Introduction to Kleene Algebra	**Lecture 7**
CS786 Spring 2002	**Thursday, February 14, 2002**

We now turn to the equational theory of Kleene algebra. This and the next lecture will be devoted to proving that equational theory of Kleene algebra is the same as the equational theory of the regular sets under the standard interpretation. In other words, an equation $s = t$ over Σ is an element of the kernel of the standard interpretation R_Σ over Reg_Σ iff $s = t$ is a consequence of the axioms of Kleene algebra.

The equational theory of the regular sets, or *regular events* as they are sometimes called, was first studied by Kleene [6], who posed axiomatization as an open problem. Salomaa [15] gave two complete axiomatizations of the algebra of regular events in 1966. Salomaa's axiomatization is not a universal Horn axiomatization, since it depends on rules whose validity is not preserved under substitution, thus are not sound under nonstandard interpretations. Redko [13] proved in 1964 that no finite set of equational axioms could characterize the algebra of regular events. The algebra of regular events and its axiomatization is the subject of the extensive monograph of Conway [4]; as we have seen, the bulk of Conway's treatment is infinitary.

In Lecture **??**, we gave a complete infinitary equational deductive system for the algebra of regular events that is sound over all star-continuous Kleene algebras [7]. A completeness theorem for relational algebras with *, a proper subclass of Kleene algebras, was given by Ng and Tarski [12, 11], but their axiomatization relies on the presence of a converse operator. Schematic equational axiomatizations for the algebra of regular events, necessarily representing infinitely many equations, have been given by Krob [9] and Bloom and Ésik [3].

Salomaa's Axiomatizations

Salomaa [15] was the first to axiomatize the equational theory of the regular events. Here is a brief account of his axiomatization.

Recall that R_Σ denotes the interpretation of regular expressions over Σ in the Kleene algebra Reg_Σ in which $R_\Sigma(a) = \{a\}$, $a \in \Sigma$. This is called the *standard interpretation*.

Salomaa [15] presented two axiomatizations F_1 and F_2 for the algebra of regular events and proved their completeness. Aanderaa [1] independently presented a system similar to Salomaa's F_1. Backhouse [2] gave an algebraic version of F_1. These systems are equational except for one rule of inference in each case that is sound under the standard interpretation R_Σ, but not sound in general over other interpretations.

Salomaa defined a regular expression to have the *empty word property* (EWP) if the regular set it denotes under R_Σ contains the null string ϵ. He also observed that the EWP can be characterized syntactically: a regular expression s has the EWP if either

- $s = 1$;
- $s = t^*$ for some t;
- s is a sum of regular expressions, at least one of which has the EWP; or
- s is a product of regular expressions, both of which have the EWP.

A simpler way to say this is that a regular expression has the EWP iff $\varepsilon(s) = 1$, where ε denotes the unique homomorphism $\varepsilon : \mathsf{RExp}_\Sigma \to \{0, 1\}$ such that $\varepsilon(a) = 0$, $a \in \Sigma$.

Salomaa's system F_1 contains the rule

$$\frac{u + st = t, \quad s \text{ does not have the EWP}}{s^* u = t}. \tag{1}$$

The rule (1) is sound under the standard interpretation R_Σ, but the proviso "s does not have the EWP" is not algebraic in the sense that it is not preserved under substitititution. Consequently, (1) is not valid under nonstandard interpretations. For example, if s, t, and u are the single letters a, b and c respectively, then (1) holds; but it does not hold after the substitution

$$a \mapsto 1 \qquad b \mapsto 1 \qquad c \mapsto 0.$$

Another way to say this is that (1) must not be interpreted as a universal Horn formula. Salomaa's system F_2 is somewhat different from F_1 but contains a similar nonalgebraic proviso.

In contrast, the axioms for Kleene algebra are all equations or equational implications in which the symbols are regarded as universally quantified, so substitution is allowed.

Equational Logic

By general considerations of equational logic, the axioms of Kleene algebra, along with the usual axioms for equality, instantiation, and rules for the introduction and elimination of implications, constitute a complete deductive system for the universal Horn theory of Kleene algebras (the set of universally quantified equational implications

$$s_1 = t_1 \wedge \cdots \wedge s_n = t_n \quad \to \quad s = t \tag{2}$$

true in all Kleene algebras) [16, 17].

More specifically, let Δ be a set of implicitly universally quantified Horn formulas over some signature and variables X (in our application, Δ is the set of axioms of Kleene algebra). Let $d, e, \ldots$ denote equations, A a sequence of equations, σ a substitution of terms for variables, and φ Horn formula. The equational axioms are

$$
\begin{aligned}
&x = x \\
&x = y \to y = x \\
&x = y \to y = z \to x = z \\
&x_1 = y_1 \to \ldots \to x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n),
\end{aligned}
$$

where in the last, f is an n-ary function symbol of the signature. These are considered to be implicitly universally quantified. This set of Horn formulas is denoted E. The rules of inference are:

$$
\vdash \sigma(\varphi), \quad \varphi \in \Delta \cup E \qquad\qquad e \vdash e
$$

$$
\frac{A \vdash \varphi}{A, e \vdash \varphi} \qquad\qquad \frac{A, e \vdash \varphi}{A \vdash e \to \varphi}
$$

$$
\frac{A \vdash e \quad A \vdash e \to \varphi}{A \vdash \varphi}
$$

and structural rules for permuting A.

Encoding Combinatorial Arguments

To show completeness, we will show how to encode several classical combinatorial constructions of the theory of finite automata algebraically. The first step will be to construct a transition matrix representing a finite automaton equivalent to a given regular expression. This construction is essentially implicit in the work of Kleene [6] and appears in Conway's monograph [4]. The algebraic approach to the elimination of ϵ-transitions appears in the work of Kuich and Salomaa [10] and Sakarovitch [14]. The results on the closure of Kleene algebras under the formation of matrices essentially go back to Conway's monograph [4] and the thesis of Backhouse [2]. It was shown in [8] how to encode algebraically two other fundamental constructions in the theory of finite automata:

- determinization of an automaton via the subset construction, and
- state minimization via equivalence modulo a Myhill-Nerode equivalence relation.

We then use the uniqueness of the minimal deterministic finite automaton to obtain completeness.

We recall some elementary consequences of the axioms of Kleene algebra proved in Exercise **??** of Homework **??**.

$$
\begin{aligned}
xy = xz &\;\to\; x^*y = yz^* \\
(xy)^*x &\;=\; x(yx)^* \\
(x+y)^* &\;=\; x^*(yx^*)^*.
\end{aligned}
$$

These are called the *bisimulation rule*, the *sliding rule*, and the *denesting rule*, respectively.

Matrices over a Kleene Algebra

Under the natural definitions of the Kleene algebra operators $+$, $\cdot$, *, 0, and 1, the family $\mathrm{Mat}(n, K)$ of $n \times n$ matrices over a Kleene algebra K again forms a Kleene algebra. This is a standard result that holds for various classes of Kleene algebra-like structures [4, 2]. The proof for Kleene algebras in our sense appeared first in [8].

Define $+$ and $\cdot$ on $\mathrm{Mat}(n, K)$ to be the usual operations of matrix addition and multiplication, respectively, Z_n the $n \times n$ zero matrix, and I_n the $n \times n$ identity matrix. The partial order $\leq$ is defined on $\mathrm{Mat}(n, K)$ by

$$A \leq B \quad \overset{\text{def}}{\Longleftrightarrow} \quad A + B = B.$$

Under these definitions, it is routine to verify that the structure

$$(\mathrm{Mat}(n, K),\ +,\ \cdot,\ Z_n,\ I_n)$$

is an idempotent semiring.

The definition of E^* for $E \in \mathrm{Mat}(n, K)$ comes from [4, 10, 5]. We first consider the case $n = 2$. This construction will later be applied inductively.

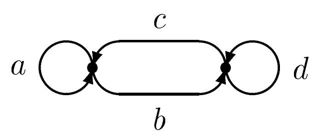
If

$$E \quad = \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

define

$$E^* \quad \overset{\text{def}}{=} \quad \begin{bmatrix} (a + bd^*c)^* & (a + bd^*c)^*bd^* \\ (d + ca^*b)^*ca^* & (d + ca^*b)^* \end{bmatrix}. \tag{3}$$

To understand where this definition comes from, consider a two-state finite automaton over the alphabet $\Sigma = \{a, b, c, d\}$ and transitions as defined in the following diagram.



The matrix E is the transition matrix of this automaton. For each i, j, the ij^{th} entry of E^* is a regular expression describing the set of strings over the alphabet Σ going from state i to state j.

Lemma 0.1 *The matrix E^* defined in* (3) *satisfies the Kleene algebra axioms for* *. *That is,*

$$\begin{aligned} I + EE^* &\leq E^* \qquad (4)\\ I + E^*E &\leq E^* \qquad (5)\end{aligned}$$

and for any X,

$$\begin{aligned} EX \leq X &\rightarrow E^*X \leq X \qquad (6)\\ XE \leq X &\rightarrow XE^* \leq X. \qquad (7)\end{aligned}$$

Proof. We show (4) and (6). The arguments for (5) and (7) are symmetric.

The matrix inequality (4) reduces to the four inequalities

$$\begin{aligned} 1 + a(a+bd^*c)^* + b(d+ca^*b)^*ca^* &\leq (a+bd^*c)^*\\ a(a+bd^*c)^*bd^* + b(d+ca^*b)^* &\leq (a+bd^*c)^*bd^*\\ c(a+bd^*c)^* + d(d+ca^*b)^*ca^* &\leq (d+ca^*b)^*ca^*\\ 1 + c(a+bd^*c)^*bd^* + d(d+ca^*b)^* &\leq (d+ca^*b)^*\end{aligned}$$

in K. These simplify to

$$\begin{aligned} 1 &\leq (a+bd^*c)^*\\ a(a+bd^*c)^* &\leq (a+bd^*c)^*\\ b(d+ca^*b)^*ca^* &\leq (a+bd^*c)^* \qquad (8)\end{aligned}$$

$$\begin{aligned} a(a+bd^*c)^*bd^* &\leq (a+bd^*c)^*bd^*\\ b(d+ca^*b)^* &\leq (a+bd^*c)^*bd^* \qquad (9)\end{aligned}$$

$$\begin{aligned} c(a+bd^*c)^* &\leq (d+ca^*b)^*ca^* \qquad (10)\\ d(d+ca^*b)^*ca^* &\leq (d+ca^*b)^*ca^*\end{aligned}$$

$$\begin{aligned} 1 &\leq (d+ca^*b)^*\\ c(a+bd^*c)^*bd^* &\leq (d+ca^*b)^* \qquad (11)\\ d(d+ca^*b)^* &\leq (d+ca^*b)^*,\end{aligned}$$

of which all but the labeled inequalities (8)–(11) are trivial. By symmetry, it suffices to show only (8) and (9). Using the denesting rule, we can rewrite these as

$$\begin{aligned} b(d^*ca^*b)^*d^*ca^* &\leq (a^*bd^*c)^*a^*\\ b(d^*ca^*b)^*d^* &\leq (a^*bd^*c)^*a^*bd^*,\end{aligned}$$

and by the sliding rule,

$$\begin{aligned} bd^*ca^*(bd^*ca^*)^* &\leq a^*(bd^*ca^*)^* \\ bd^*(ca^*bd^*)^* &\leq a^*bd^*(ca^*bd^*)^*, \end{aligned}$$

which follow directly from the axioms.

We now establish (6). We show that (6) holds for X an arbitrary column vector of length 2; then (6) for X any $2 \times n$ matrix follows by applying this result to the columns of X separately. Let

$$X = \begin{bmatrix} x \\ y \end{bmatrix}.$$

We need to show that under the assumptions

$$ax + by \leq x \tag{12}$$
$$cx + dy \leq y \tag{13}$$

we can derive

$$(a + bd^*c)^*x + (a + bd^*c)^*bd^*y \leq x \tag{14}$$
$$(d + ca^*b)^*ca^*x + (d + ca^*b)^*y \leq y. \tag{15}$$

By symmetry, it suffices to show just (14). Simplifying (14), it suffices to show

$$(a + bd^*c)^*x \leq x \tag{16}$$
$$(a + bd^*c)^*bd^*y \leq x. \tag{17}$$

For both (16) and (17), it suffices to show

$$bd^*y + (a + bd^*c)x \leq x,$$

and for this it suffices to show $ax \leq x$, $bd^*cx \leq x$, and $bd^*y \leq x$. The first is immediate from the assumption (12). The second is immediate from the last and (13). For the last, we have $d^*y \leq y$ by (13) and an axiom of Kleene algebra, and then $bd^*y \leq by \leq x$ by (12) and monotonicity. □

To extend to matrices of arbitrary dimension, we recall the following fact established in Lecture **??**:

Lemma 0.2 *In any Kleene algebra, a^*b is the unique least solution of the inequality $b+ax \leq x$, and ba^* is the unique least solution of $b + xa \leq x$.*

Lemma 0.3 *Let $E \in \mathrm{Mat}(n, K)$. There is a unique matrix $E^* \in \mathrm{Mat}(n, K)$ satisfying the Kleene algebra axioms* (4)–(7).

Proof. Partition E into submatrices A, B, C, and D such that A and D are square.

$$E = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \tag{18}$$

By the induction hypothesis, D^* exists and is unique. Let $F = A + BD^*C$. Again by the induction hypothesis, F^* exists and is unique. We define

$$E^* = \left[\begin{array}{c|c} F^* & F^*BD^* \\ \hline D^*CF^* & D^* + D^*CF^*BD^* \end{array}\right] \tag{19}$$

and claim that E^* satisfies (4)–(7). The proof is essentially identical to the proof of Lemma 0.1. We must check that the axioms and basic properties of Kleene algebra used in the proof of Lemma 0.1 still hold when the primitive symbols of regular espressions are interpreted as matrices of various dimensions, provided there is no type mismatch in the application of the operators.

The uniqueness of E^* follows from Lemma 0.2. $\square$

It follows from 0.3 that

Theorem 0.4 *The structure*

$$(\mathrm{Mat}(n, K),\ +,\ \cdot,\ ^*,\ Z_n,\ I_n)$$

is a Kleene algebra.

The inductive definition (19) of E^* in Lemma 0.3 is independent of the partition of E chosen in (18). This is a consequence of Lemma 0.2, once we have established that the resulting structure is a Kleene algebra under *some* partition; cf. [4, Theorem 4, p. 27], which establishes the same result for S-algebras.

In the proof of Lemma 0.3, we needed to know that the axioms of Kleene algebra still hold when the primitive letters of regular expressions are interpreted as matrices of various shapes, possibly nonsquare, provided there is no type mismatch in the application of operators. For example, one cannot add two matrices unless they are the same shape, one cannot form the matrix product AB unless the column dimension of A is the same as the row dimension of B, and one cannot form the matrix A^* unless A is square. In general, all the axioms and basic properties of Kleene algebra still hold when the primitive letters are interpreted as possibly nonsquare matrices over a Kleene algebra, provided that there are no type conflicts in the application of the Kleene algebra operators.

For example, consider the distributive law

$$a(b+c) \quad = \quad ab+ac.$$

Interpreting a, b, and c as matrices over a Kleene algebra K, this equation makes sense provided the shapes of b and c are the same and the column dimension of a is the same as the row dimension of b and c. Other than that, there are no type constraints. It is easy to verify that the distributive law holds for any matrices a, b and c satisfying these constraints.

For a more involved example, consider the equational implication

$$ax = xb \quad \to \quad a^*x = xb^*.$$

The type constraints say that a and b must be square (say $s \times s$ and $t \times t$ respectively) and that x must be $s \times t$. Under this typing, all steps of the proof of this implication involve only well-typed expressions, thus the proof remains valid.

References

[1] S. Anderaa. On the algebra of regular expressions. Appl. Math., Harvard Univ., 1965. Cambridge, Mass., 1–18.

[2] Roland Carl Backhouse. *Closure Algorithms and the Star-Height Problem of Regular Languages*. PhD thesis, Imperial College, London, U.K., 1975.

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

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

[5] S. Eilenberg. *Automata, Languages, and Machines*, volume A. Academic Press, New York, 1974.

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

[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] Daniel Krob. A complete system of B-rational identities. *Theoretical Computer Science*, 89(2):207–343, October 1991.

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

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

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

[13] V. N. Redko. On defining relations for the algebra of regular events. *Ukrain. Mat. Z.*, 16:120–126, 1964. In Russian.

[14] Jacques Sakarovitch. Kleene's theorem revisited: A formal path from Kleene to Chomsky. In A. Kelemenova and J. Keleman, editors, *Trends, Techniques, and Problems in Theoretical Computer Science*, volume 281 of *Lecture Notes in Computer Science*, pages 39–50, New York, 1987. Springer-Verlag.

[15] Arto Salomaa. Two complete axiom systems for the algebra of regular events. *J. Assoc. Comput. Mach.*, 13(1):158–169, January 1966.

[16] A. Selman. Completeness of calculi for axiomatically defined classes of algebras. *Algebra Universalis*, 2:20–32, 1972.

[17] Walter Taylor. Equational logic. *Houston J. Math.*, pages i–83, 1979. Survey.