Supplementary Lecture A

Kleene Algebra and Regular Expressions

In Lecture 9, we gave a combinatorial proof that every finite automaton has an equivalent regular expression. Here is an algebraic proof that generalizes that argument. It is worth looking at because it introduces the notion of *Kleene algebra* and the use of matrices. We will show how to use matrices and Kleene algebra to solve systems of linear equations involving sets of strings.

Kleene algebra is named after Stephen C. Kleene, who invented the regular sets [70].

Kleene Algebra

We have already observed in Lecture 9 that the set operations $\cup$, $\cdot$, and * on subsets of Σ^*, along with the distinguished subsets $\varnothing$ and $\{\epsilon\}$, satisfy certain important algebraic properties. These were listed in Lecture 9, axioms (9.1) through (9.13). Let us call any algebraic structure satisfying these properties a *Kleene algebra.* In general, a Kleene algebra $\mathcal{K}$ consists of a nonempty set with two distinguished constants 0 and 1, two binary operations $+$ and $\cdot$ (usually omitted in expressions), and a unary operation * satisfying the following axioms.

$$a + (b + c) = (a + b) + c \quad \text{associativity of } + \tag{A.1}$$

$$a + b = b + a \quad \text{commutativity of } + \tag{A.2}$$

D. C. Kozen, *Automata and Computability*

$$a + a = a \qquad \text{idempotence of } + \tag{A.3}$$

$$a + 0 = a \qquad 0 \text{ is an identity for } + \tag{A.4}$$

$$a(bc) = (ab)c \qquad \text{associativity of } \cdot \tag{A.5}$$

$$a1 = 1a = a \qquad 1 \text{ is an identity for } \cdot \tag{A.6}$$

$$a0 = 0a = 0 \qquad 0 \text{ is an annihilator for } \cdot \tag{A.7}$$

$$a(b + c) = ab + ac \qquad \text{distributivity} \tag{A.8}$$

$$(a + b)c = ac + bc \qquad \text{distributivity} \tag{A.9}$$

$$1 + aa^* = a^* \tag{A.10}$$

$$1 + a^*a = a^* \tag{A.11}$$

$$b + ac \leq c \Rightarrow a^*b \leq c \tag{A.12}$$

$$b + ca \leq c \Rightarrow ba^* \leq c \tag{A.13}$$

In (A.12) and (A.13), $\leq$ refers to the naturally defined order

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

In 2^{Σ^*}, $\leq$ is just set inclusion $\subseteq$.

Axioms (A.1) through (A.9) discuss the properties of addition and multiplication in a Kleene algebra. These properties are the same as those of ordinary addition and multiplication, with the addition of the idempotence axiom (A.3). These axioms can be summed up briefly by saying that $\mathcal{K}$ is an *idempotent semiring.* The remaining axioms (A.10) through (A.13) discuss the properties of the operator *. They say essentially that * behaves like the asterate operator on sets of strings or the reflexive transitive closure operator on binary relations.

It follows quite easily from the axioms that $\leq$ is a partial order; that is, it is reflexive ($a \leq a$), transitive ($a \leq b$ and $b \leq c$ imply $a \leq c$), and antisymmetric ($a \leq b$ and $b \leq a$ imply $a = b$). Moreover, $a + b$ is the least upper bound of a and b with respect to $\leq$. All the operators are monotone with respect to $\leq$; in other words, if $a \leq b$, then $ac \leq bc$, $ca \leq cb$, $a + c \leq b + c$, and $a^* \leq b^*$.

By (A.10) and distributivity, we have

$$b + aa^*b \leq a^*b,$$

which says that a^*b satisfies the inequality $b + ac \leq c$ when substituted for c. The implication (A.12) says that a^*b is the $\leq$-least element of $\mathcal{K}$ for which this is true. It follows that

Lemma A.1 *In any Kleene algebra, a^*b is the $\leq$-least solution of the equation $x = ax+b$.*

Proof. Miscellaneous Exercise 21. □

Instead of (A.12) and (A.13), we might take the equivalent axioms

$$ac \leq c \Rightarrow a^*c \leq c, \tag{A.14}$$

$$ca \leq c \Rightarrow ca^* \leq c \tag{A.15}$$

(see Miscellaneous Exercise 22).

Here are some typical theorems of Kleene algebra. These can be derived by purely equational reasoning from the axioms above (Miscellaneous Exercise 20).

$$a^*a^* = a^*$$

$$a^{**} = a^*$$

$$(a^*b)^*a^* = (a+b)^* \qquad \text{denesting rule} \tag{A.16}$$

$$a(ba)^* = (ab)^*a \qquad \text{shifting rule} \tag{A.17}$$

$$a^* = (aa)^* + a(aa)^*$$

Equations (A.16) and (A.17), the *denesting rule* and the *shifting rule*, respectively, turn out to be particularly useful in simplifying regular expressions.

The family 2^{Σ^*} of all subsets of Σ^* with constants $\varnothing$ and $\{\epsilon\}$ and operations $\cup, \cdot$, and * forms a Kleene algebra, as does the family of all regular subsets of Σ^* with the same operations. As mentioned in Lecture 9, it can be shown that an equation $\alpha = \beta$ is a theorem of Kleene algebra, that is, is derivable from axioms (A.1) through (A.13), if and only if α and β are equivalent as regular expressions [73].

Another example of a Kleene algebra is the family of all binary relations on a set X with the empty relation for 0, the identity relation

$$\iota \stackrel{\text{def}}{=} \{(u,u) \mid u \in X\}$$

for 1, $\cup$ for $+$, relational composition

$$R \circ S \stackrel{\text{def}}{=} \{(u,w) \mid \exists v \in X \ (u,v) \in R \text{ and } (v,w) \in S\}$$

for $\cdot$, and reflexive transitive closure for *:

$$R^* \stackrel{\text{def}}{=} \bigcup_{n \geq 0} R^n,$$

where

$$R^0 \stackrel{\text{def}}{=} \iota,$$

$$R^{n+1} \stackrel{\text{def}}{=} R^n \circ R.$$

Still another example is the family of $n \times n$ Boolean matrices with the zero matrix for 0, the identity matrix for 1, componentwise Boolean matrix addition and multiplication for + and ·, respectively, and reflexive transitive closure for *. This is really the same as the previous example, where the set X has n elements.

Matrices

Given an arbitrary Kleene algebra $\mathcal{K}$, the set of $n \times n$ matrices over $\mathcal{K}$, which we will denote by $\mathcal{M}(n, \mathcal{K})$, also forms a Kleene algebra. In $\mathcal{M}(2, \mathcal{K})$, for example, the identity elements for + and · are

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

respectively, and the operations +, ·, and * are given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \overset{\text{def}}{=} \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix},$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} \overset{\text{def}}{=} \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}, \quad \text{and}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* \overset{\text{def}}{=} \begin{bmatrix} (a+bd^*c)^* & (a+bd^*c)^*bd^* \\ (d+ca^*b)^*ca^* & (d+ca^*b)^* \end{bmatrix}, \tag{A.18}$$

respectively. In general, + and · in $\mathcal{M}(n, \mathcal{K})$ are ordinary matrix addition and multiplication, respectively, the identity for + is the zero matrix, and the identity for · is the identity matrix.

To define E^* for a given $n \times n$ matrix E over $\mathcal{K}$, we proceed by induction on n. If $n = 1$, the structure $\mathcal{M}(n, \mathcal{K})$ is just $\mathcal{K}$, so we are done. For $n > 1$, break E up into four submatrices

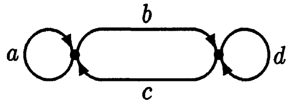
$$E = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$$

such that A and D are square, say $m \times m$ and $(n-m) \times (n-m)$, respectively. By the induction hypothesis, $\mathcal{M}(m, \mathcal{K})$ and $\mathcal{M}(n-m, \mathcal{K})$ are Kleene algebras, so it makes sense to form the asterates of any $m \times m$ or $(n-m) \times (n-m)$ matrix over $\mathcal{K}$, and these matrices will satisfy all the axioms for *. This allows us to define

$$E^* \overset{\text{def}}{=} \left[\begin{array}{c|c} (A+BD^*C)^* & (A+BD^*C)^*BD^* \\ \hline (D+CA^*B)^*CA^* & (D+CA^*B)^* \end{array}\right]. \tag{A.19}$$

Compare this definition to (A.18).

The expressions on the right-hand sides of (A.18) and (A.19) may look like they were pulled out of thin air. Where did we get them from? The answer will come to you if you stare really hard at the following mandala:



It can be shown that $\mathcal{M}(n, \mathcal{K})$ is a Kleene algebra under these definitions:

Lemma A.2 *If $\mathcal{K}$ is a Kleene algebra, then so is $\mathcal{M}(n, \mathcal{K})$.*

Proof. Miscellaneous Exercise 24. We must verify that $\mathcal{M}(n, \mathcal{K})$ satisfies the axioms (A.1) through (A.13) of Kleene algebra assuming only that $\mathcal{K}$ does. □

If E is a matrix of indeterminates, and if the inductive construction of E^* given in (A.19) is carried out ***symbolically***, then the entries of the resulting matrix E^* will be regular expressions in those indeterminates. This construction generalizes the construction of Lecture 9, which corresponds to the case $m = 1$.

Systems of Linear Equations

It is possible to solve systems of linear equations over a Kleene algebra $\mathcal{K}$. Suppose we are given a set of n variables $x_1, \ldots, x_n$ ranging over $\mathcal{K}$ and a system of n equations of the form

$$x_i = a_{i1}x_1 + \cdots + a_{in}x_n + b_i, \quad 1 \leq i \leq n,$$

where the a_{ij} and b_i are elements of $\mathcal{K}$. Arranging the a_{ij} in an $n \times n$ matrix A, the b_i in a vector b of length n, and the x_i in a vector x of length n, we obtain the matrix-vector equation

$$x = Ax + b. \tag{A.20}$$

It is now not hard to show

Theorem A.3 *The vector A^*b is a solution to (A.20); moreover, it is the $\leq$-least solution in $\mathcal{K}^n$.*

Proof. Miscellaneous Exercise 25. □

Now we use this to give a regular expression equivalent to an arbitrarily given deterministic finite automaton

$$M = (Q,\ \Sigma,\ \delta,\ s,\ F).$$

Assume without loss of generality that $Q = \{1, 2, \ldots, n\}$. For each $q \in Q$, let X_q denote the set of strings in Σ^* that would be accepted by M if q were the start state; that is,

$$X_q \overset{\text{def}}{=} \{x \in \Sigma^* \mid \widehat{\delta}(q, x) \in F\}.$$

The X_q satisfy the following system of equations:

$$X_q = \begin{cases} \sum_{a \in \Sigma} aX_{\delta(q,a)} & \text{if } q \notin F, \\ \sum_{a \in \Sigma} aX_{\delta(q,a)} + 1 & \text{if } q \in F. \end{cases}$$

Moreover, the X_q give the least solution with respect to $\subseteq$. As above, these equations can be arranged in a single matrix-vector equation of the form

$$X = AX + b, \tag{A.21}$$

where A is an $n \times n$ matrix containing sums of elements of Σ, b is a 0-1 vector of length n, and X is a vector consisting of $X_1, \ldots, X_n$. The vector X is the least solution of (A.21). By Theorem A.3,

$$X = A^*b.$$

Compute the matrix A^* symbolically according to (A.19), so that its entries are regular expressions, then multiply by b. A regular expression for $L(M)$ can then be read off from the sth entry of A^*b, where s is the start state of M.

Historical Notes

Salomaa [108] gave the first complete axiomatization of the algebra of regular sets. The algebraic theory was developed extensively in the monograph of Conway [27]. Many others have contributed to the theory, including Redko [103], Backhouse [6], Bloom and Ésik [10], Boffa [11, 12], Gécseg and Peák [41], Krob [74], Kuich and Salomaa [76], and Salomaa and Soittola [109]. The definition of Kleene algebra and the complete axiomatization given here is from Kozen [73].