Alternative Axiomatizations

There has been some dissent regarding the proper axiomatization of Kleene algebra. Many inequivalent axiomatizations have been proposed [5, 16, 17, 7, 8], all serving roughly the same purpose. It is important to understand the relationships between these classes in order to extract the axiomatic essence of Kleene algebra. In this lecture we present some of these alternative axiomatizations and discuss some of the relationships among them.

Recall that our official definition is that a Kleene algebra is an idempotent semiring satisfying

$$1 + xx^* \leq x^* \tag{3.1}$$
$$1 + x^*x \leq x^* \tag{3.2}$$
$$b + ax \leq x \rightarrow a^*b \leq x \tag{3.3}$$
$$b + xa \leq x \rightarrow ba^* \leq x. \tag{3.4}$$

Star-Continuity

A Kleene algebra is called *star-continuous* (or sometimes *star-complete*) if it satisfies the axiom

$$xy^*z = \sup_{n \geq 0} xy^n z, \tag{3.5}$$

where $y^0 = 1$, $y^{n+1} = yy^n$, and sup refers to the *supremum* or *least upper bound* with respect to the natural order $\leq$. This property says that any possibly infinite set of the form $\{xy^nz \mid n \geq 0\}$ has a least upper bound, and that least upper bound is xy^*z. The property (3.5) is called *star-continuity.* Star-continuous Kleene algebras have been used to model programs in Dynamic Logic [7].

Every star-continuous idempotent semiring is a Kleene algebra, since one can easily show that in any idempotent semiring, the star-continuity condition (3.5) implies the axioms (3.1)–(3.4) of Kleene algebra. However, as we shall see later, not every Kleene algebra is star-continuous, although all naturally occurring ones are.

The property (3.5) is actually an infinitary condition. It is equivalent to infinitely many inequalities

$$xy^nz \leq xy^*z, \quad n \geq 0, \tag{3.6}$$

which together say that xy^*z is an upper bound for all xy^nz, $n \geq 0$, along with the infinitary Horn formula

$$(\bigwedge_{n\geq 0} xy^nz \leq w) \quad \rightarrow \quad xy^*z \leq w, \tag{3.7}$$

which says that it is the least such upper bound.

Another way to view (3.5) is as a combination of the statement that y^* is the supremum of y^n, $n \geq 0$, along with two infinitary distributivity properties, one on the left and one on the right.

To show that every star-continuous idempotent semiring is a Kleene algebra, we first show that (3.1) holds.

$$\begin{aligned} 1 + xx^* &= 1 + \sup_n xx^n \\ &= x^0 + \sup_n x^{n+1} \\ &= \sup_n x^n \\ &= x^*. \end{aligned}$$

The general property we have used in the third step is that if A and B are any subsets of an upper semilattice such that $\sup A$ and $\sup B$ exist, then $\sup A \cup B$ exists and is equal to $\sup A + \sup B$. The proof of (3.2) is symmetric.

To show (3.3), assume that $b + ax \leq x$. We would like to show that $a^*b \leq x$. By star-continuity, it suffices to show that for all $n \geq 0$, $a^nb \leq x$. This is easily shown by induction on n. For the basis $n = 0$, we have $a^0b = b \leq x$ from our assumption. Now assuming $a^nb \leq x$, we have $a^{n+1}b = aa^nb \leq ax$ by monotonicity, and $ax \leq x$ by our assumption. Again, the proof of (3.4) is symmetric.

Closed Semirings

In the design and analysis of algorithms, a related family of structures called *closed semirings* form an important algebraic abstraction. They give a unified framework for deriving efficient algorithms for transitive closure and all-pairs shortest paths in graphs and constructing regular expressions from finite automata [19, 1, 11]. Very fast algorithms for all these problems can be derived as special cases of a single general algorithm over an arbitrary closed semiring. Closed semirings are defined in terms of a countable summation operator $\sum$ as well as $\cdot$, 0, and 1; the operator * is defined in terms of $\sum$. Under the operations of (finite) $+$, $\cdot$, *, 0, and 1, any closed semiring is a star-continuous Kleene algebra. In fact, in the treatment of [1, 11], the sole purpose of $\sum$ seems to be to define *. A more descriptive name for closed semirings might be *ω-complete idempotent semirings*.

Formally, a *closed semiring* is an idempotent semiring in which every countable set A has a supremum $\sum A$ with respect to the natural order $\leq$, and such that for any countable set A,

$$x \cdot (\sum A) \cdot z \;=\; \sum_{y \in A} xyz. \tag{3.8}$$

The presence of x and z in (3.8) ensure a kind of infinite distributivity property on the left and right.

In any closed semiring, one can define * by

$$x^* \;\stackrel{\mathrm{def}}{=}\; \sum_{n \geq 0} x^n,$$

where $x^0 = 1$ and $x^{n+1} = xx^n$. By infinite distributivity,

$$xy^*z \;=\; \sum_n xy^nz,$$

thus any closed semiring is a star-continuous Kleene algebra.

The regular sets Reg_Σ do not form a closed semiring: if A is nonregular, the countable set $\{\{x\} \mid x \in A\}$ has no supremum. However, the power set of Σ^* does form a closed semiring.

Similarly, the family of all binary relations on a set forms a closed semiring under the relational operations described in Lecture **??** and set union for $\sum$.

The definition of closed semiring given above is somewhat stronger than those found in the literature on design and analysis of algorithms [1, 11]. According to [1], a closed semiring is an idempotent semiring equipped with a summation operator $\sum$ defined on countable *sequences* (not sets) that satisfies infinitary associativity and distributivity. Infinitary idempotence and commutativity are not assumed. Also, the relation between the between finitary + and infinitary $\sum$ is not explicitly mentioned in [1], but can be inferred from the use of the notation $x_0 + x_1 + x_2 + \cdots$ for the infinitary sum. The element x^* is defined to be $1 + x + x^2 + \cdots$.

Infinitary associativity is defined as follows. If $(x_n \mid n \geq 0)$ is any countable sequence of elements, then for any way of partitioning the index set $\mathbb{N}$ into intervals, the sum $\sum_i x_i$ is the same as the sum of the sums of the intervals. If an interval is finite, then its sum is computed with +. If an interval is infinite, then its sum is computed with $\sum$. Note that any such partition must consist either of

- infinitely many finite intervals, or
- finitely many intervals, all of which are finite except the last, which is infinite.

Infinitary distributivity says that

$$x \cdot (\sum_i y_i) \cdot z \quad = \quad \sum x y_i z.$$

This is not the same as (3.8), since it says nothing about suprema.

The axiomatization in [11] postulates infinitary commutativity as well. Infinitary commutativity says that for any partition of the index set (not necessarily into intervals), the sum of the sums of the partition elements is the same as the sum of the original sequence.

Infinitary idempotence says that if all $x_i = x$, then $\sum_i x_i = x$. This does not follow from the axiomatizations of [1, 11], nor does the equation $x^{**} = x^*$. It can be shown that $0^* = 1$, but not that $1^* = 1$.

To see this, consider an idempotent semiring with elements $\mathbb{N} \cup \{\infty\}$. Define finitary addition $+$ to be max in the natural order on $\mathbb{N}$, with ∞ being the largest element. Multiplication is ordinary multiplication in $\mathbb{N}$, extended to ∞ as follows:

$$\infty \cdot x \quad = \quad x \cdot \infty \quad \stackrel{\text{def}}{=} \quad \begin{cases} 0, & \text{if } x = 0 \\ \infty, & \text{otherwise.} \end{cases}$$

The constants 0 and 1 in the semiring are the natural numbers 0 and 1, respectively.

To define $\sum$ in this algebra, define the *support* of an infinite sequence $x = (x_n \mid n \geq 0)$ to be the set

$$\mathsf{supp}\, x \quad \stackrel{\text{def}}{=} \quad \{n \mid x_n \neq 0\}.$$

We define

$$\sum_n x_n \quad \stackrel{\text{def}}{=} \quad \begin{cases} \sum_{n \in \mathsf{supp}\, x} x_n, & \text{if } \mathsf{supp}\, x \text{ is finite} \\ \infty, & \text{otherwise.} \end{cases}$$

One can show that infinitary associativity, commutativity, and distributivity are satisfied, and $0^* = 1$. However, $0^{**} = 1^* = \infty$, so $\sum$ is not idempotent (since $1^* = 1 + 1 + 1 + \cdots$) and $0^{**} \neq 0^*$.

It is conjectured that the axiomatization of [1] does not imply infinitary commutativity. In particular, it is conjectured that

$$x_0 + x_1 + x_2 + \cdots \quad = \quad (x_0 + x_2 + x_4 + \cdots) + (x_1 + x_3 + x_5 + \cdots)$$

is not provable.

One can show that our official definition of closed semirings is equivalent to a countable summation operator $\sum$ satisfying infinitary associativity, commutativity, idempotence, and distributivity. Surely supremum is associative, commutative, and idempotent, and the axiom (3.8) gives distributivity as well.

Conversely, if $\sum$ is infinitely associative, commutative, and idempotent, then its value on a given sequence is independent of the order and multiplicity of elements occurring in the sequence. Thus we might as well define $\sum$ on finite or countable subsets instead of sequences. In this view, $\sum$ gives the supremum with respect to the natural order $\leq$. To see this, let A be a nonempty finite or countable set of elements. If $x \in A$, then

$$\begin{aligned} x + \sum A &= \sum (A \cup \{x\}) \\ &= \sum A \ , \end{aligned}$$

thus $x \leq \sum A$; and if $x \leq y$ for all $x \in A$, then $x + y = y$ for all $x \in A$, thus

$$\begin{aligned} (\sum A) + y &= (\sum_{x \in A} x) + (\sum_{x \in A} y) \\ &= \sum_{x \in A} (x + y) \\ &= \sum_{x \in A} y \\ &= y \ , \end{aligned}$$

therefore

$$\sum A \leq y.$$

Thus $\sum$ gives the supremum of countable sets.

Conway's Hierarchy

Closed semirings and star-continuous Kleene algebras are strongly related to several classes of algebras defined by Conway in his 1971 monograph [5]. Conway's S-algebras are similar to closed semirings, except that arbitrary sums, not just countable ones, are permitted. A better name for S-algebras might be *complete idempotent semirings*. The operation * is defined as in closed semirings in terms of $\sum$, and again this seems to be the main purpose of $\sum$.

Conway's N-algebras are algebras of signature $(+, \cdot, {}^*, 0, 1)$ that are subsets of S-algebras containing 0 and 1 and closed under (finite) $+$, $\cdot$, and *. We will show later that the classes of N-algebras and star-continuous Kleene algebras coincide.

An R-algebra is any algebra of signature $(+, \cdot, {}^*, 0, 1)$ satisfying the equational theory of the N-algebras.

According to the definition in [5], an S-algebra

$$(S, \ \sum, \ \cdot, \ 0, \ 1)$$

is similar to a closed semiring, except that $\sum$ is defined not on sequences but on multisets of elements of S. A *multiset* is a set whose elements have multiplicity; equivalently, it is an equivalence class of sequences, where two sequences are considered equivalent if one is a permutation of the other. In other words, a multiset is like a sequence, except that we ignore the order of the elements. However, there is no cardinality restriction on the multiset. One consequence of this approach is that $\sum$ is too big to be represented in Zermelo-Fraenkel set theory! Since $\sum$ is a function that must be defined on multisets of arbitrary cardinality, it cannot be a set itself. However, as with closed semirings, the value that $\sum$ takes on a given multiset is independent of the multiplicity of the elements, so $\sum$ might as well be defined on subsets of S instead of multisets. So defined, $\sum A$ gives the supremum of A with respect to the order $\leq$. (We assume the axiom $\sum\{a\} = a$, which is omitted in [5].)

Thus, the only essential difference between S-algebras and closed semirings is that closed semirings are only required to contain suprema of countable sets, whereas S-algebras must contain suprema of all sets. Thus every S-algebra is automatically a closed semiring and every continuous semiring morphism (semiring morphism preserving all suprema) is automatically ω-continuous (preserves all countable suprema), and these notions coincide on countable algebras.

In a subsequent lecture we will show some very strong relationships among these classes of algebras. We will eventually show that the R-algebras, Kleene algebras, star-continuous Kleene algebras (a.k.a. N-algebras), closed semirings, and S-algebras each contain the next in the list, and all inclusions are strict. Moreover, each star-continuous Kleene algebra extends in a canonical way to a closed semiring, and each closed semiring to an S-algebra, by a construction known as *ideal completion*.

Other Approaches

There are many other approaches besides these, which we will not consider in this course.

Many authors consider Kleene algebra as synonymous with relation algebra and are not opposed to adding other relational operators such as residuation and complementation. Relation algebras were first studied by Tarski and his students and colleagues [20, 15, 14, 6]; see also [12, 13, 18, 9]. Bloom and Ésik [4, 2, 3] study a related structure called *iteration theories*.

In [16, 17], Pratt gives two definitions of Kleene algebras in the context of dynamic algebra. In [16], Kleene algebras are defined to be the Kleenean component of separable dynamic algebras; in [17], this class is enlarged to contain all subalgebras of such algebras.

Generalizations of Kleene's and Parikh's Theorems have been given by Kuich [10] in ℓ-*complete semirings*, which are similar to S-algebras in all respects except that idempotence of $\sum$ is replaced by a weaker condition called ℓ-completeness.

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] Stephen L. Bloom and Zoltán Ésik. Floyd–Hoare logic in iteration theories. *J. Assoc. Comput. Mach.*, 38(4):887–934, October 1991.

[3] Stephen L. Bloom and Zoltán Ésik. Program correctness and matricial iteration theories. In *Proc. 7th Int. Conf. Mathematical Foundations of Programming Semantics*, volume 598 of *Lecture Notes in Computer Science*, pages 457–476. Springer-Verlag, 1992.

[4] Stephen L. Bloom and Zoltán Ésik. Equational axioms for regular sets. *Math. Struct. Comput. Sci.*, 3:1–24, 1993.

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

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

[7] 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.

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

[9] Dexter Kozen. On action algebras. In J. van Eijck and A. Visser, editors, *Logic and Information Flow*, pages 78–88. MIT Press, 1994.

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

[12] B. Möller. Calculating with pointer structures. In R. Bird and L. Meertens, editors, *Algorithmic Languages and Calculi. Proc. IFIP TC2/WG2.1 Working Conference*, pages 24–48. Chapman and Hall, February 1997.

[13] B. Möller. Safer ways to pointer manipulation. Technical Report 2000-4, Institut für Informatik, Universität Augsburg, 2000.

[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] V. R. Pratt. Dynamic algebras and the nature of induction. In *Proc. 12th Symp. Theory of Comput.*, pages 22–28. ACM, 1980.

[17] V. R. Pratt. Dynamic algebras as a well-behaved fragment of relation algebras. In D. Pigozzi, editor, *Proc. Conf. on Algebra and Computer Science*. Springer-Verlag, June 1988.

[18] Vaughan Pratt. Action logic and pure induction. In J. van Eijck, editor, *Proc. Logics in AI: European Workshop JELIA '90*, volume 478 of *Lecture Notes in Computer Science*, pages 97–120, New York, September 1990. Springer-Verlag.

[19] Robert E. Tarjan. A unified approach to path problems. *J. Assoc. Comput. Mach.*, pages 577–593, 1981.

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