Typed Kleene Algebra

Dexter Kozen
Department of Computer Science
Cornell University
Ithaca, New York 14853-7501, USA

March 17, 1998

Abstract

In previous work we have found it necessary to argue that certain theorems of Kleene algebra hold even when the symbols are interpreted as nonsquare matrices. In this note we define and investigate *typed Kleene algebra*, a typed version of Kleene algebra in which objects have types $\mathsf{s} \to \mathsf{t}$. Although nonsquare matrices are the principal motivation, there are many other useful interpretations: traces, binary relations, Kleene algebra with tests.

We give a set of typing rules and show that every expression has a unique *most general typing* (mgt). Then we prove the following metatheorem that incorporates the abovementioned results for nonsquare matrices as special cases. Call an expression *1-free* if it contains only the Kleene algebra operators (binary) $+$, (unary) $^+$, 0, and $\cdot$, but no occurrence of 1 or *. Then *every universal 1-free formula that is a theorem of Kleene algebra is also a theorem of typed Kleene algebra under its most general typing.* The metatheorem is false without the restriction to 1-free formulas.

1 Introduction

Typed Kleene algebra is motivated primarily by the desire to interpret regular expressions as matrices of various shapes, possibly nonsquare. For example, in the completeness proof of [6, 7], it must be argued that a few essential theorems of Kleene algebra, such as

$$ax \leq xb \;\;\rightarrow\;\; a^*x \leq xb^*, \tag{1}$$

still hold when the symbols are interpreted as matrices of various sizes and shapes, provided there is no type mismatch. The equational implication (1) holds in $\mathrm{Mat}(n, \mathcal{K})$, the $n \times n$ matrices over a Kleene algebra $\mathcal{K}$, simply by virtue of the fact that $\mathrm{Mat}(n, \mathcal{K})$ is a Kleene algebra. However, for the purposes of [6, 7], we need to know that it holds even when a is interpreted as an $m \times m$ matrix, x is interpreted as an $m \times n$ matrix, and b is interpreted as an $n \times n$ matrix for any m and n.

In [6, 7] we gave ad hoc arguments for each of the few theorems of Kleene algebra needed in the completeness proof. This was done by embedding non-square matrices in the upper left corner of sufficiently large square matrices. However, there are certain situations in which this technique fails; in particular, dealing with the identity matrix correctly presents subtle technical difficulties.

Understanding these subtleties and extending the theory to handle non-square matrices with sufficient generality and rigor calls for the introduction of a type discipline. We introduce such a type discipline in which regular expressions α have types of the form $\mathsf{s} \rightarrow \mathsf{t}$, where s and t are elements of an abstract set Ω. Every expression has a *most general typing* (mgt) under which the expression is well-typed and which refines every other typing for which this is true. For example, the most general typing of the expression ab^*c is $a : \mathsf{u} \rightarrow \mathsf{v}$, $b : \mathsf{v} \rightarrow \mathsf{v}$, $c : \mathsf{v} \rightarrow \mathsf{w}$, where u, v, and w are distinct. Most general typings exist and are unique up to a bijection. The Kleene algebra axioms under their most general typings give rise to a theory called *typed Kleene algebra*.

In our principal interpretation, $\Omega = \mathbb{N}$ and $\alpha : \mathsf{s} \rightarrow \mathsf{t}$ indicates that α is a matrix with row and column dimensions s and t, respectively. However, this is not the only interesting model of typed Kleene algebra. For example, consider sets of traces in a labeled transition system. We cannot compose traces p and q unless the terminal state of p is the same as the initial state of q; this can be handled with the type discipline. In this interpretation, the set Ω would be the set of states, and the type judgement $p : \mathsf{s} \rightarrow \mathsf{t}$ specifies that p has initial state s and terminal state t. For another example, interpreting s and t as subsets of a set X, the type judgement $\alpha : \mathsf{s} \rightarrow \mathsf{t}$ could be used to specify that α is a binary relation $\alpha \subseteq s \times t$. Here $\Omega = 2^X$. A third interpretation is the family of regular sets of guarded strings, the free Kleene algebra with tests [8, 9]. Finally, consider the semiadditive categories with * as defined by Manes [12]. A semiadditive category is one with zero morphisms, binary coproducts, and a natural transformation $\mathbf{id}_s \mapsto \mathbf{id}_s + \mathbf{id}_s$. The operator * is asserted to exist and satisfy the axioms of Section 2.1; it does not arise from the categorical structure. The categorical structure together with * give rise to a typed Kleene algebra whose elements are morphisms, pretypes are objects, multiplication is composition of morphisms, and addition is derived from the coproduct.

Our initial intent was to prove something like the following, which seemed deceptively obvious at first:

Proposition 1.1 *Every universal formula that is a theorem of Kleene algebra is a theorem of typed Kleene algebra under its most general typing.*

Unfortunately, Proposition 1.1 is false, even for universal Horn formulas. The Horn formula

$$0 = a \;\wedge\; a = 1 \quad\to\quad b = c$$

is a theorem of untyped Kleene algebra, but not of typed Kleene algebra under its mgt $a : \mathsf{u} \to \mathsf{u}$, $b : \mathsf{s} \to \mathsf{t}$, $c : \mathsf{s} \to \mathsf{t}$.

As noted above for the special case of matrices, the failure of Proposition 1.1 is apparently related to the presence of the multiplicative identity 1. To remedy the situation, we restrict attention to *1-free expressions*, a wide class of formulas that is almost fully general. An expression is *1-free* if it is built from the operators (binary) $+$, $\cdot$, 0, and (unary) $^+$ defined by $a^+ = aa^*$, but has no occurrence of 1 or *. There is a strong relationship between Kleene algebra and 1-free Kleene algebra that is detailed in Section 2.2.

All the theorems needed in the completeness proof of [6, 7] are equivalent to 1-free formulas; for example, in the presence of the other axioms, (1) above is equivalent to

$$ax \le xb \quad\to\quad a^+x \le xb^+.$$

Our main theorem can now be stated.

Theorem 1.2 *Every universal 1-free formula that is a theorem of Kleene algebra is a theorem of typed Kleene algebra under its most general typing.*

Whether the restriction to 1-free formulas can be weakened is a matter for further investigation.

One possible approach to proving Theorem 1.2 would be proof-theoretic. For Horn formulas $E \to \alpha = \beta$, one might show that every untyped proof in an equational deductive system also has a typed proof under the mgt of $E \to \alpha = \beta$. This would presumably involve transforming the untyped proof to a typed proof that does not impose any extra type constraints than are already present in the mgt of $E \to \alpha = \beta$. But this is not just a matter of typing intermediate expressions in the proof under their mgt; the problem is that the untyped proof might include some expressions that collapse types unnecessarily, so that the proof would not be well-typed under the mgt of $E \to \alpha = \beta$.

For example, one step of the untyped proof might use the rule of congruence for multiplication to obtain

$$\alpha = \beta \quad \to \quad \alpha 0 = \beta 0.$$

The left-hand side imposes a type constraint that the right-hand side does not, namely that if $\alpha : \mathsf{s} \to \mathsf{t}$ and $\beta : \mathsf{u} \to \mathsf{v}$, then $\mathsf{t} = \mathsf{v}$. The transitivity rule also poses a problem: after we apply it in the derivation

$$\alpha = \beta \wedge \beta = \gamma \quad \to \quad \alpha = \gamma,$$

the type constraints imposed by β are no longer present. We would have to show that these steps are extraneous and can be eliminated in a systematic way. Looking at these examples, one might conjecture that if $\vdash E \to \alpha = \beta$, then

$$\mathrm{mgt}\,(E \cup \{\alpha = \beta\}) \quad = \quad \mathrm{mgt}\, E.$$

This is not true either, as can be seen by considering the untyped theorem

$$\varnothing \to x^+ = x^+.$$

These pathologies indicate that the problem is more subtle and interesting than might first be imagined.

Our solution is model-theoretic rather than proof-theoretic. We define *1-free Kleene algebras*, a class of structures closely related to Kleene algebras, and show that every typed 1-free Kleene algebra can be embedded in an untyped 1-free Kleene algebra (a typed Kleene algebra in which Ω is a singleton). The conclusion follows from a strong functorial relationship between Kleene algebras and 1-free Kleene algebras, both typed and untyped.

2 Definitions

2.1 Kleene Algebra

Kleene algebras abound in computer science and mathematics, although often in disguised form [2, 4, 14, 15, 6, 7, 5, 16, 10, 11, 1, 13]. The definition used here was introduced in [6, 7].

A *Kleene algebra* is an algebraic structure

$$\mathcal{K} \quad = \quad (K,\, +,\, \cdot,\, ^*,\, 0,\, 1)$$

satisfying the following equations and equational implications:

$$\begin{array}{ll}
a + (b + c) = (a + b) + c & a + b = b + a \\
a + 0 = a & a + a = a \\
a(bc) = (ab)c & 1a = a1 = a \\
a(b + c) = ab + ac & (a + b)c = ac + bc \\
0a = a0 = 0 & \\
1 + aa^* = a^* & 1 + a^*a = a^*
\end{array}$$

$$b + ax \leq x \quad \rightarrow \quad a^*b \leq x \tag{2}$$

$$b + xa \leq x \quad \rightarrow \quad ba^* \leq x \tag{3}$$

where $\leq$ refers to the natural partial order:

$$a \leq b \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad a + b = b.$$

Instead of (2) and (3), we might take the equivalent axioms

$$ax \leq x \quad \rightarrow \quad a^*x \leq x \tag{4}$$

$$xa \leq x \quad \rightarrow \quad xa^* \leq x. \tag{5}$$

See [3, 6, 7] for some elementary consequences of these axioms.

We usually abbreviate $a \cdot b$ as ab and avoid parentheses by assigning the precedence $^* > \cdot > +$ to the operators.

A Kleene algebra is *-*continuous* if

$$ab^*c \quad = \quad \sup_{n \geq 0} ab^nc \tag{6}$$

where $b^0 = 1$, $b^{n+1} = bb^n$, and the supremum is with respect to the natural order $\leq$. The *-continuity condition (6) can be regarded as the conjunction of infinitely many axioms $ab^nc \leq ab^*c$ and the infinitary Horn formula

$$\bigwedge_{n \geq 0} (ab^nc \leq y) \quad \rightarrow \quad ab^*c \leq y.$$

This is not part of the axiomatization. Not all Kleene algebras are *-continuous, but all known natural examples are.

We also consider the unary $^+$ operator defined by

$$a^+ \stackrel{\text{def}}{=} aa^*. \tag{7}$$

Conversely, the operator * can be defined in terms of 1 and $^+$:

$$a^* = 1 + a^+. \tag{8}$$

2.2 1-Free Kleene Algebra

A *1-free Kleene algebra* is like a Kleene algebra, except that we omit the operators 1 and * and take the defined operator $^+$ as primitive. Formally, a *1-free Kleene algebra* is a structure

$$\mathcal{K} = (K,\ +,\ \cdot,\ ^+,\ 0)$$

satisfying the following equations and equational implications:

$$\begin{array}{ll}
a + (b + c) = (a + b) + c & a + b = b + a \\
a + 0 = a & a + a = a \\
a(bc) = (ab)c & \\
a(b + c) = ab + ac & (a + b)c = ac + bc \\
0a = a0 = 0 & \\
a + aa^+ = a^+ & a + a^+a = a^+
\end{array}$$

$$b + ax \leq x \quad \rightarrow \quad b + a^+b \leq x \tag{9}$$

$$b + xa \leq x \quad \rightarrow \quad b + ba^+ \leq x. \tag{10}$$

Instead of (9) and (10), we might take the equivalent axioms

$$ax \leq x \quad \rightarrow \quad a^+x \leq x \tag{11}$$

$$xa \leq x \quad \rightarrow \quad xa^+ \leq x. \tag{12}$$

These are just like the axioms of Kleene algebra, except that the axiom $1a = a1 = a$ has been omitted, and the axioms that refer to * have been altered to use $^+$ instead.

The *-continuity condition also has a 1-free analog:

$$ab^+c \quad = \quad \sup_{n \geq 1} ab^n c. \tag{13}$$

This is not part of the axiomatization, however.

There is a close functorial relationship between the category KA of Kleene algebras and Kleene algebra homomorphisms and the category $\mathsf{1fKA}$ of 1-free and Kleene algebras and 1-free Kleene algebra homomorphisms. Every Kleene algebra gives rise to a 1-free Kleene algebra by defining $^+$ as in (7) and "forgetting" 1 and *. This is the forgetful functor $\mathbb{F} : \mathsf{KA} \to \mathsf{1fKA}$.

Conversely, there is a natural construction $\mathbb{A} : \mathsf{1fKA} \to \mathsf{KA}$ that adds a multiplicative identity 1 to any 1-free Kleene algebra $\mathcal{K} = (K, +, \cdot, ^+, 0)$. The Kleene algebra $\mathbb{A}\,\mathcal{K}$ has domain $\{0, 1\} \times K$. Elements of the form $(1, a)$ are denoted $1 + a$ and elements of the form $(0, a)$ are denoted a. We thus regard the embedding $a \mapsto (0, a)$ as the identity map. The Kleene algebra operations $+$, $\cdot$, *, 0, 1 are defined on $\mathbb{A}\,\mathcal{K}$ as follows. The operations $+$, $\cdot$, and 0 applied to elements of $\mathcal{K}$ take the same values in $\mathbb{A}\,\mathcal{K}$ as they do in $\mathcal{K}$. The remaining values are defined as follows:

$$\begin{aligned}
(1 + a) + b &\stackrel{\text{def}}{=} 1 + (a + b) \\
a + (1 + b) &\stackrel{\text{def}}{=} 1 + (a + b) \\
(1 + a) + (1 + b) &\stackrel{\text{def}}{=} 1 + (a + b) \\
(1 + a)b &\stackrel{\text{def}}{=} b + ab \\
a(1 + b) &\stackrel{\text{def}}{=} a + ab \\
(1 + a)(1 + b) &\stackrel{\text{def}}{=} 1 + (a + b + ab) \\
a^* &\stackrel{\text{def}}{=} 1 + a^+ \\
(1 + a)^* &\stackrel{\text{def}}{=} 1 + a^+ \\
1 &\stackrel{\text{def}}{=} 1 + 0.
\end{aligned}$$

It is a straightforward matter to check that the resulting structure satisfies all the axioms of Kleene algebra. We verify axiom (4) explicitly. There are four cases to consider:

(i) $ax \leq x \quad \Rightarrow \quad (1+a^+)x \leq x$

(ii) $(1+a)x \leq x \quad \Rightarrow \quad (1+a^+)x \leq x$

(iii) $a(1+x) \leq 1+x \quad \Rightarrow \quad (1+a^+)(1+x) \leq 1+x$

(iv) $(1+a)(1+x) \leq 1+x \quad \Rightarrow \quad (1+a^+)(1+x) \leq 1+x.$

By the definitions above, these reduce to

(i) $ax \leq x \quad \Rightarrow \quad x + a^+x \leq x$

(ii) $x + ax \leq x \quad \Rightarrow \quad x + a^+x \leq x$

(iii) $a + ax \leq 1+x \quad \Rightarrow \quad 1 + a^+ + x + a^+x \leq 1+x$

(iv) $1 + a + x + ax \leq 1+x \quad \Rightarrow \quad 1 + a^+ + x + a^+x \leq 1+x,$

respectively. Now (i) and (ii) follow from axiom (11), and (iv) is subsumed by (iii), so it remains to show

$$a + ax \leq 1+x \quad \Rightarrow \quad 1 + a^+ + x + a^+x \leq 1+x,$$

or in other words

$$a + ax + 1 + x = 1+x \quad \Rightarrow \quad 1 + a^+ + x + a^+x + 1 + x = 1+x,$$

which by the definitions above reduces to

$$1 + a + ax + x = 1+x \quad \Rightarrow \quad 1 + a^+ + x + a^+x = 1+x.$$

Since $1+b = 1+c$ iff $c = d$ for $c, d \in K$, this reduces to

$$a + ax + x = x \quad \Rightarrow \quad a^+ + x + a^+x = x,$$

or more simply,

$$a + ax \leq x \quad \Rightarrow \quad a^+ + a^+x \leq x.$$

By axiom (11), it suffices to show

$$a + ax \leq x \quad \Rightarrow \quad a^+ \leq x,$$

and by the axiom $a + a^+a = a^+$, it suffices to show

$$a + ax \le x \quad \Rightarrow \quad a + a^+a \le x.$$

But this is an instance of axiom (9).

The functors $\mathbb{A}$ and $\mathbb{F}$ are adjoints. This means essentially that any 1-free homomorphism $h : \mathcal{K} \to \mathbb{F}\ \mathcal{L}$ from a 1-free Kleene algebra $\mathcal{K}$ to the 1-free part $\mathbb{F}\ \mathcal{L}$ of a Kleene algebra $\mathcal{L}$ extends uniquely to a Kleene algebra homomorphism $\widehat{h} : \mathbb{A}\ \mathcal{K} \to \mathcal{L}$.

The close relationship between Kleene algebra and 1-free Kleene algebra is reflected in the following result:

Theorem 2.1 *Any universal formula in the language of 1-free Kleene algebra is true in all Kleene algebras iff it is true in all 1-free Kleene algebras.*

Proof. More accurately, if φ is a universal 1-free formula, then φ is true in all 1-free Kleene algebras iff it is true in all 1-free Kleene algebras of the form $\mathbb{F}\ \mathcal{K}$ for $\mathcal{K}$ a Kleene algebra. The forward implication is immediate. Conversely, for any 1-free Kleene algebra $\mathcal{K}$, if φ is true in $\mathbb{F}\ \mathbb{A}\ \mathcal{K}$, then since $\mathcal{K}$ is a subalgebra of $\mathbb{F}\ \mathbb{A}\ \mathcal{K}$ and φ is universal, φ is also true in $\mathcal{K}$. $\square$

3 A Type Calculus

Terms in the language of Kleene algebra are built from variables $x, y, \ldots$, binary operators $+$ and $\cdot$, unary operators * and $^+$, and constants 0 and 1. Terms are often called *regular expressions* and are denoted $\alpha, \beta, \ldots$. Atomic formulas are equations between terms. The expressions $\alpha \le \beta$ and $\beta \ge \alpha$ are abbreviations for $\alpha + \beta = \beta$.

An expression or formula is *1-free* if it has no occurrences of * or 1, but only (binary) $+$, (unary) $^+$, $\cdot$, and 0.

Let Ω be a set and $\omega : \{x, y, \ldots\} \to \Omega^2$. Elements of Ω are denoted $\mathsf{s}, \mathsf{t}, \mathsf{u}, \mathsf{v}, \ldots$ and are called *pretypes*. Elements of Ω^2 are called *types* and are denoted $\mathsf{s} \to \mathsf{t}$. We also include a type 2 for Boolean values.

The map ω is called a *type environment*. If $\omega(x) = \mathsf{s} \to \mathsf{t}$, we write $x : \mathsf{s} \to \mathsf{t}$ and say that *x has type $\mathsf{s} \to \mathsf{t}$ under ω*.

We can use the following calculus to derive types for certain expressions from ω. A *type judgement* is an expression

$$\alpha : \mathsf{s} \to \mathsf{t} \qquad \text{or} \qquad \alpha = \beta : 2$$

where α and β are regular expressions and $\mathsf{s} \to \mathsf{t}$ and $\mathsf{2}$ are types. Given a type environment ω, types for compound terms and formulas are inferred inductively according to the following rules:

$$\frac{\alpha : \mathsf{s} \to \mathsf{t} \quad \beta : \mathsf{s} \to \mathsf{t}}{\alpha + \beta : \mathsf{s} \to \mathsf{t}} \qquad \frac{\alpha : \mathsf{s} \to \mathsf{t} \quad \beta : \mathsf{t} \to \mathsf{u}}{\alpha\beta : \mathsf{s} \to \mathsf{u}} \qquad \frac{\alpha : \mathsf{s} \to \mathsf{s}}{\alpha^* : \mathsf{s} \to \mathsf{s}}$$

$$0 : \mathsf{s} \to \mathsf{t} \qquad 1 : \mathsf{s} \to \mathsf{s} \qquad \frac{\alpha : \mathsf{s} \to \mathsf{t} \quad \beta : \mathsf{s} \to \mathsf{t}}{\alpha = \beta : \mathsf{2}}$$

The following rules can be derived:

$$\frac{\alpha : \mathsf{s} \to \mathsf{s}}{\alpha^+ : \mathsf{s} \to \mathsf{s}} \qquad \frac{\alpha : \mathsf{s} \to \mathsf{t} \quad \beta : \mathsf{s} \to \mathsf{t}}{\alpha \le \beta : \mathsf{2}} \qquad \frac{\alpha : \mathsf{s} \to \mathsf{t} \quad \beta : \mathsf{s} \to \mathsf{t}}{\alpha \ge \beta : \mathsf{2}}$$

Note that 0 has all types and 1 all square types (types of the form $\mathsf{s} \to \mathsf{s}$ for some $\mathsf{s} \in \Omega$).

Every type environment ω extends uniquely to a minimal set of type judgements closed under these rules. This unique extension is also denoted ω and is called a *typing*. An expression α is *well-typed* under the typing ω if ω contains a type judgement $\alpha : \mathsf{s} \to \mathsf{t}$. A set of expressions is said to be *well-typed* under ω if every expression in the set is well-typed under ω.

Not all expressions are well-typed under all typings. For example, if $x : \mathsf{s} \to \mathsf{t}$ and $\mathsf{s} \neq \mathsf{t}$, the expression x^* is not well-typed. Moreover, the type of an expression under a typing ω is not unique; for example, if $x : \mathsf{s} \to \mathsf{t}$, then $x0 : \mathsf{s} \to \mathsf{u}$ for all u. However, the type of a variable is unique.

Like the other operators $+$, $\cdot$, *, $^+$, different occurrences of 0 and 1 in the same expression can be typed differently depending on context. For example, if $x : \mathsf{s} \to \mathsf{t}$, then in a derivation of $x0x = 0 : \mathsf{2}$, the occurrence of 0 on the left-hand side would have type $\mathsf{t} \to \mathsf{s}$, and the occurrence of 0 on the right-hand side would have type $\mathsf{s} \to \mathsf{t}$.

3.1 Type Refinement and Most General Typing

In this section we define the concept of *most general typing* (mgt) of an expression or set of expressions and prove that most general typings exist and are unique up to a bijection.

Intuitively, a representation of the mgt of an expression can be constructed as follows. Assign a unique pair of pretypes to each symbol in the expression, then equate all and only those pretypes that must be equal in order for a type to be derivable for the expression. For example, consider the expression xy^*z. We would initially assign $x : \mathsf{p} \to \mathsf{q}$, $y : \mathsf{s} \to \mathsf{t}$, and $z : \mathsf{u} \to \mathsf{v}$, where $\mathsf{p}, \mathsf{q}, \mathsf{s}, \mathsf{t}, \mathsf{u}, \mathsf{v}$ are all distinct; but in order to type the expression, we would need $\mathsf{q} = \mathsf{s}$, $\mathsf{s} = \mathsf{t}$, and $\mathsf{t} = \mathsf{u}$. After collapsing these pretypes, we would be able to derive the typing $xy^*z : \mathsf{p} \to \mathsf{v}$.

Let Ω and Ω' be two sets of pretypes, and let ω and ω' be typings over Ω and Ω', respectively. The typing ω is said to *refine* ω' if there exists a function $h : \Omega \to \Omega'$ such that for all variables x, if $x : \mathsf{s} \to \mathsf{t}$ in the typing ω then $x : h(\mathsf{s}) \to h(\mathsf{t})$ in the typing ω'.

Lemma 3.1 *If ω refines ω', then any expression well-typed under ω is also well-typed under ω'.*

There may be expressions well-typed under ω' but not under ω. For example, if ω refines ω' via the function h, if $\mathsf{s} \neq \mathsf{t}$ but $h(\mathsf{s}) = h(\mathsf{t})$, and if $x : \mathsf{s} \to \mathsf{t}$ under ω, then x^* is well-typed under ω' but not under ω.

There are two extremal typings $\bot$ and $\top$, the "least collapsed" and "most collapsed" typings, respectively. The typing $\bot$ is generated by the type environment

$$x : \mathsf{s}_x \to \mathsf{t}_x$$

where s_x and t_x are distinct pretypes for each variable x. This typing types the fewest expressions. The typing $\top$ is generated by the type environment

$$x : \mathsf{o} \to \mathsf{o}$$

where o is the only pretype. Under this typing, every expression is typed. This gives the untyped theory. The typing $\bot$ refines every typing, and every typing refines $\top$.

Lemma 3.2 *Modulo the equivalence relation of mutual refinement, the set of typings forms a complete lattice ordered by refinement. Moreover, typing is continuous with respect to this lattice structure: for any expression α and any set D of typings, α is well-typed under* $\inf D$ *iff it is well-typed under all elements of D, and for any* directed *set D, α is well-typed under* $\sup D$ *iff it is well-typed under some element of D.*

Proof. Define

$$\Upsilon \stackrel{\text{def}}{=} \{\mathsf{s}_x, \mathsf{t}_x \mid x \text{ a variable}\}.$$

For any typing $\omega : \{x, y, \ldots\} \to \Omega^2$, collapse two elements of Υ if they have the same image under the unique map $\Upsilon \to \Omega$ under which $\perp$ refines ω. This gives an equivalence relation on Υ whose equivalence classes are in one-to-one correspondence with Ω. Thus every typing is equivalent under mutual refinement to a typing whose pretypes are equivalence classes of some equivalence relation on Υ. Moreover, two such typings inducing distinct equivalence relations on Υ are not equivalent under mutual refinement. Thus the set of typings modulo mutual refinement ordered by refinement is isomorphic to the complete lattice of equivalence relations on Υ.

Continuity follows from the fact that the coarsest common refinement of a set D of equivalence relations on Υ collapses two elements of Υ iff they are collapsed in all elements of D, and the join of a directed set D of equivalence relations on Υ collapses two elements of Υ iff they are collapsed in some element of D. □

Definition 3.3 A *most general typing* of a set E of expressions, denoted mgt E, is a typing under which E is typed and which refines any other typing under which E is typed. □

Theorem 3.4 *For any set E of expressions,* mgt E *exists and is unique up to mutual refinement.*

Proof. The set E is well-typed under $\top$. By Lemma 3.2, the typings under which E is well-typed have an infimum mgt E that is unique up to mutual refinement, and by continuity, E is well-typed under mgt E. □

3.2 Typed Kleene Algebra

Informally, a *typed Kleene algebra* is structure in which

- each element has a unique type of the form $\mathsf{s} \to \mathsf{t}$;
- there is a collection of polymorphic typed operators $+$, $\cdot$, *, 0, 1 whose application is governed by the typing rules of Section 3;

- all well-typed instances of the Kleene algebra axioms of Section 2.1 hold.

Formally, a *typed Kleene algebra* is a structure

$$\mathcal{K} \quad = \quad (K,\ \Omega,\ \omega,\ +,\ \cdot,\ ^*,\ 0,\ 1,\ =)$$

where K and Ω are sets and $\omega : K \to \Omega^2$. Elements of K are denoted $a, b, c, \ldots$. We write $\omega(a) = \mathsf{s} \to \mathsf{t}$ and $a : \mathsf{s} \to \mathsf{t}$ interchangeably.

For $\mathsf{s}, \mathsf{t} \in \Omega$, define

$$K_{\mathsf{s}\to\mathsf{t}} \quad = \quad \{a \in K \mid \omega(a) = \mathsf{s} \to \mathsf{t}\}.$$

The operators $+$, $\cdot$, *, 0, 1 and relation $=$ have the following polymorphic types:

$$\begin{array}{rcl} + & : & \Lambda\mathsf{s},\mathsf{t} \in \Omega.(\mathsf{s} \to \mathsf{t}) \times (\mathsf{s} \to \mathsf{t}) \to (\mathsf{s} \to \mathsf{t}) \\ \cdot & : & \Lambda\mathsf{s},\mathsf{t},\mathsf{u} \in \Omega.(\mathsf{s} \to \mathsf{t}) \times (\mathsf{t} \to \mathsf{u}) \to (\mathsf{s} \to \mathsf{u}) \\ ^* & : & \Lambda\mathsf{s} \in \Omega.(\mathsf{s} \to \mathsf{s}) \to (\mathsf{s} \to \mathsf{s}) \\ 0 & : & \Lambda\mathsf{s},\mathsf{t} \in \Omega.(\mathsf{s} \to \mathsf{t}) \\ 1 & : & \Lambda\mathsf{s} \in \Omega.(\mathsf{s} \to \mathsf{s}) \\ = & : & \Lambda\mathsf{s},\mathsf{t} \in \Omega.(\mathsf{s} \to \mathsf{t}) \times (\mathsf{s} \to \mathsf{t}) \to 2. \end{array}$$

This means for example that $+$ consists of a family of functions $+_{\mathsf{s}\to\mathsf{t}} : K^2_{\mathsf{s}\to\mathsf{t}} \to K_{\mathsf{s}\to\mathsf{t}}$, one for each choice of $\mathsf{s}, \mathsf{t} \in \Omega$. The operator $+_{\mathsf{s}\to\mathsf{t}}$ can only be applied to arguments of type $\mathsf{s} \to \mathsf{t}$ and produces a sum of type $\mathsf{s} \to \mathsf{t}$. The polymorphic constant 0 represents a family of elements $0_{\mathsf{s}\to\mathsf{t}}$, one for each choice of $\mathsf{s}, \mathsf{t} \in \Omega$. The polymorphic constant 1 represents a family of square elements $1_{\mathsf{s}\to\mathsf{s}}$, $\mathsf{s} \in \Omega$.

To be a typed Kleene algebra, $\mathcal{K}$ must also satisfy all well-typed instances of the Kleene algebra axioms. For example, the multiplicative associativity property $a(bc) = (ab)c$ must hold whenever the expression $a(bc) = (ab)c$ makes type sense; that is, whenever $a : \mathsf{s} \to \mathsf{t}$, $b : \mathsf{t} \to \mathsf{u}$, and $c : \mathsf{u} \to \mathsf{v}$ for some $\mathsf{s}, \mathsf{t}, \mathsf{u}, \mathsf{v} \in \Omega$.

Typed 1-free Kleene algebras are defined similarly, except we use the axiomatization of Section 2.2. The operator $^+$ has the same polymorphic type as *:

$$^+ \quad : \quad \Lambda s \in \Omega.(\mathsf{s} \to \mathsf{s}) \to (\mathsf{s} \to \mathsf{s}).$$

3.3 Homomorphisms

Let $\mathcal{K}$ and $\mathcal{K}'$ be typed structures of the signature of Kleene algebra. A *typed Kleene algebra homomorphism* $h : \mathcal{K} \to \mathcal{K}'$ is a two-sorted map

$$h : \Omega \ \to \ \Omega' \qquad\qquad h : K \ \to \ K'$$

such that for any a, s, and t,

$$a : \mathsf{s} \to \mathsf{t} \ \ \Rightarrow \ \ h(a) : h(\mathsf{s}) \to h(\mathsf{t}),$$

and h commutes with the distinguished operations in the sense that all well-typed instances of the following equations hold:

$$\begin{array}{rcl} h(a+b) & = & h(a)+h(b) \\ h(ab) & = & h(a)h(b) \\ h(a^*) & = & h(a)^* \\ h(0) & = & 0 \\ h(1) & = & 1. \end{array}$$

A *1-free homomorphism* is similar, except that that it is only required to preserve 0, $+$, $\cdot$, and $^+$.

4 Proof of Theorem 1.2

Lemma 4.1 *Every typed 1-free Kleene algebra can be embedded into an untyped 1-free Kleene algebra.*

Proof. Let

$$\mathcal{K} \ \ = \ \ (K,\ \Omega,\ \omega,\ +,\ ^+,\ \cdot,\ 0)$$

be a typed 1-free Kleene algebra. Form the untyped 1-free Kleene algebra $\mathrm{Mat}_1(\Omega, \mathcal{K})$ as follows. An $\Omega \times \Omega$ *matrix over* $\mathcal{K}$ is an element of the dependent product

$$\prod_{\mathsf{s},\mathsf{t} \in \Omega} K_{\mathsf{s}\to\mathsf{t}};$$

that is, a map $A : \Omega^2 \to K$ such that $A(\mathsf{s},\mathsf{t}) \in K_{\mathsf{s}\to\mathsf{t}}$. A matrix A is *of finite support* iff $A(\mathsf{s},\mathsf{t}) = 0_{\mathsf{s}\to\mathsf{t}}$ for all but finitely many pairs s,t. The algebra $\mathrm{Mat}_1(\Omega,\mathcal{K})$ consists of all $\Omega\times\Omega$ matrices of finite support over $\mathcal{K}$. The operations $+$, $\cdot$, 0 are the usual matrix sum, matrix product, and zero matrix:

$$\begin{aligned}(A+B)(\mathsf{s},\mathsf{t}) &\stackrel{\text{def}}{=} A(\mathsf{s},\mathsf{t}) + B(\mathsf{s},\mathsf{t})\\ (AB)(\mathsf{s},\mathsf{t}) &\stackrel{\text{def}}{=} \sum_{\substack{\mathsf{u}\in\Omega\\ A(\mathsf{s},\mathsf{u})B(\mathsf{u},\mathsf{t})\neq 0}} A(\mathsf{s},\mathsf{u})B(\mathsf{u},\mathsf{t})\\ 0(\mathsf{s},\mathsf{t}) &\stackrel{\text{def}}{=} 0_{\mathsf{s}\to\mathsf{t}}.\end{aligned}$$

The operation $^+$ is defined as follows. For any A, let Ω' be any finite subset of Ω containing the support of A; that is, such that $A(\mathsf{s},\mathsf{t}) = 0_{\mathsf{s}\to\mathsf{t}}$ if either $\mathsf{s}\notin\Omega'$ or $\mathsf{t}\notin\Omega'$. Let A' be the $\Omega'\times\Omega'$ submatrix of A. Since A' is finite, we can form A'^* and prove that it satisfies (4) and (5) as in [6, 7]. Then $A'^+ \stackrel{\text{def}}{=} A'A'^*$ satisfies (11) and (12). We define A^+ to be the matrix

$$A^+(\mathsf{s},\mathsf{t}) \stackrel{\text{def}}{=} \begin{cases} A'^+(\mathsf{s},\mathsf{t}), & \text{if } \mathsf{s},\mathsf{t}\in\Omega'\\ 0_{\mathsf{s}\to\mathsf{t}}, & \text{otherwise.}\end{cases}$$

It is not difficult to check that the matrix algebra $\mathrm{Mat}_1(\Omega,\mathcal{K})$ satisfies all the axioms of 1-free Kleene algebra.

We can embed $\mathcal{K}$ into $\mathrm{Mat}_1(\Omega,\mathcal{K})$ as follows. Let $h : \mathcal{K}\to\mathrm{Mat}_1(\Omega,\mathcal{K})$ be the map

$$h(a)_{\mathsf{s}\to\mathsf{t}} \stackrel{\text{def}}{=} \begin{cases} a, & \text{if } a : \mathsf{s}\to\mathsf{t}\\ 0_{\mathsf{s}\to\mathsf{t}}, & \text{otherwise.}\end{cases}$$

It is easily checked that h is a typed 1-free homomorphism. □

Note that even if A is of finite support, A^* need not be; in fact, we have not even defined A^* or 1. However, A^+ is always of finite support if A is. Moreover, there is no obvious way to extend the embedding h constructed in the proof of Lemma 4.1 to include A^* or 1.

Proof of Theorem 1.2. Let φ be a 1-free universal formula that is true in all Kleene algebras. Let

$$\mathcal{K} = (K,\ \Omega,\ \omega,\ +,\ \cdot,\ ^*,\ 0,\ 1,\ =)$$

be any typed Kleene algebra and σ a valuation of the variables in φ over $\mathcal{K}$ under which φ is well-typed. We wish to argue that φ holds under σ.

By Lemma 4.1, there is a 1-free embedding $h : \mathbb{F}\,\mathcal{K} \to \mathrm{Mat}_1(\Omega, \mathcal{K})$. Let $\tau = h \circ \sigma$. The map τ interprets φ in $\mathrm{Mat}_1(\Omega, \mathcal{K})$. Since this is an untyped 1-free Kleene algebra, and since by assumption φ is a theorem of untyped 1-free Kleene algebra, we have that

$$\mathrm{Mat}_1(\Omega, \mathcal{K}), \tau \quad \models \quad \varphi.$$

Since h is one-to-one, this implies that $\mathcal{K}, \sigma \models \varphi$.

Since $\mathcal{K}$ and σ were arbitrary, the universal formula φ is a theorem of typed 1-free Kleene algebra under any typing in which it is well-typed; in particular, by Theorem 3.4, under its most general typing. □

Acknowledgements

I am indebted to Michael Slifker and Mark Hopkins for valuable ideas and comments. This work was supported by the National Science Foundation under grant CCR-9708915.

References

[1] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms.* Addison-Wesley, Reading, Mass., 1975.

[2] Jean Berstel and Christophe Reutenauer. *Rational Series and Their Languages.* Springer-Verlag, Berlin, 1984.

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

[4] S. 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.

[5] Dexter Kozen. On induction vs. *-continuity. In Kozen, editor, *Proc. Workshop on Logic of Programs*, volume 131 of *Lecture Notes in Computer Science*, pages 167–176, New York, 1981. Springer-Verlag.

[6] Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. In *Proc. 6th Symp. Logic in Comput. Sci.*, pages 214–225, Amsterdam, July 1991. IEEE.

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

[8] Dexter Kozen. Kleene algebra with tests. *Transactions on Programming Languages and Systems*, pages 427–443, May 1997.

[9] 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.

[10] Werner Kuich. The Kleene and Parikh theorem in complete semirings. In T. Ottmann, editor, *Proc. 14th Colloq. Automata, Languages, and Programming*, volume 267 of *Lecture Notes in Computer Science*, pages 212–225, New York, 1987. EATCS, Springer-Verlag.

[11] Werner Kuich and Arto Salomaa. *Semirings, Automata, and Languages.* Springer-Verlag, Berlin, 1986.

[12] Ernest Manes. *Predicate transformer semantics.* Cambridge University Press, 1992.

[13] Kurt Mehlhorn. *Data Structures and Algorithms 2: Graph Algorithms and NP-Completeness.* EATCS Monographs on Theoretical Computer Science. Springer-Verlag, 1984.

[14] K. C. Ng. *Relation Algebras with Transitive Closure.* PhD thesis, University of California, Berkeley, 1984.

[15] K. C. Ng and A. Tarski. Relation algebras with transitive closure, abstract 742-02-09. *Notices Amer. Math. Soc.*, 24:A29–A30, 1977.

[16] Vaughan Pratt. Dynamic algebras as a well-behaved fragment of relation algebras. In D. Pigozzi, editor, *Proc. Conf. on Algebra and Computer Science*, volume 425 of *Lecture Notes in Computer Science*, pages 77–110, Ames, Iowa, June 1988. Springer-Verlag.