Abstract—It is known that certain program transformations require a small amount of mutable state, a feature not explicitly provided by Kleene algebra with tests (KAT). In this paper we show how to axiomatically extend KAT with this extra feature in the form of mutable tests. The extension is conservative and is formulated as a general commutative coproduct construction. We give several results on deductive completeness and complexity of the system, as well as some examples of its use.

I. INTRODUCTION

Kleene algebra with tests (KAT) is a propositional equational system that combines Kleene algebra (KA) with Boolean algebra. It has been shown to be an effective tool for many low-level program analysis and verification tasks involving communication protocols, safety analysis, source-to-source program transformation, concurrency control, and compiler optimization [1–7]. A notable recent success is its adoption as a basis for NetKAT, a foundation for software-defined networks (SDN) [8].

One advantage of KAT is that it allows a clean separation of the theory of the domain of computation from the program restructuring operations. The former typically involves first-order reasoning, whereas the latter is typically propositional. It is often advantageous to separate the two, because the theory of the domain of computation may be highly undecidable. With KAT, one typically isolates the needed properties of the domain as premises in a Horn formula

\[ s_1 = t_1 \land \cdots \land s_n = t_n \rightarrow s = t, \]

where the conclusion \( s = t \) expresses a more complicated equivalence between (say) an unoptimized or unannotated version of a program and its optimized or annotated version. The premises are verified once and for all using the properties of the domain, and the conclusion is then verified propositionally in KAT under those assumptions.

Certain premises that arise frequently in practice can be incorporated as part of the theory using a technique known as elimination of hypotheses, in which Horn formulas with premises of a certain form can be reduced to the equational theory without loss of efficiency [3, 9, 10]. However, there are a few useful ones that cannot. In particular, it is known that there are certain program transformations that cannot be effected in pure KAT, but require extra structure. Two paradigmatic examples are the Böhm–Jacopini theorem [11] (see also [12–16]) and the folklore result that all while programs can be transformed to a program with a single while loop [17, 18].

The Böhm–Jacopini theorem states that every deterministic flowchart can be written as a while program. The construction is normally done at the first-order level and introduces auxiliary variables to remember values across computations. It has been shown that the construction is not possible without some kind of auxiliary structure of this type [12, 19, 20].

Akin to the Böhm–Jacopini theorem, and often erroneously conflated with it, is the folklore theorem that every while program can be written with a single while loop. Like the proof of the Böhm–Jacopini theorem, the proofs of [18, 21], as reported in [17], are normally done at the first-order level and use auxiliary variables. It was a commonly held belief that this result had no purely propositional proof [17], but a partial refutation of this view was given in [6] using a construction that foreshadows the construction of this paper.

One can carry out these constructions in an uninterpreted first-order version of KAT called schematic KAT (SKAT) [1, 22], but as SKAT is undecidable in general [23], one would prefer a less radical extension.

In this paper we investigate the minimal amount of structure that suffices to perform these transformations and show how to incorporate it in KAT without sacrificing deductive completeness or decidability. Our main results are:

- We show how to extend KAT with a set of independent mutable tests. The construction is done axiomatically with generators and additional equational axioms. We formulate the construction as a general commutative coproduct construction that satisfies a certain universality property. The generators are abstract setters of the form \( \texttt{b}! \) and \( \texttt{b}? \) and testers \( \texttt{b}? \) and \( \texttt{b}! \) for a test symbol \( b \). We can think of these intuitively as operations that set and test the value of a Boolean variable, although we do not introduce any explicit notion of storage or variable assignment.
- We prove a representation theorem (Theorem 2.4) for the commutative coproduct of an arbitrary KAT \( K \) and a finite relation algebra, namely that it is isomorphic to a certain matrix algebra over \( K \).
- As a corollary to the representation theorem, we show that the extension is conservative; that is, an arbitrary KAT \( K \) can be augmented with mutable tests without affecting the theory of \( K \). This is captured formally by a general property of the commutative coproduct, namely injectivity. It is not known whether the coproduct of KATs is injective in general, but we show that it is injective if at least one of the two cofactors is a finite relation algebra.
which is the case in our application.

- We show that the free mutable test algebra on generators $b_i, 1 \leq i \leq n$, is isomorphic to the full binary relation algebra on $2^n$ states. We also characterize the primitive operations in terms of a tensor product of $n$ copies of a 2-state system. We show that the equational theory of this algebra is PSPACE-complete, thus no easier or harder to decide than KAT.

- We show that the equational theory of an arbitrary KAT $K$ augmented with mutable tests is axiomatically reducible to the theory of $K$. In particular, the free KAT, augmented with mutable tests, is completely axiomatized by the KAT axioms plus the axioms for mutable tests.

- We show that the equational theory of KAT with mutable tests is EXPSPACE-complete.

- We demonstrate that the program transformations mentioned above, namely the Böhm–Jacopini theorem and the folklore result about while programs, can be carried out in KAT with mutable tests.

This paper is organized as follows. In §II we briefly review KA and KAT and introduce the theory of mutable tests, and prove that the free mutable test algebra on $n$ generators is isomorphic to the full binary relation algebra on a set of size $2^n$. We also introduce the commutative coproduct construction and prove our representation theorem for the commutative coproduct of an arbitrary KAT $K$ and a finite relation algebra. In §III we prove our main completeness and complexity results. In §IV we apply the theory to give an axiomatic treatment of two applications involving program transformations. In §V we present conclusions and open problems.

Omitted proofs can be found in the appendix.

II. KAT AND MUTABLE TESTS

A. KA and KAT

A Kleene algebra $(K, +, \cdot, *, 0, 1)$ is an idempotent semiring with an iteration operator $*$ satisfying

\[
1 + pp^* = p^* \quad q + pr \leq r \rightarrow p^* q \leq r
\]

\[
1 + p^* p = p^* \quad q + rp \leq r \rightarrow qp^* \leq r
\]

where $\leq$ refers to the natural partial order on $K$. 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, as well as other more unusual interpretations used in shortest path algorithms and computational geometry.

The following are some typical KA identities:

\[
(p^* q)^* p^* = (p + q)^* \quad (1)
\]

\[
p(qp)^* = (pq)^* p \quad (2)
\]

\[
p^* = (p^n)^* (1 + p + \cdots + p^{n-1}) \quad (3)
\]

All KA operations are monotone with respect to $\leq$.

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

\[
(K, +, *, 0, 1) \text{ is a Kleene algebra,}
\]

\[
(B, +, -, 0, 1) \text{ is a Boolean algebra, and}
\]

$B$ as a semiring is a subalgebra of $K$.

The Boolean complementation operator $-$ is defined only on $B$. Elements of $B$ are called tests. The letters $p, q, r, s$ denote arbitrary elements of $K$ and $a, b, c$ denote tests. The operators $+, -, 0, 1$ each play two roles: applied to arbitrary elements of $K$, they refer to nondeterministic choice, composition, fail, and skip, respectively; and applied to tests, they take on the additional meaning of Boolean disjunction, conjunction, falsity, and truth, respectively. These two usages do not conflict; for example, sequential testing of $b$ and $c$ is the same as testing their conjunction.

Conventional imperative programming constructs and propositional Hoare logic is subsumed. The deductive completeness and complexity results for KA and KAT [9, 24, 25] say that the axioms are complete for the equational theory of standard language and relational models and that the equational theory is decidable in PSPACE.

See [6] for a more thorough introduction.

B. Mutable Tests

Let $T_n = \{t_1, \ldots, t_n\}$ be a set of primitive test symbols. Consider a set of primitive actions $\{t! ? \mid t \in T_n\}$ (note that $\overline{t!} = t!$). We write $t?$ for the test $t$ to emphasize the distinction between $t?$ and $t!$. Let $F_n$ be the free KAT over primitive actions $\{t! ? \mid t \in T_n\}$ and primitive tests $T_n$ modulo the following equations:

\[
(i) \quad t! t? = t!
\]

\[
(ii) \quad t? t! = t?
\]

\[
(iii) \quad t!! = \overline{t!}
\]

\[
(iv) \quad s! t! = t! s!, \text{ provided } s \neq \overline{t}.
\]

\[
(v) \quad s! t? = t! s!, \text{ provided } s \notin \{t, \overline{t}\}.
\]

Intuitively, axiom (i) says that the action $t!$ makes a subsequent test $t?$ true, (ii) says that if $t?$ is already true, then the action $t!$ is redundant, (iii) says that setting a value overrides a previous such action on the same value, and (iv) and (v) say that actions and tests on different values are independent.

The theory B! refers to the equational consequences of (i)–(v) along with the axioms of KAT on terms over $T_n$. Two immediate such consequences are

\[
(vi) \quad t! t! = t!
\]

\[
(vii) \quad t!! = 0.
\]

An atom of $T_n$ is a sequence $s_1 s_2 \cdots s_n$, where each $s_i$ is either $t_i$ or $\overline{t_i}$. Atoms are denoted $\alpha, \beta, \ldots$. The set of atoms is denoted $At$. We write $\alpha \leq t$ if $t$ appears in $\alpha$. Let $\alpha[t]$ denote the atom $\alpha$ if $\alpha \leq t$ and $\alpha$ with $\overline{t}$ replaced by $t$ if $\alpha \leq \overline{t}$. Each atom $\alpha = s_1 \cdots s_n$ determines a complete test $\alpha! = s_1? s_2! \cdots s_n? \in F_n$ and a complete assignment $\alpha! = s_1! s_2! \cdots s_n! \in F_n$. The following are elementary
consequences of $B!$:

$$t? = \sum_{\alpha \leq t} \alpha?\alpha! \quad t! = \sum_{\alpha} \alpha?\alpha[t]!$$

(4)

$$\alpha!\alpha? = \alpha! \quad \alpha?\alpha! = \alpha? \quad \alpha!\beta! = \beta! \quad \alpha?\beta? = 0 \text{ if } \alpha \neq \beta.$$  

(5)

C. Mutable Tests and Binary Relations

The following theorem characterizes the free $B!$ algebra $F_n$. The theorem shows that $B!$ is sound in the sense that the free model does not trivialize to the one-element algebra.

**Theorem 2.1:** The algebra $F_n$ is isomorphic to the full binary relation algebra on a set of size $2^n$.

**Proof:** The set $At$ is of size $2^n$. Consider the algebra of binary relations on $At$. This algebra is isomorphic to $\text{Mat}(At, 2)$, the KAT of $At \times At$ matrices over the two-element KAT with the usual Boolean matrix operations. We will construct an isomorphism $h_n : F_n \to \text{Mat}(At, 2)$.

For the generators, let $h_n(t?)$ and $h_n(t!)$ be $At \times At$ matrices with components

$$h_n(t?)_{\alpha\beta} = \begin{cases} 
1 & \text{if } \alpha \leq t \text{ and } \beta = \alpha[t] \\
0 & \text{otherwise}, 
\end{cases}$$

and

$$h_n(t!)_{\alpha\beta} = \begin{cases} 
1 & \text{if } \beta = \alpha[t] \\
0 & \text{otherwise}. 
\end{cases}$$

One can show without difficulty that the axioms (i)–(v) of $B!$ are satisfied under the interpretation $h_n$. For example, for (ii),

$$(h_n(t?)h_n(t!))_{\alpha\beta} = \sum_{\gamma} h_n(t?)_{\alpha\gamma} h_n(t!)_{\gamma\beta} = h_n(t?)_{\alpha\alpha} h_n(t!)_{\alpha\beta}$$

$$= \begin{cases} 
1 & \text{if } \alpha \leq t \text{ and } \beta = \alpha[t] \\
0 & \text{otherwise}, 
\end{cases}$$

$$= \begin{cases} 
1 & \text{if } \alpha \leq t \text{ and } \beta = \alpha \\
0 & \text{otherwise}. 
\end{cases}$$

$$= h_n(t?)_{\alpha\beta}.$$  

Since $F_n$ is the free $B!$ algebra on generators $T_n$, $h_n$ extends uniquely to a KAT homomorphism $h_n : F_n \to \text{Mat}(At, 2)$. Under this extension, $h_n(\alpha?\beta!)$ is the matrix with 1 in location $\alpha\beta$ and 0 elsewhere. As every matrix in $\text{Mat}(At, 2)$ is a sum of such matrices, $h_n$ is surjective.

We wish also to show that $h_n$ is injective. To do this, we show that every element of $F_n$ is a sum of elements of the form $\alpha?\beta!$. This is true for primitive tests $t?$ and primitive actions $t!$ by (4). The constants 1 and 0 are equivalent to $\sum_\alpha \alpha?\alpha!$ and the empty sum, respectively.

For sums, the conclusion is trivial. For products, we observe using (5) that $\alpha?\beta!\gamma! = 0$ if $\beta \neq \gamma$ and $\alpha?\beta!\beta! = \alpha?\beta!$. By distributivity, this allows the product of two sums of elements of the form $\alpha?\beta!$ to be reduced to a sum of the same form. For $e$, any element of the form $e^s$ where $e$ is a sum of elements of the form $\alpha?\beta!$ is equivalent to $1 + e + e^2 + \cdots + e^m$ for some $m$, since $At$ is finite.

Now if $A \subseteq At^2$, then $h_n(\sum_{\alpha\beta \in A} \alpha?\beta!)$ is the matrix with 1 in locations $\alpha\beta \in A$ and 0 elsewhere. Thus if $A, B \subseteq At^2$ and $h_n(\sum_{\alpha\beta \in A} \alpha?\beta!) = h_n(\sum_{\alpha\beta \in B} \alpha?\beta!)$, then $A = B$, therefore $\sum_{\alpha\beta \in A} \alpha?\beta! = \sum_{\alpha\beta \in B} \alpha?\beta!$.  

There are some interesting facts about $F_n$ that are worth observing, although we will not need them in the sequel. We can express the state set $At$ as the tensor product of $n$ copies of $2$, one copy for each $t \in T_n$. The structure $F_1$ is the algebra $\text{Mat}(2, 2)$ of $2 \times 2$ matrices. The matrices $h_n(t?)$ and $h_n(t!)$ are Kronecker products

$$h_1(t?) \otimes \bigotimes_{s \neq t} I \quad h_1(t!) \otimes \bigotimes_{s \neq t} I$$

where $h_1(t?)$ and $h_1(t!)$ are the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

respectively, where the first row and column correspond to index $t$ and the second to index $\bar{t}$, and $I$ is the $2 \times 2$ identity matrix. Matrix multiplication in $F_n$ satisfies

$$(A_1 \otimes \cdots \otimes A_n)(B_1 \otimes \cdots \otimes B_n) = A_1 B_1 \otimes \cdots \otimes A_n B_n,$$

which can be regarded as an independence condition on the $n$ components. Every matrix in $F_n$ can be expressed as a sum of Kronecker products of $2 \times 2$ matrices with exactly one nonzero entry corresponding to expressions of the form $\alpha?\beta!$.

D. The Commutative Coproduct

Let $K$ and $F$ be KATs. The commutative coproduct of $K$ and $F$ is the usual coproduct (direct sum) of $K$ and $F$ modulo commutativity conditions $\{ps = sp \mid p \in K, \ s \in F\}$ that say that elements of $K$ and $F$ commute multiplicatively. The commutativity conditions model the idea that operations in $K$ and $F$ are independent of each other.

The usual coproduct $K \oplus F$ comes equipped with canonical injections $i_K : K \to K \oplus F$ and $i_F : F \to K \oplus F$, although these “injections” need not be injective. The coproduct is said to be injective if $i_K$ and $i_F$ are injective.

Injectivity is important because it means the extension of an algebra $K$ with extra features $F$ is conservative in the sense that it does not introduce any new equations. The coproduct of KATs is not known to be injective in general; however, we shall show that if $F$ is a finite relation algebra, then the coproduct and commutative coproduct are injective.

Our proof relies on an explicit coproduct construction from universal algebra that holds for any variety or quasivariety $V$ (class of algebras defined by universally quantified equations or equational implications) over any signature $\Sigma$. We briefly review the construction here.

Let $T_K$ be the set of $\Sigma$-terms over $K$. The identity function $K \to K$ extends uniquely to a canonical homomorphism $T_K \to K$. The diagram of $K$, denoted $\Delta_K$, is the kernel of this homomorphism; this is the set of equations between $\Sigma$-terms over $K$ that hold in $K$. It follows from general considerations of universal algebra that $T_K/\Delta_K \cong K$, where $T/E$ denotes the quotient of $T$ modulo the $V$-congruence generated by equations $E$; that is, the smallest $\Sigma$-congruence $\Sigma m \oplus Z_n \cong Z_{gcd(m,n)}$ in the category of commutative rings.
on $T$ containing $E$ and closed under the equations and equational implications defining $V$.

Now let $T_{K,F}$ denote the set of mixed $\Sigma$-terms over the disjoint union of the carriers of $K$ and $F$. The coproduct is

$$K \oplus F = T_{K,F}/(\Delta_K \cup \Delta_F).$$

The canonical injection $i_K : K \to K \oplus F$ is obtained from the identity embedding $T_K \to T_{K,F}$ reduced modulo $\Delta_K$ on the left and $\Delta_K \cup \Delta_F$ on the right; the map is well-defined on $\Delta_K$-classes since $\Delta_K$ refines $\Delta_K \cup \Delta_F$. This construction satisfies the usual universality property for coproducts, namely that for any pair of homomorphisms $k : K \to H$ and $f : F \to H$, there is a unique homomorphism $(k,f) : K \oplus F \to H$ such that $k = (k,f) \circ i_K$ and $f = (k,f) \circ i_F$.

Now let $K$ and $F$ be KATs, and let $D$ be the set of commutativity conditions

$$D = \{ ps = sp \mid p \in K, \ s \in F \}$$
on $K \oplus F$. (This is actually an abuse of notation; it would be more accurate to say

$$D = \{ i_K(p)i_F(s) = i_F(s)i_K(p) \mid p \in K, \ s \in F \}.$$}

The commutative coproduct is the quotient $(K \oplus F)/D$. Composed with the canonical map $[\cdot] : K \oplus F \to (K \oplus F)/D$, $i_K$ and $i_F$ inject $K$ and $F$, respectively, into $(K \oplus F)/D$. The following universality property is satisfied:

**Lemma 2.2:** For any pair of homomorphisms $k : K \to H$ and $f : F \to H$ such that

$$\forall p \in K \forall s \in F \ k(p)f(s) = f(s)k(p),$$

there is a unique universal arrow $(k,f)_D : (K \oplus F)/D \to H$ such that $k = (k,f)_D \circ [\cdot] \circ i_K$ and $f = (k,f)_D \circ [\cdot] \circ i_F$.

![Fig. 1: Universality property of the commutative coproduct](image)

**Proof:** Property (6) implies that $D$ refines the kernel of $(k,f) : K \oplus F \to H$, therefore $(k,f)$ factors uniquely as $(k,f)_D \circ [\cdot]$, as shown in Fig. 1.

Our main results depend on the following key lemma.

**Lemma 2.3:** Let $K$ and $F$ be KATs. If $F$ is finite, then every element of $(K \oplus F)/D$ can be expressed as a finite sum $\sum_{s \in F} p_s s$, where $p_s \in K$.

**Remark.** The lemma is not true in general without the assumption of finiteness. For example, it can be shown that the commutative coproduct of two copies of the free KA on one generator does not satisfy the lemma.

**Proof:** The lemma is certainly true of individual elements of $K$ and $F$. We show that the property is preserved under the KAT operations. The cases of $+$ and $\cdot$ are quite easy, using commutativity and distributivity.

The only difficult case is that of $\cdot$. We wish to show that $\left( \sum_{s \in F} p_s s \right)^\cdot$ is equivalent to a finite sum of the form $\sum_{t \in F} q_t t$. Let $\Sigma = \{ a_s \mid s \in F \}$ be a finite alphabet with one letter for each element of $F$, and let $Reg_{\Sigma}$ be the free KA on generators $\Sigma$. Consider the following homomorphisms generated by the indicated actions on $\Sigma$:

$$f : \Sigma^* \to F \quad g : Reg_{\Sigma} \to K \quad h : Reg_{\Sigma} \to K$$

For each $t \in F$, the set $f^{\cdot-1}(t) = \{ x \in \Sigma^* \mid f(x) = t \}$ is a regular set, as it is the set accepted by the deterministic finite automaton with states $F$, start state 1, accept state $t$, and transitions $\delta(s,a) = s \cdot f(a)$. It is easily shown by induction that for all $x \in \Sigma^*$, $\delta(s,x) = s \cdot f(x)$. Thus the automaton accepts $x$ exactly when $t = \delta(1,x) = f(x)$, that is, when $x \in f^{\cdot-1}(t)$.

Let $A$ be the $F \times F$ transition matrix of this automaton: $A_{st} = \sum_{sr \in A} a_{sr}$. Then $(A^*)_{st}$ represents the set of strings $x$ such that $s \cdot f(x) = t$. Moreover,

$$\left( \sum_{s \in F} a_s \right)^\cdot = \sum_{t \in F} (A^*)_{1t}$$

since every string is accepted at some state $t$.

Let $M$ be the $F \times F$ diagonal matrix with diagonal elements $M_{ss} = s$ and off-diagonal elements $M_{st} = 0$ for $s \neq t$. The homomorphisms $g$ and $h$ lift to $F \times F$ matrices over $Reg_{\Sigma}$ with

$$g(A)_{st} = \sum_{sr \in A} p_r r \quad h(A)_{st} = \sum_{sr \in A} p_r r.$$

Then for any $s,t \in F$,

$$(M \cdot g(A))_{st} = \sum_r M_{sr} g(A)_{rt} = M_{ss} g(A)_{st} = s \sum_{sr \in A} p_r r$$

$$= \sum_{sr \in A} p_r r \sum_{st \in A} p_t t = h(A)_{st} M_{tt}$$

$$= \sum_r h(A)_{sr} M_{rt} = (h(A) \cdot M)_{st}.$$ Since $s,t$ were arbitrary, $M \cdot g(A) = h(A) \cdot M$. By the bisimulation rule of KA [24, Proposition 4],

$$M \cdot g(A^*) = M \cdot g(A)^* = h(A)^* \cdot M = h(A^*) \cdot M,$$

thus for all $s,t \in F$,

$$s g(A^*)_{st} = M_{ss} g(A^*)_{st} = \sum_r M_{sr} g(A^*)_{rt} = (M \cdot g(A^*))_{st}$$

$$= (h(A^*) \cdot M)_{st} = \sum_r h(A^*)_{sr} M_{rt}$$

$$= h(A^*)_{st} M_{tt} = h(A^*)_{st} t.$$ In particular, setting $s = 1$ and summing over $t \in F$,

$$\sum_{t \in F} g(A^*)_{1t} = \sum_{t \in F} h(A^*)_{1t}.$$
Using (7) and (8),
\[
(\sum_{s \in F} p_s)\ast = \sum_{s \in F} g(a_s) = g(\sum_{s \in F} a_s) = g(\sum_{t \in F} (A^s)_{1t}) = \sum_{t \in F} g(A^s)_{1t} = \sum_{t \in F} h(A^s)_{1t}.
\]
Setting \(q_t = \sum_{t \in F} h(A^s)_{1t}\), we have expressed \(\sum_{s \in F} p_s\ast\) in the desired form.

**Theorem 2.4:** If \(K\) is a KAT and \(F\) is the full relation algebra on a finite set \(S\), then \((K \oplus F)/D \cong \text{Mat}(S, K)\).

**Proof:** For \(p \in K\), let \(k(p) \in \text{Mat}(S, K)\) be the \(S \times S\) diagonal matrix with \(p\) on the main diagonal and 0 elsewhere. For \(s \in F\), let \(f(s)\) be the standard representation of the binary relation \(s\) as an \(S \times S\) Boolean matrix. The maps \(k : K \to \text{Mat}(S, K)\) and \(f : F \to \text{Mat}(S, K)\) are injective KAT homomorphisms and embed \(K\) and \(F\) isomorphically in \(\text{Mat}(S, K)\). The image of \(F\) under \(f\) is \(\text{Mat}(S, 2)\), a subalgebra of \(\text{Mat}(S, K)\). By the universality property for coproducts, we have that \(k(p)f(s) = f(s)k(p)\), thus Lemma 2.2 applies and we have a KAT homomorphism \((k, f) : (K \oplus F)/D \to \text{Mat}(S, K)\). That this homomorphism is an isomorphism follows from Lemma 2.3 by the same argument as in Lemma 2.1. The construction is illustrated in Fig. 2.

**Fig. 2:** Matrix representation of the commutative coproduct

**Corollary 2.5:** If \(K\) is a KAT and \(F\) is any relation algebra on a finite set \(S\), then \((K \oplus F)/D\) is isomorphic to a subalgebra of \(\text{Mat}(S, K)\).

**Proof:** Compose an embedding of \(F\) into the full relation algebra on \(S\) with the map \(f\) of Theorem 2.4.

The following corollary says that the extension of an arbitrary KAT with mutable tests is conservative.

**Corollary 2.6:** If \(K\) is a KAT and \(F\) is any relation algebra on a finite set \(S\), then the commutative coproduct \((K \oplus F)/D\) is injective.

**Proof:** The maps \(k = (k, f) \circ i_K : K \to \text{Mat}(S, K)\) and \(f = (k, f) \circ i_F : F \to \text{Mat}(S, K)\) are injective. By Theorem 2.4, \((K \oplus F)/D \cong \text{Mat}(S, K)\), and \(k\) and \(f\) compose with this isomorphism to give the canonical injections from \(K\) and \(F\), respectively, to \((K \oplus F)/D\).

III. Completeness and Complexity

In §II, we showed that an arbitrary KAT \(K\) can be conservatively extended with a small amount of state in the form of a finite set of mutable tests and their corresponding mutation actions. As shown in Theorem 2.4, the resulting algebra is isomorphic to \(\text{Mat}(\text{At}, K)\), where \(\text{At}\) is the set of atoms of the free Boolean algebra generated by the mutable tests.

In this section we prove three results. First, the KAT axioms along with the axioms B! for mutable tests and the commutativity conditions \(D\) are complete for the equational theory of \((K \oplus F_n)/D\) relative to the equational theory of \(K\). This is quite a strong result in the sense that it holds for an arbitrary KAT \(K\), regardless of its nature. In particular, for the special case in which \(K\) is the free KAT on some set of generators, the model \((K \oplus F_n)/D\) is the free KAT with mutable tests \(T_n\). Most of the work for this result has already been done in §II.

The second result is that the equational theory \(B!\) is complete for PSPACE. This complexity class is characterized by alternation polynomial-time Turing machines; see [26].

The third result is that the equational theory of a free KAT augmented with mutable tests is complete for EXPSPACE, deterministic exponential space. This result is quite surprising, as both KAT and B! separately are complete for PSPACE, yet their combination is exponentially more complex in the worst case.

A. Completeness

Let \(K\) be an arbitrary KAT. Let \(KAT+B!\) denote the deductive system consisting of the axioms of KAT, the axioms for mutable tests \(B!\), and the commutativity conditions \(D\) over a language of KAT terms with primitive action and test symbols interpreted in \(K\) as well as a set of mutable tests \(T_n\). Let \(\Delta_K\) be the diagram of \(K\).

**Theorem 3.1:** The axioms \(KAT+B!+\Delta_K\) are complete for the equational theory of \((K \oplus F_n)/D\). In other words, the axioms \(KAT+B!\) are complete for the equational theory of \((K \oplus F_n)/D\) relative to the equational theory of \(K\).

**Proof:** Let \(e_1\) and \(e_2\) be expressions denoting elements of \((K \oplus F_n)/D\). By Theorem 2.1 and Lemma 2.3, we have

\[
KAT+B!+\Delta_K \vdash e_1 = \sum_{\alpha, \beta \in \text{At}} p_{\alpha\beta}\alpha?\beta!
\]

\[
KAT+B!+\Delta_K \vdash e_2 = \sum_{\alpha, \beta \in \text{At}} q_{\alpha\beta}\alpha?\beta!.
\]

If \((K \oplus F_n)/D \models e_1 = e_2\), we have under the canonical interpretation \(\langle k, i \rangle\) that the matrices \(\langle k, i\rangle(e_1)\) and \(\langle k, i\rangle(e_2)\) are equal, thus for all \(\alpha, \beta \in \text{At}\),

\[
p_{\alpha\beta} = \langle k, i\rangle(e_1)_{\alpha\beta} = \langle k, i\rangle(e_2)_{\alpha\beta} = q_{\alpha\beta},
\]

and conversely.

**Corollary 3.2:** The axioms \(KAT+B!\) are complete for the equational theory of \((K \oplus F_n)/D\), where \(K\) is the free KAT on some set of generators.
B. Complexity

Theorem 3.3: The equational theory $B!$ is PSPACE-complete.

Remark. We note that neither the upper nor the lower bound follows from previous results. The upper bound does not follow from results on elimination of hypotheses [3, 9, 10], as axioms (i) and (ii) can be eliminated by these results, but not the others.

Proof: We first show that the problem of deciding $\alpha\beta! \leq e$, where $\alpha, \beta \in At$, is in PSPACE. We give an alternating polynomial-time algorithm that operates inductively on the structure of $e$.

To decide $\alpha\beta! \leq t$ or $\alpha\beta! \leq !t$, using (4) we can ask whether $\alpha = \beta \leq t$ or $\beta = \alpha[t]$, respectively.

For addition, we have $\alpha\beta! \leq e_1 + e_2$ iff $\alpha\beta! \leq e_1$ or $\alpha\beta! \leq e_2$. We nondeterministically choose one of these alternatives and check it recursively.

For multiplication, we have $\alpha\beta! \leq e_1e_2$ iff there exists $\gamma$ such that $\alpha\gamma! \leq e_1$ and $\gamma\beta! \leq e_2$. We guess $\gamma$ nondeterministically using existential branching and check both conditions recursively using universal branching.

Finally, to check $\alpha\beta! \leq e^*$, by Theorem 2.1 it suffices to check that $\alpha\beta! \leq e^k$ for some $0 \leq k < 2^n$. We guess $k$ nondeterministically using existential branching. To check $\alpha\beta! \leq e^k$, we guess $\gamma$ nondeterministically using existential branching, and for each such $\gamma$, we check recursively using universal branching that $\alpha\gamma! \leq e^{k/2}$ and $\gamma\beta! \leq e^{k/2}$.

To decide the equational theory in PSPACE, we note that $e_1 \leq e_2$ if for all $\alpha, \beta \in At$, if $\alpha\beta! \leq e_1$, then $\alpha\beta! \leq e_2$. The $\alpha$ and $\beta$ can be chosen universally and the implication $\alpha\beta! \leq e_1 \Rightarrow \alpha\beta! \leq e_2$ checked in PSPACE.

To show PSPACE-hardness, we encode the membership problem for deterministic linear-bounded automata, a well known PSPACE-complete problem. Let $M$ be a deterministic linear-bounded automaton with states $Q$ and tape alphabet $\Gamma$. Let $x = x_1 \cdots x_n$ be an input string of length $n$ over $M'$s input alphabet. For $a \in \Gamma$, $q \in Q$, and $0 \leq i \leq n + 1$, introduce mutable tests $P_i^n$ and $Q_i^q$ with the following intuitive meanings:

$P_i^n = \text{the symbol currently occupying tape cell } i$ is $a$,

$Q_i^q = \text{the machine is currently in state } q$ scanning tape cell $i$.

The operation of the machine is governed by a transition function $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{+1, -1\}$. Intuitively, the transition $\delta(p, a) = (q, b, d)$ means, \textit{“When in state } p \text{ scanning symbol } a, \text{ print } b \text{ on that cell, move the head in direction } d, \text{ and enter state } q.”$ For each such transition, consider the expressions

$$P_i^nQ_i^q\overline{P_i^n}Q_i^qP_i^nQ_i^q \text{ for all } i.$$  \hfill (9)

for all $i$. The part $P_i^n?Q_i^q?$ tests whether the machine is currently scanning $a$ on cell $i$ in state $p$. If so, $\overline{P_i^n}Q_i^qP_i^nQ_i^q$ affects the transition to the new configuration as dictated by the transition function $\delta$. The truth values of variables not mentioned do not change.

Assume that the input is delimited by left and right endmarkers $\uparrow$ and $\downarrow$, that $M$ starts in its start state $s$ scanning the left endmarker $\downarrow$, that $M$ never overwrites the endmarkers, and that before accepting, $M$ erases its tape by writing a blank symbol $\omega$ on all tape cells except for the endmarkers, moves its head all the way to the left, and enters state $t$. The start and accept configurations are atoms

$$\begin{align*}
\text{start} &= Q_0^nP_0^nP_1^nP_2^n \cdots P_n^nQ_n^nU \\
\text{accept} &= Q_0^nP_0^nP_1^nP_2^n \cdots P_n^nQ_n^nV
\end{align*}$$

where $U$ and $V$ are the negations of the remaining variables. Let $e$ be the sum of all expressions (9). Then $M$ accepts $x$ if and only if $\text{start}\uparrow! \leq e^\ast$.

Let $K$ be the free KAT on some set of generators. As shown in Corollary 3.2, the equational theory of $\langle K \cup F_n \rangle / D$ is completely axiomatized by $KAT+B$.

Theorem 3.4: The set of equational consequences of $KAT+B$! (that is, the equational theory of a free KAT augmented with mutable tests) is EXPSPACE-complete.

Proof: Let $K$ be the free KAT on generators $\Sigma$ and $B$ augmented with mutable tests $T_n$. The tests $B$ are ordinary KAT tests and are not mutable. For the upper bound, to decide whether $e_1 \leq e_2$, first replace each primitive symbol in $e_1$ and $e_2$ with an $At \times At$ matrix as defined in the proof of Theorem 2.4. This gives a pair of expressions over $\text{Mat}(At, K)$. Now using the construction of Kleene’s theorem, construct nondeterministic finite automata $M_1$ and $M_2$ from these two expressions. These are nondeterministic automata on guarded strings over $\Sigma \cup B$ [27] with exponentially many states. We wish to know whether there exists a string $\alpha?x\beta! \leq e_1$ such that $\alpha?x\beta! \nleq e_2$, where $x$ is a guarded string over $\Sigma \cup B$. This is equivalent to asking whether there exists a guarded string accepted by $M_1$ but not by $M_2$, where the start and accept states are chosen appropriately to encode $\alpha?x\beta!$. We nondeterministically guess such a string $x$ letter by letter and a path through $M_1$, simultaneously keeping track of all states $M_2$ could be in at any time. This requires only exponential space. We have found such an $x$ if at any time $M_1$ is in an accept state but the set of states $M_2$ could be in does not contain an accept state. The algorithm can be made deterministic by Savitch’s theorem.

For the corresponding lower bound, we encode the membership problem for exponential-space bounded Turing machines. Given such a machine $M$ and an input $x$ of length $n$, we use $n$ mutable tests to construct an integer counter that can count up to $2^n - 1$, as illustrated in Fig. 3. We use the counter as a “yardstick” to construct an expression $e$ simulating a nondeterministic automaton that accepts all strings that are not valid computation histories of $M$ on input $x$. The automaton decides nondeterministically where to look for an incorrect move of $M$. It remembers a few symbols of the input string, then starts the counter. With each iteration of the counter, it skips over an input symbol (not shown in Fig. 3). In this way it can compare symbols a distance $2^n$ apart to check whether the transition rules of $M$ are followed. The expression $e$ generates…
A strictly deterministic automaton not equivalent to any while program

With strictly deterministic automata, Boolean values are provided by the environment in the form of an input string consisting of an infinite sequence of atoms, and the program responds with actions, including halting or failing. This is the correct propositional semantics: it allows all possible interpretations of the actions that could cause tests to become true or false. Two strictly deterministic automata are considered equivalent if they generate the same set of finite guarded strings (see [20] for formal definitions and details).

The Böhm–Jacopini theorem is true in the presence of mutable tests. The technique is well known, so rather than give a general account, we illustrate with the strictly deterministic automaton of Fig. 4. We introduce mutable tests \( t_0, t_1, \) and \( t_2, \) which serve as program counters. An equivalent deterministic while program with mutable tests is shown in Fig. 5. The major difference here is that the mutable tests are under the control of the program instead of the environment.

We have not given the formal definition of the set of guarded strings generated by a strictly deterministic automaton with mutable tests, but under the appropriate definition, it can be shown that this while program and the strictly deterministic automaton of Fig. 4 generate the same set of guarded strings.

B. A Folk Theorem

In this section we illustrate how KAT+B! can be used in practice. We will show, reasoning equationally in KAT+B!, a classical result of program schematology: Every while program can be simulated by a while program with at most one while loop, assuming that we allow extra Boolean variables. Many of the proofs are long sequences of simple equational inferences and are not very interesting in themselves, so we relegate them to an appendix.

We work with a programming language that has atomic programs (written \( a, b, \ldots, \)) the constant programs skip and fail, atomic tests, as well as the constructs: sequential composition \( f;g, \) conditional test if \( p \) then \( f \) else \( g, \) and iteration while \( p \) do \( f. \) These constructs are modeled in KAT as follows:

\[
\begin{align*}
skip &= 1 & fail &= 0 & f;g &= fg \\
&\quad \text{if } e \text{ then } f \text{ else } g &= ef + eg & \text{while } e \text{ do } f &= (ef)^* e
\end{align*}
\]

There is a semantic justification for these translations, using the standard relation-theoretic semantics for the input-output behavior of while programs. Intuitively, to show the result we introduce extra Boolean variables that encode the control structure of the program. These variables are modeled in KAT+B! using mutable tests \( t_1, t_2, \ldots, \) which are taken to

all strings iff \( M \) does not accept \( x. \) This construction is quite standard (see for example [26, 28, 29]), so we omit further details.

IV. APPLICATIONS

A. The Böhm-Jacopini Theorem

A well-studied problem in program schematology is that of transforming unstructured flowgraphs to structured form. An early seminal result is the Böhm–Jacopini theorem [11], which states that any deterministic flowchart program is equivalent to a deterministic while program. This theorem has reappeared in many contexts and has been reproved by many different methods [12–16].

Like most early work in program schematology, the Böhm–Jacopini theorem is usually formulated at the first-order level. This allows auxiliary individual or Boolean variables to be introduced to preserve information across computations. This is an essential ingredient of the Böhm–Jacopini construction, and they asked whether it was strictly necessary. This question was answered affirmatively by Ashcroft and Manna [12] and Kosaraju [19].

In [20], a purely propositional account of this negative result was given. A class of automata called strictly deterministic automata was presented, an abstraction of deterministic flowchart schemes. The three-state strictly deterministic automaton of Fig. 4 was shown not to be equivalent to any deterministic while program, where the \( \alpha_i \) are mutually exclusive and exhaustive tests and the \( p_{ij} \) are primitive actions.

![Fig. 4: A strictly deterministic automaton not equivalent to any while program](image-url)

We have not given the formal definition of the set of guarded strings (see [20] for formal definitions and details).
be disjoint from any mutable tests that might already appear in the program.

**Commutativity axioms:** KAT+B! has axioms that say that primitive actions commute with the mutable test symbols, that is, \( t!a = at! \) and \( t!a = at! \). Moreover, we assume \( t!p = pt! \) and \( t!\overline{p} = pt! \) for every atomic KAT test \( p \). The equations \( t!p = pt! \) are already axioms of KAT (tests commute). The following claims establish that using the axioms of KAT+B! more commutativity equations can be shown.

**Claim 4.1:** If the mutable test symbols \( t, \overline{t} \) do not appear in the KAT+B! test term \( p \), then we have that \( t!p = pt! \) and \( t!\overline{p} = pt! \).

**Claim 4.2:** If the mutable test symbols \( t, \overline{t} \) do not appear in the KAT+B! term \( f \), then \( t!f = ft! \) and \( t!f = ft! \).

The theorem that follows is a normal form theorem, from which the result we want to show follows immediately. Working in a bottom-up fashion, every while program term is brought in the normal form. That the transformed program in normal form is equivalent to the original one is shown in KAT+B!.

**Theorem 4.3:** For any while program \( f \), there are while-free \( u, p, \varphi \) and a finite collection \( t_1, \ldots, t_k \) of extra mutable tests such that \( f; z = u; \) while \( p \) do \( \varphi; \) \( z \), where \( z = t_1!; \ldots; t_k! \).

**Proof:** In the normal form given above, the pre-computation \( u \), the while-guard \( p \), and the while-body \( \varphi \) may involve the extra mutable test symbols \( t_1, \ldots, t_k \). These symbols do not appear in \( f \). The post-computation \( z = t_1!; \ldots; t_k! \) “zeroes out” all the extra mutable Boolean variables. Its rôle is in some sense to simply project out this extra finite state. The proof proceeds by induction on the structure of the while program term \( f \).

**Base case:** Suppose that \( f \) is a while-free program term, and let \( t \) be a fresh mutable test symbol. Intuitively, \( t? \) holds if \( f \) has not been executed yet, and \( t? \) holds when \( f \) has been executed. Reasoning in KAT+B!:

**Claim 4.4:** \( f; z = t!; \) while \( t\overline{?} \) do \( (f; t!); z \), where \( z = t! \).

**Induction step:** From the induction hypothesis, we can bring the programs \( f \) and \( g \) in normal form so that \( f; z = u; \) while \( p \) do \( \varphi; \) \( z \); and \( g; z = v; \) while \( q \) do \( \psi; \) \( z \), where \( z \) sets to zero all the mutable tests that appear in the transformations of \( f \) and \( g \). For the cases of a conditional test if \( e \) then \( f \) else \( g \) and composition \( f; g \), we introduce a fresh mutable test symbol \( t \).

**Conditional:** We handle the case if \( e \) then \( f \) else \( g \). Intuitively, the Boolean variable \( t \) records the symbol \( t \) records the branch to be taken. So, \( t? \) holds when \( f \) should be executed, and \( t? \) holds when \( g \) should be executed. Reasoning in KAT+B!:

**Claim 4.5:** The program (if \( e \) then \( f \) else \( g \)); \( z; t! \) is equal to

\[
\begin{align*}
\text{if } e & \text{ then } (t!; u) \text{ else } (t?; v) ; \\
\text{while } ((t? \land p) \lor (t? \land q)) & \text{ do } (\text{if } e \text{ then } \varphi \text{ else } \psi) ; \\
& \text{z; t!}.
\end{align*}
\]

**Sequential composition:** We handle the case \( f; g \). Intuitively, the Boolean variable \( t \) records the current position of execution. So, \( t? \) holds when we are executing \( f \), and \( t? \) when we are executing \( g \).

**Claim 4.6:** The program \( f; g; z; t! \) is provably equal to

\[
\begin{align*}
t!u; \\
\text{while } ((t? \lor (t? \land q)) \land \varphi) & \text{ do } (\text{if } e \text{ then } \psi) ; \\
& \text{z; t!}.
\end{align*}
\]

**Loop:** It remains to handle the case of the while loop while \( e \) do \( f \). First, we observe that

**Claim 4.7:** while \( e \) do \( f; z = \text{while } e \text{ do } (f; z) ; z \).

Using the above claim, we can bring the program in a more convenient form:

**Claim 4.8:** The program (while \( e \) do \( f \)); \( z \) is provably equal to

\[
\begin{align*}
\text{if } e \text{ then } (u; \text{while } (e + p) \text{ do } \psi) & \text{ else } (z; u) ; \\
& \text{z; t!}.
\end{align*}
\]

But we already know how to transform conditional statements. So, we apply that transformation to bring the term in the desired normal form.

**V. Conclusion**

We have shown how to axiomatically extend Kleene algebra with tests with a finite amount of mutable state. This extra feature allows certain program transformations to be effected at the propositional level without passing to a full first-order system. The extension is conservative and deductively complete relative to the theory of the underlying algebra. The full theory is decidable and complete for EXPSPACE. We have given a representation theorem of the free models in terms of matrices.

An intriguing open problem is whether the coproduct of two KATs is injective. We have shown that it is if one of the two cofactors is a relation algebra on a finite set.

**Acknowledgment**

Thanks to Bob Constable, Nate Foster, Fritz Henglein, Mark Reitblatt, Ross Tate, and Laure Thompson for valuable conversations and insights. The DIKU-affiliated author expresses his thanks to the Department of Computer Science at Cornell University for hosting him in the Fall 2013 and to the Danish Council for Independent Research for financial support for this work under Project 11-106278, “Kleene Meets Church (KMC): Regular Expressions and Types.”

**References**


APPENDIX

Proof of Claim 4.1: By induction on $p$. If $p$ is an atomic KAT test, then the claim follows directly from axioms. The cases of the constants 0 and 1 are trivial. If $p$ is a mutable test $s?$, then by our assumption we have that $s \neq t$, and therefore $t!s? = s!t? and t!s?! = s!!t?! are axioms of B!. For the induction step, consider the case $p + q$:

$$t!(p + q) = t!p + t!q = pt! + qt! = (p + q)t!$$

The case $p?q$ is similar. For the case of $t$, the equation $t!p = pt!$ follows from the induction hypothesis for $p$. Similarly, $t!p = t!p = pt! = \bar{p}t!$.

Proof of Claim 4.2: We only show the part involving $t!$, for $t$ the proof is essentially the same. We argue by induction on the structure of $f$. If $f$ is a test, then the result follows from Claim 4.1. If $f$ is an atomic program $a$, then from the stipulated axioms we have that $a! = a?!$. For composition and choice we have using the induction hypothesis: $t!fg = ft!g = fgt!$, and $t!(f + g) = t!f + t!g = ft! + gt! = (f + g)t!$.

It remains to show that $t!f = f*t$. By virtue of the bisimulation rule, it suffices to see that $t!f = ft!$, which is the induction hypothesis.

Proof of Claim 4.4: First, we unravel the expression $(f\langle ? f! \rangle)^*$ twice and observe that

$$(f\langle ? f! \rangle)^* = 1 + t?f\langle t? f! \rangle)^*$$

$$= 1 + t?f\langle 1 + t? f\langle t? f! \rangle \rangle)^*$$

$$= 1 + t?f! + t!f\langle t!f\rangle^*$$

$$= 1 + t?f!,$$

because $t?t? = t??t? = 0$. So, we conclude that

$$RHS = t!\langle t? f! \rangle^* \Rightarrow t!?$$

$$= t!(1 + t? f!)?$$

$$= t?? + t?! t? f! ?,$$

which is equal to $t!f! = f!t! = ft! = f; z$, since $t$ was chosen to be fresh (Claim 4.2).

Proof of Claim 4.5: The while-free pre-computation in the normal form translation is equal to $c!u + c?l!v$. The guard of the while loop is $t?p + t?q$, and the body is $t?\varphi + t?l?$. So,

$$((t? \land p) \lor (t? \land q)); (if t? then \varphi else \psi) = (t?p + t?l?q)(t?? \varphi \lor t?\psi) = t?p?\varphi \lor t?q?\psi.$$

The negation of the guard of the loop is $(t?q + t?q) = (t?q + t?) = t?q + t?q + t?q.$

First, we claim that $t!(t?\varphi)^* = t!(p\varphi)^*$. Since $t? \leq 1$ and $*$ is monotone, we have that $t?(p\varphi)^* \leq (p\varphi)^*$, and therefore
$t?(t?pϕ)∗ ≤ t?(pϕ)∗$. In order to show that $t?(pϕ)∗ ≤ t?(t?pϕ)∗$, it suffices to see that $t? ≤ t?(t?pϕ)∗$, and that


Now, we want to show that $t?(t?pϕ + t?qψ)∗ = t?(t?pϕ)∗$. By monotonicity of $∗$, the right-hand side is less than or equal to the left-hand side. For the other part, we need to show that

$$t?(t?pϕ)∗ (t?pϕ + t?qψ) = t?τ(t?pϕ)∗ (t?pϕ + t?qψ) = [prev\ claim]$$

$$t?τ(t?pϕ)∗ (t?pϕ + t?qψ) = [t \ not \ in \ p, ϕ]$$

$$t?τ(t?pϕ)∗ (t?pϕ + t?qψ) = [prev\ claim]$$

$$t?(t?pϕ)∗ t?pϕ = t?(t?pϕ)∗ t?pϕ,$$

which is $≤ t?(t?pϕ)∗$.

Let $W$ abbreviate the entire while loop of the normal form translation. We have already seen that


and therefore


because $t?qψ ≤ t?q$. So, we have

$$eRHS = e(CTLu + τfv)W z?τ = etluW z?τ = etluτW z?τ = etlu(pϕ)∗ t?pz?τ = e(u(pϕ)∗ t?pz?τ, which is equal to $efz?τ$ by the induction hypothesis. Similarly, it can be shown $τRHS = τgz?τ$. We thus conclude that

$$RHS = (e + τ)RHS = eRHS + τRHS = efz?τ + τgz?τ = (ef + τg)z?τ,$$

which is equal to $(if e \ then \ f \ else \ g); z; ?τ$, namely the left-hand size of the equation we wanted to show.


So, the Fisher-Ladner encoding of the while loop is


where we put $A = t?pϕ + t?pϕz?τ$.


$$(qψT?)∗ T?qψ = (qψT?)∗ qψT? = (qψT?)∗ T?qψ,$$

which is $≤ (qψT?)∗ T?$. We have thus shown that the while loop is equal to $A∗(qψT?)∗ T? = A∗(t?qψA∗)∗ T?.$

Now, we focus on simplifying the expression $t?A∗ T? = t?(t?pϕ + t?pϕz?τ)∗ T?$. First, we observe that unfolding $(t?pϕz?τ)∗$ twice gives us the equation


Moreover, $T?(t?pϕ)∗ T? = T?(1 + t?pϕ(pϕ)∗) = T?$. Therefore, using the denesting rule, we obtain that $t?A∗ T?$ is provably equal to


Finally, we can work on the right-hand side of the equation we want to establish:

$$RHS = tluAτ(qψψ)∗ qz?τ = tluAτ(qψψ)∗ qz?τ = tlu(qψψ)∗ pϕz?τ(qψψ)∗ qz?τ = u(pϕψ)∗ pϕz?τ(qψψ)∗ z?τ,$$

which is equal by the induction hypothesis to $fzg z?τ = fgz?τ = f; g; z; ?τ.$

\textbf{Proof of Claim 4.7:} The left-hand side is equal to $(ef)∗ τz$, and the right-hand side is equal to $(ef)∗ τz$. It suffices to show that $(ef)∗ z = (ef)∗ z$. $(ef)∗ z ≤ (ef)∗ z ↔ efz(ef)∗ z ≤ (ef)∗ z,$
which holds because $efz(ef)^*z = ef(ef)^*zz \leq (ef)^*z$.

Now, we observe that $(efz)^*z \leq z(efz)^*$ by the bisimulation rule, because $efzz = zefz$ (both are equal to $efz$). So,

$$(ef)^*z \leq (efz)^*z \iff ef(efz)^*z \leq (efz)^*z,$$

which holds because $ef(efz)^*z = ef(efz)^*zz = efz(efz)^*z \leq (efz)^*z$.

Proof of Claim 4.8: The above program is equal to

$$\begin{align*}
\tau z + eu[(e + p)(p\varphi + pzu)]^* (e + \overline{p})z &= \\
\tau z + eu[ep\varphi + epzu + p\varphi]^* \overline{z} p z &= \\
\tau z + eu(p\varphi + epzu)^* \overline{z} p z,
\end{align*}$$

because $ep\varphi \leq p\varphi$. Using the denesting rule (1) and then the sliding rule (2), we see that this is equal to

$$\begin{align*}
\tau z + eu(p\varphi)^* (epzu(p\varphi)^*)^* \overline{z} p z &= \\
\tau z + eu(p\varphi)^* (pzu(p\varphi)^*)^* \overline{z} p z &= \\
\tau z + (eu(p\varphi)^* \overline{z} p z)^* eu(p\varphi)^* \overline{z} p zz &= \\
\tau z + (efz)^* eu(p\varphi)^* \overline{z} p z &= \\
\tau z + (efz)^* (efz) \overline{z} z &= \\
(1 + (efz)^*) (efz) \overline{z} z =
\end{align*}$$

which is equal to $(efz)^* \overline{z} z = \text{while} e \text{ do } (f; z); z = (\text{while } e \text{ do } f); z$. □