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 $\mathsf{Reg}\,\Sigma$ 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 [9], who posed axiomatization as an open problem. Salomaa [20] 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 [18] 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 [5]; as we have seen, the bulk of Conway's treatment is infinitary.

In a previous lecture, we gave a complete infinitary equational deductive system for the algebra of regular events that is sound over all star-continuous Kleene algebras [10]. A completeness theorem for relational algebras with *, a proper subclass of Kleene algebras, was given by Ng and Tarski [16, 17]. 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 [13] and Bloom and Ésik [4].

Salomaa's Axiomatizations

Salomaa [20] was the first to axiomatize the equational theory of the regular sets. Here is a brief account of his axiomatization.

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

Salomaa [20] presented two axiomatizations F_1 and F_2 for the equational theory of the regular sets 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.

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

Salomaa's system F_1 contains the rule

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

where s, t, and u are regular expressions. The rule (1) is sound under the standard interpretation R_Σ, but not under nonstandard interpretations. The problem is that the side-condition "s does not have the EWP" is not preserved under substitutition. For example, if s, t, and u are single letters, then (1) holds; but it does not hold after the substitution

$$s \mapsto 1 \qquad\qquad t \mapsto 1 \qquad\qquad u \mapsto 0,$$

as $0 + 1 \cdot 1 = 1$ but $1^* \cdot 0 \neq 1$. Thus (1) must not be interpreted as a universal Horn formula

$$u + st = t \Rightarrow s^* u = t.$$

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

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

true in all Kleene algebras) [22, 23].

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

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

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:

$$\vdash \sigma(\varphi),\ \ \varphi \in \Delta \cup E \qquad e \vdash e \qquad \frac{A \vdash \varphi}{A, e \vdash \varphi} \qquad \frac{A, e \vdash \varphi}{A \vdash e \Rightarrow \varphi} \qquad \frac{A \vdash e \qquad A \vdash e \Rightarrow \varphi}{A \vdash \varphi}$$

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 [9] and appears in Conway's monograph [5]. The algebraic approach to the elimination of ε-transitions appears in the work of Kuich and Salomaa [14] and Sakarovitch [19]. The results on the closure of Kleene algebras under the formation of matrices essentially go back to Conway's monograph [5] and the thesis of Backhouse [2]. It was shown in [11] 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 Homework 2.

$$xy = yz \Rightarrow x^*y = yz^* \tag{3}$$

$$(xy)^*x = x(yx)^* \tag{4}$$

$$(x+y)^* = x^*(yx^*)^*. \tag{5}$$

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 $K^{n\times n}$ 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 [2,5]. The proof for Kleene algebras in our sense is from [11].

Define $+$ and $\cdot$ on $K^{n\times n}$ 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. For example, for $n = 2$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \qquad Z_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \qquad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Be careful: multiplication is not commutative in general, so the order of the letters is important.

The partial order $\le$ is defined on $K^{n\times n}$ by

$$A \le B \overset{\text{def}}{\Leftrightarrow} A + B = B.$$

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

$$(K^{n\times n}, +, \cdot, Z_n, I_n)$$

is an idempotent semiring.

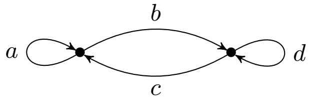
The definition of E^* for $E \in K^{n\times n}$ comes from [5,6,14]. We first consider the case $n = 2$. This construction will later be applied inductively. If

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

define

$$E^* \overset{\text{def}}{=} \begin{bmatrix} (a+bd^*c)^* & (a+bd^*c)^*bd^* \\ (d+ca^*b)^*ca^* & (d+ca^*b)^* \end{bmatrix}. \tag{6}$$

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 pair of states s, t, the st^{th} entry of E^* is a regular expression describing the set of strings over the alphabet Σ going from state s to state t.

Lemma 1. *The matrix E^* defined in (6) satisfies the Kleene algebra axioms for *. That is, for any X,*

$$I + EE^* \le E^* \qquad\qquad EX \le X \Rightarrow E^*X \le X \tag{7}$$

$$I + E^*E \le E^* \qquad\qquad XE \le X \Rightarrow XE^* \le X. \tag{8}$$

Proof. We prove the left-handed star rules (7). The arguments for the right-hand rules (8) are symmetric.

The matrix inequality on the left-hand side of (7) reduces to the four inequalities

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

in K. These simplify to

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

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

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

$$\begin{aligned}
1 &\le (d+ca^*b)^* \\
c(a+bd^*c)^*bd^* &\le (d+ca^*b)^* \qquad (12) \\
d(d+ca^*b)^* &\le (d+ca^*b)^*,
\end{aligned}$$

of which all but the labeled inequalities (9)–(12) are trivial. By symmetry, it suffices to show only (9) and (10). Using the denesting rule, we can rewrite these as

$$b(d^*ca^*b)^*d^*ca^* \le (a^*bd^*c)^*a^* \qquad\qquad b(d^*ca^*b)^*d^* \le (a^*bd^*c)^*a^*bd^*,$$

and by the sliding rule,

$$bd^*ca^*(bd^*ca^*)^* \le a^*(bd^*ca^*)^* \qquad\qquad bd^*(ca^*bd^*)^* \le a^*bd^*(ca^*bd^*)^*,$$

which follow directly from the axioms.

We now establish the implication on the right-hand side of (7). We show that this implication holds for an arbitrary column vector X of length 2; then it will also hold for any $2 \times n$ matrix X by applying this result to the columns of X separately. Let

$$X = \left[\begin{array}{c} x \\ y \end{array}\right].$$

We need to show that under the assumptions

$$ax + by \le x \tag{13}$$

$$cx + dy \le y \tag{14}$$

we can derive

$$(a+bd^*c)^*x+(a+bd^*c)^*bd^*y \le x \tag{15}$$

$$(d+ca^*b)^*ca^*x+(d+ca^*b)^*y \le y. \tag{16}$$

Note that (15) and (16) are the same inequality under the exchange $a \leftrightarrow d$, $b \leftrightarrow c$, $x \leftrightarrow y$, so by symmetry it suffices to show just (15). Simplifying, it suffices to show

$$(a+bd^*c)^*x \le x \tag{17}$$

$$(a+bd^*c)^*bd^*y \le x. \tag{18}$$

For both (17) and (18), it suffices to show

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

and for this it suffices to show (i) $ax \le x$, (ii) $bd^*cx \le x$, and (iii) $bd^*y \le x$. Now (i) is immediate from the assumption (13), and (ii) is immediate from (iii) and (14). For (iii), we have $d^*y \le y$ by (14) and an axiom of Kleene algebra, and then $bd^*y \le by \le x$ by (13) and monotonicity. □

To extend to matrices of arbitrary dimension, we recall the following fact established in a previous lecture:

Lemma 2. *In any Kleene algebra, a^*b is the unique least solution of the inequality $b+ax \le x$, and ba^* is the unique least solution of $b+xa \le x$.*

Lemma 3. *Let $E \in K^{n\times n}$. There is a unique matrix $E^* \in K^{n\times n}$ satisfying the Kleene algebra axioms (7).*

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

$$E = \left[\begin{array}{cc} A & B \\ C & D \end{array}\right] \tag{19}$$

By the induction hypothesis, A^* and D^* exist and are unique. Again by the induction hypothesis, $A+BD^*C$ and $D+CA^*B$ exist and are unique (one must also check that these matrices are square–note that B and C are not necessarily square). We define

$$E^* \overset{\text{def}}{=} \left[\begin{array}{cc} (A+BD^*C)^* & (A+BD^*C)^*BD^* \\ (D+CA^*B)^*CA^* & (D+CA^*B)^* \end{array}\right] \tag{20}$$

and claim that E^* satisfies (7). The proof is essentially identical to the proof of Lemma 1. We must check that the axioms and basic properties of Kleene algebra used in the proof of Lemma 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 2. □

It follows from Lemma 3 that

Theorem 4. *The structure $(K^{n\times n}, +, \cdot, ^*, Z_n, I_n)$ is a Kleene algebra.*

The inductive definition (20) of E^* in Lemma 3 is independent of the partition of E chosen in (19). This is a consequence of Lemma 2, once we have established that the resulting structure is a Kleene algebra under *some* partition; cf. [5, Theorem 4, p. 27], which establishes the same result for S-algebras.

In the proof of Lemma 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

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

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

$$ax = xb \Rightarrow a^*x = xb^*.$$

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.

Finite Automata

Regular expressions and finite automata have traditionally been used as syntactic representations of the regular languages over an alphabet Σ. The equivalence of these two formalisms was first established in Kleene's original paper [9]. Subsequent work has developed the relationship further, from both combinatorial [8,12,15] and algebraic [3,6,7,19,21] perspectives.

One can define the notion of an automaton over an arbitrary Kleene algebra. In subsequent sections, we will use this formalism to derive the classical results of the theory of finite automata (equivalence with regular expressions, determinization via the subset construction, elimination of ε-transitions, and state minimization) as consequences of the axioms of Kleene algebra.

Although we consider regular expressions and automata as syntactic objects, as a matter of convenience we will be reasoning modulo the axioms of Kleene algebra. Officially, regular expressions will denote elements of $\mathcal{F}_\Sigma$, the free Kleene algebra over Σ. The Kleene algebra $\mathcal{F}_\Sigma$ is constructed by taking the quotient of the regular expressions modulo the congruence generated by the axioms of Kleene algebra. The associated canonical map assigns to each regular expression its equivalence class in $\mathcal{F}_\Sigma$. Since we will be interpreting expressions only over Kleene algebras, and all interpretations factor through $\mathcal{F}_\Sigma$ via the canonical map, this usage is without loss of generality.

We recall the following basic theorems of Kleene algebra that were proved in Homework 2, of which we will make extensive use:

$$xy = yz \Rightarrow x^*y = yz^* \tag{21}$$

$$(xy)^*x = x(yx)^* \tag{22}$$

$$(x+y)^* = x^*(yx^*)^*. \tag{23}$$

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

Definition 5. *Let K be an arbitrary Kleene algebra. A* finite automaton *over K is a triple $\mathcal{A} = (u, A, v)$, where $u, v \in \{0,1\}^n$ and $A \in K^{n\times n}$ for some n.*

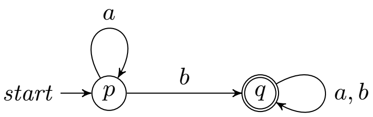
The states *are the row and column indices. The vector u determines the* start states *and the vector v determines the* accept states*; a* start state *is an index i for which $u(i) = 1$ and a* final state *is one for which $v(i) = 1$. The $n \times n$ matrix A is called the* transition matrix.

The language accepted by $\mathcal{A}$ *is the element $u^T A^* v \in K$.*

For automata over $\mathcal{F}_\Sigma$, the free Kleene algebra on free generators Σ, this definition is essentially equivalent to the classical combinatorial definition of an automaton over the alphabet Σ as found in [8, 15]. A similar definition can be found in [5].

Example 6. *Consider the two-state automaton in the sense of [8, 15] with states $\{p, q\}$, start state p, final state q, and transitions*

$$p \xrightarrow{a} p \qquad q \xrightarrow{a} q \qquad p \xrightarrow{b} q \qquad q \xrightarrow{b} q.$$



Classically, this automaton accepts the set of strings over $\Sigma = \{a, b\}$ containing at least one occurrence of b. In our formalism, this automaton is specified by the triple

$$\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} a & b \\ 0 & a+b \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right).$$

Modulo the axioms of Kleene algebra, we have

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & a+b \end{bmatrix}^* \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a^* & a^*b(a+b)^* \\ 0 & (a+b)^* \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a^*b(a+b)^*. \tag{24}$$

The language in $\mathsf{Reg}\,\Sigma$ accepted by this automaton is the image under R_Σ of the expression (24).

Definition 7. *Let $\mathcal{A} = (u, A, v)$ be an automaton over $\mathcal{F}_\Sigma$, the free Kleene algebra on free generators Σ. The automaton $\mathcal{A}$ is said to be* simple *if A can be expressed as a sum*

$$A = J + \sum_{a\in\Sigma} a \cdot A_a \tag{25}$$

where J and the A_a are 0-1 matrices. In addition, $\mathcal{A}$ is said to be ε-free *if J is the zero matrix. Finally, $\mathcal{A}$ is said to be* deterministic *if it is simple and ε-free, and u and all rows of A_a have exactly one 1.*

In Definition 7, ε refers to the null string. The matrix A_a in (25) corresponds to the adjacency matrix of the graph consisting of edges labeled a in the combinatorial model of automata [8, 15] or the image of a under a linear representation map in the algebraic approach of [3, 21]. An automaton is deterministic according to this definition iff it is deterministic in the sense of [8, 15].

The automaton of Example 6 is simple, ε-free, and deterministic.

We are moving toward a proof of the completeness of the axioms of Kleene algebra for the algebra of regular events. Another way of stating this is that $\mathsf{Reg}\,\Sigma$ is isomorphic to $\mathcal{F}_\Sigma$, the free Kleene algebra on free generators Σ, and the standard interpretation $R_\Sigma : \mathcal{F}_\Sigma \to \mathsf{Reg}\,\Sigma$ collapses to an isomorphism of Kleene algebras.

Kleene's theorem [3, 6, 9, 19] states that regular expressions and finite automata are equivalent in expressive power as representations of regular sets of strings over a finite alphabet. Our first lemma asserts that one direction of this theorem, that every regular expression is equivalent to a finite automaton, is a theorem of Kleene algebra.

Lemma 8. *For every regular expression $e \in \mathsf{Exp}\,\Sigma$ (or more accurately, its image in $\mathcal{F}_\Sigma$ under the canonical map), there is a simple automaton (u, A, v) over $\mathcal{F}_\Sigma$ such that $e = u^T A^* v$ in $\mathcal{F}_\Sigma$.*[1]

Proof. The proof is by induction on the structure of the regular expression. We essentially implement the combinatorial constructions as found for example in [8, 15]. The ideas behind this construction are well known and can be found for example in [5].

For $a \in \Sigma$, the automaton

$$\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

suffices, since

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}^* \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a.$$

For the expression $e_1 + e_2$, let $\mathcal{A} = (u, A, v)$ and $\mathcal{B} = (s, B, t)$ be automata such that

$$e_1 = u^T A^* v \qquad\qquad e_2 = s^T B^* t.$$

Consider the automaton

$$\left(\begin{bmatrix} u \\ s \end{bmatrix}, \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}, \begin{bmatrix} v \\ t \end{bmatrix}\right).$$

This construction corresponds to the combinatorial construction of forming the disjoint union of the two sets of states, taking the start states to be the union of the start states of $\mathcal{A}$ and $\mathcal{B}$, and the final states to be the union of the final states of $\mathcal{A}$ and $\mathcal{B}$. Then

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}^* = \begin{bmatrix} A^* & 0 \\ 0 & B^* \end{bmatrix},$$

and

$$\begin{bmatrix} u^T & s^T \end{bmatrix} \cdot \begin{bmatrix} A^* & 0 \\ 0 & B^* \end{bmatrix} \cdot \begin{bmatrix} v \\ t \end{bmatrix} = u^T A^* v + s^T B^* t = e_1 + e_2.$$

For the expression $e_1 e_2$, let $\mathcal{A} = (u, A, v)$ and $\mathcal{B} = (s, B, t)$ be automata such that

$$e_1 = u^T A^* v \qquad\qquad e_2 = s^T B^* t.$$

[1] That is, $\mathcal{F}_\Sigma, [\cdot] \vDash e = u^T A^* v$, where $[\cdot] : \mathsf{Exp}\,\Sigma \to \mathcal{F}_\Sigma$ is the canonical interpretation.

Consider the automaton

$$\left(\left[\begin{array}{c} u \\ 0 \end{array}\right], \left[\begin{array}{cc} A & vs^T \\ 0 & B \end{array}\right], \left[\begin{array}{c} 0 \\ t \end{array}\right]\right)$$

This construction corresponds to the combinatorial construction of forming the disjoint union of the two sets of states, taking the start states to be the start states of $\mathcal{A}$, the final states to be the final states of $\mathcal{B}$, and connecting the final states of $\mathcal{A}$ with the start states of $\mathcal{B}$ by ε-transitions (this is the purpose of the vs^T in the upper right corner of the matrix). Then

$$\left[\begin{array}{cc} A & vs^T \\ 0 & B \end{array}\right]^* = \left[\begin{array}{cc} A^* & A^*vs^TB^* \\ 0 & B^* \end{array}\right],$$

and

$$\left[\begin{array}{cc} u^T & 0 \end{array}\right] \cdot \left[\begin{array}{cc} A^* & A^*vs^TB^* \\ 0 & B^* \end{array}\right] \cdot \left[\begin{array}{c} 0 \\ t \end{array}\right] = u^TA^*vs^TB^*t = e_1e_2.$$

For the expression e^*, let $\mathcal{A} = (u, A, v)$ be an automaton such that $e = u^TA^*v$. We first produce an automaton equivalent to the expression ee^*. Consider the automaton

$$(u, A + vu^T, v).$$

This construction corresponds to the combinatorial construction of adding ε-transitions from the final states of $\mathcal{A}$ back to the start states. Using (23) and (22),

$$u^T(A + vu^T)^*v = u^TA^*(vu^TA^*)^*v = u^TA^*v(u^TA^*v)^* = ee^*.$$

Once we have an automaton for ee^*, we can get an automaton for $e^* = 1 + ee^*$ by the construction for $+$ given above, using a trivial one-state automaton for 1. □

Now we get rid of ε-transitions. This construction is also folklore and can be found for example in [14,19]. This construction models algebraically the combinatorial idea of computing the *ε-closure* of a state; see [8,15].

Lemma 9. *For every simple automaton (u, A, v) over $\mathcal{F}_\Sigma$, there is a simple ε-free automaton (s, B, t) such that*

$$u^TA^*v = s^TB^*t.$$

Proof. By Definition 7, the matrix A can be written as a sum $A = J + A'$ where J is a 0-1 matrix and A' is ε-free. Then

$$u^TA^*v = u^T(J + A')^*v = u^TJ^*(A'J^*)^*v$$

by (23), so we can take

$$s^T = u^TJ^* \qquad\qquad B = A'J^* \qquad\qquad t = v.$$

Note that J^* is 0-1 and therefore B is ε-free. □

The next step in the proof will be to give algebraic analogs of the determinization of finite automata via the subset construction and the minimization of deterministic automata via the collapsing of equivalent states under a Myhill-Nerode equivalence relation. We will do this next time.

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

[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. Dover edition, 2012.

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

[7] F. Gécseg and I. Peák. *Algebraic Theory of Automata.* Akadémiai Kiadó, Budapest, 1972.

[8] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages and Computation.* Addison-Wesley, 1979.

[9] 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.

[10] 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.

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

[12] Dexter Kozen. *Automata and Computability.* Springer-Verlag, New York, 1997.

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

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

[15] Harry R. Lewis and Christos H. Papadimitriou. *Elements of the Theory of Computation.* Prentice Hall, 1981.

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

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

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

[19] 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.

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

[21] Arto Salomaa and Matti Soittola. *Automata Theoretic Aspects of Formal Power Series.* Springer-Verlag, New York, 1978.

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

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