, but all naturally occurring Kleene algebras, including all relational models, are star-continuous.

The axioms for * say essentially that * behaves like the Kleene asterate operator of formal language theory or the reflexive transitive closure operator of relational algebra.

Standard models include the family of regular sets over a finite alphabet; the family of binary relations on a set; and the family of $n \times n$ matrices over another Kleene algebra. Other interpretations include the min,+ algebra or *tropical semiring* used in shortest path algorithms and models consisting of convex polyhedra used in computational geometry.

The completeness result of [19] says that all true identities between regular expressions interpreted as regular sets of strings are derivable from the axioms. In other words, the algebra of regular sets of strings over a finite alphabet P is the free Kleene algebra on generators P. The axioms are also complete for the equational theory of relational models.

2.2 Kleene Algebra with Tests

A *Kleene algebra with tests* (KAT) [20] is just a Kleene algebra with an embedded Boolean subalgebra. That is, it is a two-sorted structure $(K,\, B,\, +,\, \cdot,\, ^*,\, ^-,\, 0,\, 1)$ such that

- $(K,\, +,\, \cdot,\, ^*,\, 0,\, 1)$ is a Kleene algebra,
- $(B,\, +,\, \cdot,\, ^-,\, 0,\, 1)$ is a Boolean algebra, and
- $B \subseteq K$.

Elements of B are called *tests*. The Boolean complementation operator $^-$ is defined only on tests. We use the symbols $\mathsf{b}, \mathsf{c}, \mathsf{d}, \ldots$ to denote tests and $\mathsf{p}, \mathsf{q}, \mathsf{r}, \ldots$ to denote arbitrary elements of K.

The **while** program constructs are encoded as in propositional Dynamic Logic [10]:

$$\begin{aligned} \mathsf{p}\,;\,\mathsf{q} \quad &\stackrel{\mathrm{def}}{=} \quad \mathsf{pq} \\ \textbf{if }\mathsf{b}\textbf{ then }\mathsf{p}\textbf{ else }\mathsf{q} \quad &\stackrel{\mathrm{def}}{=} \quad \mathsf{bp} + \overline{\mathsf{b}}\mathsf{q} \\ \textbf{while }\mathsf{b}\textbf{ do }\mathsf{p} \quad &\stackrel{\mathrm{def}}{=} \quad (\mathsf{bp})^*\overline{\mathsf{b}}. \end{aligned}$$

The Hoare partial correctness assertion $\{\mathsf{b}\}\ \mathsf{p}\ \{\mathsf{c}\}$ is expressed as an equation $\mathsf{bp}\overline{\mathsf{c}} = 0$, or equivalently, $\mathsf{bp} = \mathsf{bpc}$. All Hoare rules are derivable in KAT; indeed, KAT is deductively complete for relationally valid propositional Hoare-style rules involving partial correctness assertions [21] (propositional Hoare logic is not).

For A a set of tests, define $\overline{A} = \{\overline{\mathsf{b}} \mid \mathsf{b} \in A\}$ and $\sim\! A = B - A$. Note that $\overline{A}$ and $\sim\! A$ are not the same in general; however, they coincide if A is an ultrafilter or maximal ideal of B.

See [19, 20, 21, 26] for a more detailed introduction to KA and KAT.

2.3 Relational Models

A *relational model* is a KAT whose elements are binary relations on some universal set U. The sequential composition operator $\cdot$ is interpreted as relational composition, the choice operator $+$ is interpreted as set-theoretic union, the iteration operator * is interpreted as reflexive transitive closure, the multiplicative identity 1 is interpreted as the identity relation on U, and the additive identity 0 is interpreted as the null relation. Tests are subsets of the identity relation on U, but not all subsets of the identity relation need be tests. The Boolean complementation operator on tests gives the set-theoretic complement in the identity relation.

A *nonstandard* relational model is the same, except that we do not require that p^* be the set-theoretic reflexive transitive closure, but only the $\leq$-least reflexive transitive relation containing p *in the algebra*.

The class of all relational KATs is denoted REL. If φ is a logical formula in the language of KAT, we write $\mathsf{REL} \vDash \varphi$ and say that φ is *relationally valid* if it is true under all relational interpretations.

For a binary relation p on a set U, define the *domain* and *range* of p to be the sets

$$\mathsf{dom}(\mathsf{p}) \stackrel{\mathrm{def}}{=} \{\mathsf{u} \mid \exists \mathsf{v}\ \ (\mathsf{u},\mathsf{v}) \in \mathsf{p}\} \qquad \mathsf{ran}(\mathsf{p}) \stackrel{\mathrm{def}}{=} \{\mathsf{v} \mid \exists \mathsf{u}\ \ (\mathsf{u},\mathsf{v}) \in \mathsf{p}\},$$

respectively.

3 Representation

We will show that the following two natural properties, along with the star-continuity condition (1), are sufficient to construct a nonstandard relational representation. These properties are quite weak.

Property 3.1 $\mathsf{pq} = 0 \ \ \Rightarrow\ \ \exists \mathsf{b}\ \ \mathsf{p} = \mathsf{pb} \wedge \mathsf{q} = \overline{\mathsf{b}}\mathsf{q}.$

Property 3.2 $\mathsf{p} \not\leq \mathsf{q} \ \ \Rightarrow\ \ \exists \mathsf{b} \exists \mathsf{c}\ \ \mathsf{bpc} \neq 0 \wedge \mathsf{bqc} = 0.$

Property 3.1 says essentially that there is a test that separates the range of p from the domain of q. This property is satisfied automatically in any system that postulates the existence of pre- and/or postconditions, such as dynamic algebra [15], Kleene algebra with domain and range operators [30], or Kleene modules [8]. It is related to expressibility conditions in Hoare logic [25] but somewhat weaker.

Property 3.2 asserts that actions can be distinguished by their interaction with tests. It is equivalent to the assertion that there exists no distinct inseparable pair, where the relation $\equiv$ of *inseparability* is defined by

$$\mathsf{p} \equiv \mathsf{q} \quad \stackrel{\mathrm{def}}{\Longleftrightarrow} \quad \forall \mathsf{b} \forall \mathsf{c}\ (\mathsf{bpc} = 0 \Leftrightarrow \mathsf{bqc} = 0).$$

The significance of this requirement is captured in the following proposition.

Proposition 3.3 *Let* p *and* q *be terms in the language of* KAT*, and let* b *and* c *be test variables not occurring in* p *or* q*. The following are equivalent:*

(i) $\mathsf{p} \le \mathsf{q}$ *is valid,*

(ii) $\mathsf{bqc} = 0 \to \mathsf{bpc} = 0$ *is valid,*

(iii) $\mathsf{bqc} = 0 \to \mathsf{bpc} = 0$ *is relationally valid.*

Proof. The implications (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii) are trivial. For (iii) $\Rightarrow$ (i), if $\mathsf{p} \le \mathsf{q}$ is not valid, then it fails in some relational model, since the equational theories of KAT and REL are the same. Let $(s,t) \in \mathsf{p} - \mathsf{q}$ in this model, and reinterpret b as $\{s\}$ and c as $\{t\}$. Then bpc contains (s,t), but $\mathsf{bqc} = 0$. □

Let K, B be a KAT satisfying Properties 3.1 and 3.2. As with all Stone-like constructions, our universal set of states will be the set of ultrafilters of B.

Recall that a *filter* is a subset F of B such that

(i) $\mathsf{bc} \in F \;\Leftrightarrow\; \mathsf{b} \in F$ and $\mathsf{c} \in F$

(ii) $1 \in F$

(iii) $0 \notin F$,

and an *ultrafilter* is a maximal filter. Dually, an *ideal* is a subset I of B such that

(i) $\mathsf{b} + \mathsf{c} \in I \;\Leftrightarrow\; \mathsf{b} \in I$ and $\mathsf{c} \in I$

(ii) $1 \notin I$

(iii) $0 \in I$.

Ideals are the kernels of Boolean algebra homomorphisms. Note that F is a filter iff $\overline{F}$ is an ideal, and u is an ultrafilter iff $\overline{u}$ is a maximal ideal. By Zorn's lemma, every filter is contained in an ultrafilter and every ideal is contained in a maximal ideal. Every ultrafilter u satisfies the property that for all b, either $\mathsf{b} \in u$ or $\overline{\mathsf{b}} \in u$, but not both; therefore $\sim u = \overline{u}$.

Let U denote the set of ultrafilters of B. The well-known Stone construction (see e.g. [3, 11]) produces a Boolean algebra isomorphic to B whose elements are subsets of U and whose Boolean operations are the usual set-theoretic ones. The subset corresponding to b is $\mathsf{b}' \stackrel{\text{def}}{=} \{u \mid \mathsf{b} \in u\}$. We denote this set-theoretic Boolean algebra by B'.

A *coideal* of a Boolean algebra B is a complement of an ideal; that is, it is a subset C of B satisfying

(i) $\mathsf{b} + \mathsf{c} \in C \;\Leftrightarrow\; \mathsf{b} \in C$ or $\mathsf{c} \in C$

(ii) $1 \in C$

(iii) $0 \notin C$.

Lemma 3.4 *Every coideal contains an ultrafilter as a subset.*

Proof. If C is a coideal, then $\sim C$ is an ideal. By Zorn's Lemma, $\sim C$ extends to a maximal ideal M. Then $\sim M$ is an ultrafilter and is a subset of C. □

Definition 3.5

$$\begin{array}{rcl} \mathsf{In}(\mathsf{p},\mathsf{q}) & \stackrel{\text{def}}{=} & \{\mathsf{d} \mid \mathsf{pdq} \neq 0\} \\ \mathsf{Pre}(\mathsf{p}) & \stackrel{\text{def}}{=} & \{\mathsf{b} \mid \mathsf{bp} \neq 0\} \;=\; \mathsf{In}(1,\mathsf{p}) \\ \mathsf{Post}(\mathsf{p}) & \stackrel{\text{def}}{=} & \{\mathsf{c} \mid \mathsf{pc} \neq 0\} \;=\; \mathsf{In}(\mathsf{p},1). \end{array}$$

□

Lemma 3.6 *If* $\mathsf{pq} \neq 0$, *then* $\mathsf{In}(\mathsf{p},\mathsf{q})$ *is a coideal. If* $\mathsf{p} \neq 0$, *then* $\mathsf{Pre}(\mathsf{p})$ *and* $\mathsf{Post}(\mathsf{p})$ *are coideals.*

Proof. For $\mathsf{In}(\mathsf{p},\mathsf{q})$,

(i) $\mathsf{p}(\mathsf{c}+\mathsf{d})\mathsf{q} \neq 0 \;\;\Leftrightarrow\;\; \mathsf{pcq}+\mathsf{pdq} \neq 0 \;\;\Leftrightarrow\;\; \mathsf{pcq} \neq 0$ or $\mathsf{pdq} \neq 0$,

(ii) $\mathsf{pq} \neq 0 \;\;\Rightarrow\;\; \mathsf{p1q} \neq 0 \;\;\Rightarrow\;\; 1 \in \mathsf{In}(\mathsf{p},\mathsf{q})$,

(iii) $\mathsf{p0q} = 0 \;\;\Rightarrow\;\; 0 \notin \mathsf{In}(\mathsf{p},\mathsf{q})$.

$\mathsf{Pre}(\mathsf{p})$ and $\mathsf{Post}(\mathsf{p})$ are special cases. □

A collection $\{C_\alpha\}$ of coideals is *downward-directed* if for any pair C_α and C_β, there is a C_γ with $C_\gamma \subseteq C_\alpha \cap C_\beta$.

Lemma 3.7 *The intersection of any downward-directed set of coideals is a coideal.*

Proof. Equivalently, the union of any upward-directed set of ideals is an ideal. The three conditions are easily checked. □

Lemma 3.8

(i) *If* $\mathsf{p}_1 \leq \mathsf{p}_2$ *and* $\mathsf{q}_1 \leq \mathsf{q}_2$, *then* $\mathsf{In}(\mathsf{p}_1,\mathsf{q}_1) \subseteq \mathsf{In}(\mathsf{p}_2,\mathsf{q}_2)$.

(ii) *If* $\mathsf{p}_1 \leq \mathsf{p}_2$, *then* $\mathsf{Post}(\mathsf{p}_1) \subseteq \mathsf{Post}(\mathsf{p}_2)$.

(iii) *If* $\mathsf{p}_1 \leq \mathsf{p}_2$, *then* $\mathsf{Pre}(\mathsf{p}_1) \subseteq \mathsf{Pre}(\mathsf{p}_2)$.

Proof. Statement (i) follows easily from the definitions. Statements (ii) and (iii) are special cases. □

We now define our relational model R. For all $\mathsf{p} \in K$, define

Definition 3.9

$$\mathsf{p}^R \;\;\stackrel{\text{def}}{=}\;\; \{(u,v) \mid \forall \mathsf{b} \in u \;\; \forall \mathsf{c} \in v \;\; \mathsf{bpc} \neq 0\}.$$

□

Since $\mathsf{bp} = 0$ iff $\mathsf{p} = \overline{\mathsf{b}}\mathsf{p}$ (see e.g. [21, Section 3]), we have the following facts:

$$\begin{array}{rclcl} \mathsf{Pre}(\mathsf{p}) &=& \{\mathsf{b} \mid \mathsf{bp} \neq 0\} &=& \{\mathsf{b} \mid \mathsf{p} \neq \overline{\mathsf{b}}\mathsf{p}\} \\ \sim\mathsf{Pre}(\mathsf{p}) &=& \{\mathsf{b} \mid \mathsf{bp} = 0\} &=& \{\mathsf{b} \mid \mathsf{p} = \overline{\mathsf{b}}\mathsf{p}\} \\ \overline{\sim\mathsf{Pre}(\mathsf{p})} &=& \{\overline{\mathsf{b}} \mid \mathsf{bp} = 0\} &=& \{\overline{\mathsf{b}} \mid \mathsf{p} = \overline{\mathsf{b}}\mathsf{p}\}. \end{array}$$

If $\mathsf{p} \neq 0$, then $\mathsf{Pre}(\mathsf{p})$ is a coideal, $\sim\mathsf{Pre}(\mathsf{p})$ is an ideal, and $\overline{\sim\mathsf{Pre}(\mathsf{p})}$ is a filter.

Lemma 3.10 *Let u be an ultrafilter. The following are equivalent:*

(i) $u \subseteq \mathsf{Pre}(\mathsf{p})$

(ii) $\overline{\sim\mathsf{Pre}(\mathsf{p})} \subseteq u$

(iii) $u \in \mathsf{dom}(\mathsf{p}^R)$.

Proof. (i) $\Leftrightarrow$ (ii): $\overline{\sim\mathsf{Pre}(\mathsf{p})} \subseteq u$ iff $\sim\mathsf{Pre}(\mathsf{p}) \subseteq \overline{u}$ iff $\sim\overline{u} \subseteq \mathsf{Pre}(\mathsf{p})$ iff $u \subseteq \mathsf{Pre}(\mathsf{p})$, since $u = \sim\overline{u}$.

(iii) $\Rightarrow$ (i): If $(u, v) \in \mathsf{p}^R$, then for all $\mathsf{b} \in u$ and $\mathsf{c} \in v$, $\mathsf{bpc} \neq 0$. Since $1 \in v$, we have that for all $\mathsf{b} \in u$, $\mathsf{bp} \neq 0$. Then $u \subseteq \mathsf{Pre}(\mathsf{p})$ by definition of $\mathsf{Pre}(\mathsf{p})$.

(i) $\Rightarrow$ (iii): If $u \subseteq \mathsf{Pre}(\mathsf{p})$, then $\mathsf{bp} \neq 0$ for all $\mathsf{b} \in u$. By Lemma 3.6, for all $\mathsf{b} \in u$, $\mathsf{Post}(\mathsf{bp})$ is a coideal. By Lemmas 3.7 and 3.8(ii), $\bigcap_{\mathsf{b} \in u} \mathsf{Post}(\mathsf{bp})$ is a coideal, therefore contains an ultrafilter v by Lemma 3.4. Thus for all $\mathsf{b} \in u$ and $\mathsf{c} \in v$, $\mathsf{c} \in \mathsf{Post}(\mathsf{bp})$, therefore $\mathsf{bpc} \neq 0$ and $(u, v) \in \mathsf{p}^R$. $\square$

The following is the main theorem of this section.

Theorem 3.11 *Let K, B be a star-continuous* KAT *satisfying Properties 3.1 and 3.2. The set $\{\mathsf{p}^R \mid \mathsf{p} \in \mathsf{K}\}$ is a nonstandard relational* KAT *with tests $\{\mathsf{b}^R \mid \mathsf{b} \in \mathsf{B}\}$, and the map $\mathsf{p} \mapsto \mathsf{p}^R$ is a* KAT *isomorphism.*

Proof. If $\mathsf{p} \leq \mathsf{q}$ then $\mathsf{p}^R \subseteq \mathsf{q}^R$, since $\mathsf{p} \leq \mathsf{q} \Rightarrow \mathsf{bpc} \leq \mathsf{bqc}$. Thus the map $\mathsf{p} \mapsto \mathsf{p}^R$ is monotone.

To show that $\mathsf{p} \mapsto \mathsf{p}^R$ is one-to-one, it suffices to show that if $\mathsf{p} \not\leq \mathsf{q}$, then $\mathsf{p}^R \not\subseteq \mathsf{q}^R$. Suppose that $\mathsf{p} \not\leq \mathsf{q}$. By Property 3.2, there exist b and c such that $\mathsf{bpc} \neq 0$ and $\mathsf{bqc} = 0$. By Lemma 3.6, $\mathsf{Pre}(\mathsf{bpc}) = \{\mathsf{d} \mid \mathsf{dbpc} \neq 0\}$ is a coideal, therefore contains an ultrafilter u by Lemma 3.4. By definition of $\mathsf{Pre}(\mathsf{bpc})$, we have $\mathsf{dbpc} \neq 0$ for all $\mathsf{d} \in u$. It follows that $\mathsf{b} \in u$, since either $\mathsf{b} \in u$ or $\overline{\mathsf{b}} \in u$, and the latter is impossible. Moreover, by Lemma 3.6, for all $\mathsf{d} \in u$, $\mathsf{Post}(\mathsf{dbpc}) = \{\mathsf{e} \mid \mathsf{dbpce} \neq 0\}$ is a coideal. In addition, it follows from Lemma 3.8(ii) that the set $\{\mathsf{Post}(\mathsf{dbpc}) \mid \mathsf{d} \in u\}$ is downward-directed, since

$$\mathsf{Post}(\mathsf{d}_1\mathsf{d}_2\mathsf{bpc}) \quad\subseteq\quad \mathsf{Post}(\mathsf{d}_1\mathsf{bpc}) \cap \mathsf{Post}(\mathsf{d}_2\mathsf{bpc}).$$

By Lemma 3.7, $\bigcap_{\mathsf{d} \in u} \mathsf{Post}(\mathsf{dbpc})$ is a coideal, therefore contains an ultrafilter v by Lemma 3.4. As with u, $\mathsf{c} \in v$. Then $(u, v) \in \mathsf{p}^R$, but $(u, v) \notin \mathsf{q}^R$ since $\mathsf{bqc} = 0$.

Next we show that $\mathsf{p} \mapsto \mathsf{p}^R$ is a homomorphism with respect to addition; that is, $(\mathsf{p} + \mathsf{q})^R = \mathsf{p}^R \cup \mathsf{q}^R$. The reverse inclusion follows from monotonicity. For the forward inclusion, suppose $(u,v) \notin \mathsf{p}^R \cup \mathsf{q}^R$. Then there exist $\mathsf{b}_1, \mathsf{b}_2 \in u$ and $\mathsf{c}_1, \mathsf{c}_2 \in v$ such that $\mathsf{b}_1\mathsf{p}\mathsf{c}_1 = 0$ and $\mathsf{b}_2\mathsf{q}\mathsf{c}_2 = 0$. Since u and v are filters, $\mathsf{b}_1\mathsf{b}_2 \in u$ and $\mathsf{c}_1\mathsf{c}_2 \in v$, and $\mathsf{b}_1\mathsf{b}_2\mathsf{p}\mathsf{c}_1\mathsf{c}_2 = 0$ and $\mathsf{b}_1\mathsf{b}_2\mathsf{q}\mathsf{c}_1\mathsf{c}_2 = 0$. Then $\mathsf{b}_1\mathsf{b}_2(\mathsf{p}+\mathsf{q})\mathsf{c}_1\mathsf{c}_2 = 0$, so $(u,v) \notin (\mathsf{p}+\mathsf{q})^R$.

Next we show that $\mathsf{p} \mapsto \mathsf{p}^R$ is a homomorphism with respect to multiplication; that is, $(\mathsf{pq})^R = \mathsf{p}^R \circ \mathsf{q}^R$. For the forward inclusion, suppose $(u,v) \in (\mathsf{pq})^R$. Then for all $\mathsf{b} \in u$ and $\mathsf{c} \in v$, $\mathsf{bpqc} \neq 0$. By Lemma 3.6, for all $\mathsf{b} \in u$ and $\mathsf{c} \in v$, $\mathsf{In}(\mathsf{bp}, \mathsf{qc})$ is a coideal. Moreover, the set $\{\mathsf{In}(\mathsf{bp}, \mathsf{qc}) \mid \mathsf{b} \in u,\ \mathsf{c} \in v\}$ is downward-directed, since

$$\mathsf{In}(\mathsf{b}_1\mathsf{b}_2\mathsf{p}, \mathsf{q}\mathsf{c}_1\mathsf{c}_2) \quad \subseteq \quad \mathsf{In}(\mathsf{b}_1\mathsf{p}, \mathsf{q}\mathsf{c}_1) \cap \mathsf{In}(\mathsf{b}_2\mathsf{p}, \mathsf{q}\mathsf{c}_2).$$

By Lemma 3.7, $\bigcap\{\mathsf{In}(\mathsf{bp}, \mathsf{qc}) \mid \mathsf{b} \in u,\ \mathsf{c} \in v\}$ is a coideal, therefore contains an ultrafilter w by Lemma 3.4. Then for all $\mathsf{b} \in u$, $\mathsf{c} \in v$, and $\mathsf{d} \in w$, $\mathsf{bpdqc} \neq 0$, therefore $\mathsf{bpd} \neq 0$ and $\mathsf{dqc} \neq 0$. It follows that $(u,w) \in \mathsf{p}^R$ and $(w,v) \in \mathsf{q}^R$, therefore $(u,v) \in \mathsf{p}^R \circ \mathsf{q}^R$.

For the reverse inclusion, we need Property 3.1. Suppose $(u,w) \in \mathsf{p}^R$ and $(w,v) \in \mathsf{q}^R$. Then for all $\mathsf{b} \in u$, $\mathsf{c} \in v$, and $\mathsf{d} \in w$, we have $\mathsf{bpd} \neq 0$ and $\mathsf{dqc} \neq 0$. If $\mathsf{bpqc} = 0$ for some $\mathsf{b} \in u$ and $\mathsf{c} \in v$, then by Property 3.1, there exists d such that $\mathsf{bp} = \mathsf{bpd}$ and $\mathsf{qc} = \overline{\mathsf{d}}\mathsf{qc}$. Either $\mathsf{d} \in w$ or $\overline{\mathsf{d}} \in w$. If the former, then $\mathsf{dqc} = \mathsf{d}\overline{\mathsf{d}}\mathsf{qc} = 0$. If the latter, then $\mathsf{bp}\overline{\mathsf{d}} = \mathsf{bpd}\overline{\mathsf{d}} = 0$. In either case, we have a contradiction. Thus for all $\mathsf{b} \in u$ and $\mathsf{c} \in v$, $\mathsf{bpqc} \neq 0$, therefore $(u,v) \in (\mathsf{pq})^R$.

For tests, we must show that $\mathsf{b}^R = \{(u,u) \mid \mathsf{b} \in u\}$, that 1^R is the identity relation on U, that 0^R is the empty relation, and that the map $\mathsf{b} \mapsto \mathsf{b}^R$ is a homomorphism with respect to negation. We have

$$\mathsf{b}^R \quad = \quad \{(u,v) \mid \forall \mathsf{c} \in u\ \forall \mathsf{d} \in v\ \ \mathsf{cbd} \neq 0\}.$$

Thus $(u,v) \in \mathsf{b}^R$ iff $u = v$ and $\mathsf{b} \in u$, therefore $\mathsf{b}^R = \{(u,u) \mid \mathsf{b} \in u\}$. In particular, $1^R = \{(u,u) \mid 1 \in u\}$, the identity relation, and $0^R = \{(u,u) \mid 0 \in u\} = \varnothing$. Since $\mathsf{b} \in u$ iff $\overline{\mathsf{b}} \notin u$,

$$\overline{\mathsf{b}}^R \quad = \quad \{(u,u) \mid \overline{\mathsf{b}} \in u\} \quad = \quad \{(u,u) \mid \mathsf{b} \notin u\} \quad = \quad 1^R - \mathsf{b}^R.$$

Finally, for *, it follows from the star-continuity of K, B and the fact that the map $\mathsf{p} \mapsto \mathsf{p}^R$ is an order isomorphism that $\mathsf{q}^{*R} = \sup_n (\mathsf{q}^R)^n$. □

4 Star

In this section we identify an algebraic condition (Condition 4.4 below) under which the construction of Section 3 yields a standard relational model. This occurs exactly when $\mathsf{q}^{R*} = \mathsf{q}^{*R}$ for all q, where q^{R*} denotes the set-theoretic reflexive transitive closure of q^R and q^{*R} is the representation of q^* in R.

Endow U with the Stone topology generated by B' and $U \times U$ with the product topology. The basic open sets of these spaces are sets of the form b' and $\mathsf{b}' \times \mathsf{c}'$, respectively. Let $\mathrm{cl}(A)$ denote the closure of A in either topology.

Lemma 4.1 *Every p^R is closed in $U \times U$.*

Proof. If $(u, v) \notin \mathsf{p}^R$, then there exist $\mathsf{b} \in u$ and $\mathsf{c} \in v$ such that $\mathsf{bpc} = 0$. Then $(u, v) \in \mathsf{b}' \times \mathsf{c}'$ and

$$(\mathsf{b}' \times \mathsf{c}') \cap \mathsf{p}^R \;\; = \;\; (\mathsf{bpc})^R \;\; = \;\; \varnothing.$$

Thus $\mathsf{b}' \times \mathsf{c}'$ is a basic open neighborhood of (u, v) disjoint from p^R. Since $(u, v) \notin \mathsf{p}^R$ was arbitrary, $(U \times U) - \mathsf{p}^R$ is open, therefore p^R is closed. $\square$

Lemma 4.2 *The sets* $\mathsf{dom}(\mathsf{p}^R)$ *and* $\mathsf{ran}(\mathsf{p}^R)$ *are closed in* U.

Proof. By Lemma 3.10, $\mathsf{dom}(\mathsf{p}^R)$ is the set of ultrafilters u extending the filter $\sim\mathsf{Pre}(\mathsf{p})$. But the set of ultrafilters extending any filter F is closed, since it is the intersection of basic closed sets:

$$\{u \mid F \subseteq u\} \;\; = \;\; \bigcap_{\mathsf{b} \in F} \{u \mid \mathsf{b} \in u\} \;\; = \;\; \bigcap_{\mathsf{b} \in F} \mathsf{b}'.$$

The argument for $\mathsf{ran}(\mathsf{p})$ is symmetric. $\square$

Lemma 4.3 *Let* $\{\mathsf{q}_\alpha\}$ *be a collection of elements of* K *and* p *an element of* K *such that for all* $\mathsf{b}, \mathsf{c} \in B$, $\mathsf{bpc} = \sup_\alpha \mathsf{bq}_\alpha\mathsf{c}$. *Then* $\mathsf{p}^R = \mathrm{cl}(\bigcup_\alpha \mathsf{q}_\alpha^R)$. *In particular,* $\mathsf{q}^{*R} = \mathrm{cl}(\mathsf{q}^{R*})$.

Proof. The inclusion $\supseteq$ holds by Lemma 4.1. If $(u, v) \in \mathsf{p}^R - \mathrm{cl}(\bigcup_\alpha \mathsf{q}_\alpha^R)$, then there exists a basic open neighborhood $\mathsf{b}' \times \mathsf{c}'$ of (u, v) disjoint from $\bigcup_\alpha \mathsf{q}_\alpha^R$. Then $(\mathsf{bq}_\alpha\mathsf{c})^R = (\mathsf{b}' \times \mathsf{c}') \cap \mathsf{q}_\alpha^R = \varnothing$ for all α, thus $\mathsf{bq}_\alpha\mathsf{c} = 0$ for all α, therefore $\sup_\alpha \mathsf{bq}_\alpha\mathsf{c} = 0$. But $(u, v) \in (\mathsf{b}' \times \mathsf{c}') \cap \mathsf{p}^R = (\mathsf{bpc})^R$, thus $(\mathsf{bpc})^R \neq \varnothing$ and $\mathsf{bpc} \neq 0$. This contradicts the assumption. $\square$

A necessary and sufficient condition for the relational model constructed in Section 3 to be standard is the following *uniform halting condition*:

Condition 4.4

$$\forall n \, \exists \mathsf{b} \in u \, \exists \mathsf{c} \in v \;\; \mathsf{bq}^n\mathsf{c} = 0 \quad \Rightarrow \quad \exists \mathsf{b} \in u \, \exists \mathsf{c} \in v \, \forall n \;\; \mathsf{bq}^n\mathsf{c} = 0.$$

Condition 4.4 says that if for each n there are properties of (u, v) that cause it not to be an input/output pair of the program q^n, then there is a pair of such properties that work uniformly over all n. Intuitively, the input/output relation of a loop depends on only finitely many testable properties. Equivalently,

$$\forall \mathsf{b} \in u \, \forall \mathsf{c} \in v \, \exists n \;\; \mathsf{bq}^n\mathsf{c} \neq 0 \quad \Rightarrow \quad \exists n \, \forall \mathsf{b} \in u \, \forall \mathsf{c} \in v \;\; \mathsf{bq}^n\mathsf{c} \neq 0.$$

Theorem 4.5 *Condition 4.4 is equivalent to the property* $\mathsf{q}^{*R} = \mathsf{q}^{R*}$.

Proof. The left-hand side of Condition 4.4 says exactly that $(u, v) \notin \mathsf{q}^{R^n}$ for all n, thus $(u, v) \notin \mathsf{q}^{R*}$. We also have

$$\bigcup_n (\mathsf{bq}^n\mathsf{c})^R \;\; = \;\; \bigcup_n (\mathsf{b}' \times \mathsf{c}') \cap \mathsf{q}^{nR} \;\; = \;\; (\mathsf{b}' \times \mathsf{c}') \cap \bigcup_n \mathsf{q}^{nR} \;\; = \;\; (\mathsf{b}' \times \mathsf{c}') \cap \mathsf{q}^{R*},$$

so that the right-hand side of Condition 4.4 can be rewritten

$$
\begin{aligned}
&\exists \mathsf{b} \in u\ \exists \mathsf{c} \in v\ \forall n\ \ \mathsf{b}\mathsf{q}^n\mathsf{c} = 0 \\
&\quad \Leftrightarrow \quad \exists \mathsf{b}\ \exists \mathsf{c}\ \ (u,v) \in \mathsf{b}' \times \mathsf{c}'\ \ \text{and}\ \ \forall n\ (\mathsf{b}\mathsf{q}^n\mathsf{c})^R = \varnothing \\
&\quad \Leftrightarrow \quad \exists \mathsf{b}\ \exists \mathsf{c}\ \ (u,v) \in \mathsf{b}' \times \mathsf{c}'\ \ \text{and}\ \ \bigcup_n (\mathsf{b}\mathsf{q}^n\mathsf{c})^R = \varnothing \\
&\quad \Leftrightarrow \quad \exists \mathsf{b}\ \exists \mathsf{c}\ \ (u,v) \in \mathsf{b}' \times \mathsf{c}'\ \ \text{and}\ \ (\mathsf{b}' \times \mathsf{c}') \cap \mathsf{q}^{R*} = \varnothing.
\end{aligned}
$$

This says exactly that there is a basic open neighborhood of (u, v) disjoint from q^{R*}. Thus the implication of Condition 4.4 says exactly that $\sim\mathsf{q}^{R*}$ is open; that is, q^{R*} is closed. By Lemma 4.3, q^{*R} is the closure of q^{R*}, therefore they are equal if and only if q^{R*} is closed. □

5 Open Problems

Theorem 4.5 does not say that a standard representation does not exist if Condition 4.4 fails. In the case of countable K, some variant of the Tarski–Rasiowa–Sikorski lemma or the Baire category theorem might be used to drop out nonstandard points from the model constructed above, giving a standard relational model or perhaps a homomorphic image of one; see [15, 18]. The constructions of [15, 18] do not seem to apply directly. On the other hand, neither do we have a negative result. The counterexamples of [17, 32] for dynamic algebra do not immediately provide counterexamples for KAT, but the counterexample of [17] may be adaptable. Such questions remain for future investigation.

Axiomatization of the universal Horn theory of relational models is another interesting open question. This theory is an extension of the universal Horn theory of the star-continuous Kleene algebras, and both theories are known to be Π^1_1-complete [22, 12], therefore not finitely axiomatizable. However, the star-continuous algebras have a succinct infinitary axiomatization containing a single infinitary rule (1). It is interesting to ask whether the relational algebras have a finitary axiomatization relative to this. Presumably the Horn formula $\mathsf{p} \leq 1 \rightarrow \mathsf{p}^2 = \mathsf{p}$ would be a candidate axiom.

Acknowledgements

Thanks to Samson Abramsky for valuable comments. It was he who suggested the term “coideal”. This work was supported in part by NSF grant CCR-0105586 and by ONR Grant N00014-01-1-0968. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of these organizations or the US Government.

References

[1] Allegra Angus and Dexter Kozen. Kleene algebra with tests and program schematology. Technical Report 2001-1844, Computer Science Department, Cornell University, July 2001.

[2] Adam Barth and Dexter Kozen. Equational verification of cache blocking in LU decomposition using Kleene algebra with tests. Technical Report 2002-1865, Computer Science Department, Cornell University, June 2002.

[3] J.S. Bell and A.B. Slomson. *Models and Ultraproducts*. North Holland, 1971.

[4] Ernie Cohen. Lazy caching in Kleene algebra. `http://citeseer.nj.nec.com/22581.html`.

[5] Ernie Cohen. Hypotheses in Kleene algebra. Technical Report TM-ARH-023814, Bellcore, 1993. `http://citeseer.nj.nec.com/1688.html`.

[6] Ernie Cohen, Dexter Kozen, and Frederick Smith. The complexity of Kleene algebra with tests. Technical Report 96-1598, Computer Science Department, Cornell University, July 1996.

[7] John Horton Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, London, 1971.

[8] Thorsten Ehm, Bernhard Möller, and Georg Struth. Kleene modules. In *Proc. 2nd Int. Workshop on Applications of Kleene Algebra*, pages 21–27, May 2003.

[9] C.J. Everett and S. Ulam. Projective algebra I. *Amer. J. Math.*, 68(1):77–88, 1946.

[10] Michael J. Fischer and Richard E. Ladner. Propositional dynamic logic of regular programs. *J. Comput. Syst. Sci.*, 18(2):194–211, 1979.

[11] P.R. Halmos. *Lectures on Boolean Algebras*. Springer Verlag, 1974.

[12] Chris Hardin and Dexter Kozen. On the complexity of the Horn theory of REL. Technical Report 2003-1896, Computer Science Department, Cornell University, May 2003.

[13] B. Jonsson and A. Tarski. Representation problems for relation algebras. *Bull. Amer. Math. Soc.*, 54:80, 1948. abstract 89t.

[14] Stephen C. Kleene. Representation of events in nerve nets and finite automata. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*, pages 3–41. Princeton University Press, Princeton, N.J., 1956.

[15] Dexter Kozen. On the duality of dynamic algebras and Kripke models. In E. Engeler, editor, *Proc. Workshop on Logic of Programs*, volume 125 of *Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag, 1979.

[16] Dexter Kozen. On the representation of dynamic algebras. Technical Report RC7898, IBM Thomas J. Watson Research Center, October 1979.

[17] Dexter Kozen. On the representation of dynamic algebras II. Technical Report RC8290, IBM Thomas J. Watson Research Center, May 1980.

[18] Dexter Kozen. A representation theorem for models of *-free *PDL*. In *Proc. 7th Colloq. Automata, Languages, and Programming*, pages 351–362. EATCS, July 1980.

[19] Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Infor. and Comput.*, 110(2):366–390, May 1994.

[20] Dexter Kozen. Kleene algebra with tests. *Transactions on Programming Languages and Systems*, 19(3):427–443, May 1997.

[21] Dexter Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1(1):60–76, July 2000.

[22] Dexter Kozen. On the complexity of reasoning in Kleene algebra. *Information and Computation*, 179:152–162, 2002.

[23] Dexter Kozen and Maria-Cristina Patron. Certification of compiler optimizations using Kleene algebra with tests. In John Lloyd, Veronica Dahl, Ulrich Furbach, Manfred Kerber, Kung-Kiu Lau, Catuscia Palamidessi, Luis Moniz Pereira, Yehoshua Sagiv, and Peter J. Stuckey, editors, *Proc. 1st Int. Conf. Computational Logic (CL2000)*, volume 1861 of *Lecture Notes in Artificial Intelligence*, pages 568–582, London, July 2000. Springer-Verlag.

[24] Dexter Kozen and Frederick Smith. Kleene algebra with tests: Completeness and decidability. In D. van Dalen and M. Bezem, editors, *Proc. 10th Int. Workshop Computer Science Logic (CSL'96)*, volume 1258 of *Lecture Notes in Computer Science*, pages 244–259, Utrecht, The Netherlands, September 1996. Springer-Verlag.

[25] Dexter Kozen and Jerzy Tiuryn. On the completeness of propositional Hoare logic. *Information Sciences*, 139(3–4):187–195, 2001.

[26] Dexter Kozen and Jerzy Tiuryn. Substructural logic and partial correctness. *Trans. Computational Logic*, 4(3):355–378, July 2003.

[27] R.C. Lyndon. The representation of relation algebras. *Ann. Math.*, 51(3):707–729, 1950.

[28] J.C.C. McKinsey. Postulates for the calculus of binary relations. *J. Symb. Logic*, 5(3):85–97, 1940.

[29] J.C.C. McKinsey. On the representation of projective algebras. *Amer. J. Math.*, 70:375–384, 1948.

[30] Bernhard Möller and Georg Struth. Greedy-like algorithms in Kleene algebra. In *Proc. 2nd Int. Workshop on Applications of Kleene Algebra*, pages 173–180, May 2003.

[31] I. Németi. Every free algebra in the variety generated by the representable dynamic algebras is separable and representable. Hungarian Academy of Sciences, Budapest, 1980.

[32] J. Reiterman and V. Trnková. Dynamic algebras which are not Kripke structures. In *Proc. 9th Symp. Math. Found. of Computer Science (MFCS'80)*, pages 528–538, August 1980.

[33] A. Tarski. On the calculus of relations. *J. Symb. Logic*, 6(3):73–89, 1941.