Completeness

Here we continue the program begun in the previous lecture to show the completeness of Kleene algebra for the equational theory of the regular sets.

As in the previous two lectures, we will make extensive use of the bisimulation, sliding, and denesting rules:

$$xy = xz \quad \to \quad x^*y = yz^* \tag{1}$$
$$(xy)^*x \quad = \quad x(yx)^* \tag{2}$$
$$(x+y)^* \quad = \quad x^*(yx^*)^*. \tag{3}$$

The following two results are algebraic analogs of the determinization of automata via the subset construction and the minimization of deterministic automata via the collapsing of equivalent states under a Myhill-Nerode equivalence relation. The original combinatorial versions of these results are due to Rabin and Scott [7] and Myhill and Nerode [5, 6] respectively; see [1, 4, 3] for an elementary exposition. The construction here is from [2].

Lemma 0.1 *For every simple ε-free automaton (u, A, v) over $\mathcal{F}_\Sigma$, there is an equivalent deterministic automaton $(\widehat{u}, \widehat{A}, \widehat{v})$ over $\mathcal{F}_\Sigma$. That is, $u^TA^*v = \widehat{u}^T\widehat{A}^*\widehat{v}$.*

Proof. We model the subset construction algebraically. Let (u, A, v) be a simple ε-free automaton with states Q. Since (u, A, v) is simple, A can be expressed as a sum

$$A \quad = \quad \sum_{a\in\Sigma} a \cdot A_a,$$

where each A_a is a 0-1 matrix.

Let 2^Q denote the power set of Q. We identify elements of 2^Q with their characteristic vectors in $\{0,1\}^n$. For each $s \in 2^Q$, let e_s be the $2^Q \times 1$ vector with 1 in position s and 0 elsewhere.

Let X be the $2^Q \times Q$ matrix whose s^{th} row is s^T; that is,

$$e_s^TX \quad = \quad s^T.$$

For each $a \in \Sigma$, let $\widehat{A}_a$ be the $2^Q \times 2^Q$ matrix whose s^{th} row is $e_{s^T A_a}$; in other words,

$$e_s^T \widehat{A}_a \;=\; e_{s^T A_a}.$$

Let

$$\begin{aligned}
\widehat{A} &= \sum_{a \in \Sigma} a \cdot \widehat{A}_a \\
\widehat{u} &= e_u \\
\widehat{v} &= Xv.
\end{aligned}$$

The automaton $(\widehat{u}, \widehat{A}, \widehat{v})$ is simple and deterministic.

The relationship between A and $\widehat{A}$ is expressed succinctly by the equation

$$XA \;=\; \widehat{A}X. \tag{4}$$

Intuitively, this says that the actions of the two automata in the two spaces K^Q and K^{2^Q} commute with the projection X. To prove (4), observe that for any $s \in 2^Q$,

$$\begin{aligned}
e_s^T XA &= s^T A \\
&= \sum_{a \in \Sigma} a \cdot s^T A_a \\
&= \sum_{a \in \Sigma} a \cdot e_{s^T A_a} X \\
&= \sum_{a \in \Sigma} a \cdot e_s^T \widehat{A}_a X \\
&= e_s^T \widehat{A} X.
\end{aligned}$$

By (4) and (1) (or rather its extension to nonsquare matrices as described in Lecture **??**), we have $XA^* = \widehat{A}^* X$. The theorem now follows:

$$\begin{aligned}
\widehat{u}^T \widehat{A}^* \widehat{v} &= e_u^T \widehat{A}^* X v \\
&= e_u^T X A^* v \\
&= u^T A^* v.
\end{aligned}$$

□

Lemma 0.2 *Let (u, A, v) be a simple deterministic automaton, and let $(\overline{u}, \overline{A}, \overline{v})$ be the equivalent minimal deterministic automaton obtained from the classical state minimization procedure. Then*

$$u^T A^* v \;=\; \overline{u}^T \overline{A}^* \overline{v}.$$

Proof. In the combinatorial approach, the unique minimal automaton is obtained as a quotient by a Myhill-Nerode equivalence relation after removing inaccessible states. We simulate this construction algebraically.

Let Q denote the set of states of (u, A, v). For $q \in Q$, let $e_q \in \{0,1\}^Q$ denote the vector with 1 in position q and 0 elsewhere. Since (u, A, v) is simple, A can be written as a sum

$$A \;=\; \sum_{a \in \Sigma} a \cdot A_a,$$

where the A_a are 0-1 matrices. For each $a \in \Sigma$ and $p \in Q$, let $\delta(p, a)$ be the unique state in Q such that the p^{th} row of A_a is $e^T_{\delta(p,a)}$; that is,

$$e_p^T A_a \;=\; e^T_{\delta(p,a)}.$$

The state $\delta(p, a)$ exists and is unique since the automaton is deterministic.

First we show how to get rid of inaccessible states. A state q is *accessible* if

$$u^T A^* e_q \;\neq\; 0,$$

otherwise it is *inaccessible*. Let R be the set of accessible states and let $U = Q - R$ be the set of inaccessible states. Partition A into four submatrices A_{RR}, A_{RU}, A_{UR}, and A_{UU} such that for $S, T \in \{R, U\}$, A_{ST} is the $S \times T$ submatrix of A. Then A_{RU} is the zero matrix, otherwise a state in U would be accessible. Similarly, partition the vectors u and v into u_R, u_U, v_R and v_U. The vector u_U is the zero vector, otherwise a state in U would be accessible. We have

$$\begin{aligned}
&u^T A^* v \\
&= \left[\begin{array}{c|c} u_R^T & 0 \end{array}\right] \cdot \left[\begin{array}{c|c} A_{RR} & 0 \\ \hline A_{UR} & A_{UU} \end{array}\right]^* \cdot \left[\begin{array}{c} v_R \\ \hline v_U \end{array}\right] \\
&= \left[\begin{array}{c|c} u_R^T & 0 \end{array}\right] \cdot \left[\begin{array}{c|c} A_{RR}^* & 0 \\ \hline A_{UU}^* A_{UR} A_{RR}^* & A_{UU}^* \end{array}\right] \cdot \left[\begin{array}{c} v_R \\ \hline v_U \end{array}\right] \\
&= u_R^T A_{RR}^* v_R.
\end{aligned}$$

Moreover, the automaton (u_R, A_{RR}, v_R) is simple and deterministic, and all states are accessible.

Assume now that (u, A, v) is simple and deterministic and all states are accessible. An equivalence relation $\equiv$ on Q is called *Myhill-Nerode* if $p \equiv q$ implies

$$\delta(p, a) \;\equiv\; \delta(q, a), \quad a \in \Sigma, \tag{5}$$

$$e_p^T v \;=\; e_q^T v. \tag{6}$$

In combinatorial terms, $\equiv$ is *Myhill-Nerode* if it is respected by the action of the automaton under any input symbol $a \in \Sigma$, and the set of final states is a union of $\equiv$-classes.

Let $\equiv$ be any Myhill-Nerode equivalence relation, and let

$$\begin{aligned} [p] &\stackrel{\text{def}}{=} \{q \in Q \mid q \equiv p\} \\ Q/\equiv &\stackrel{\text{def}}{=} \{[p] \mid p \in Q\}. \end{aligned}$$

For $[p] \in Q/\equiv$, let $e_{[p]} \in \{0,1\}^{Q/\equiv}$ denote the vector with 1 in position $[p]$ and 0 elsewhere. Let Y be the $Q \times Q/\equiv$ matrix whose $[p]^{\text{th}}$ column is the characteristic vector of $[p]$; that is,

$$e_p^T Y = e_{[p]}^T.$$

For each $a \in \Sigma$, let $\overline{A}_a$ be the $Q/\equiv \times Q/\equiv$ matrix whose $[p]^{\text{th}}$ row is $e_{[\delta(p,a)]}$; that is,

$$e_{[p]}^T \overline{A}_a = e_{[\delta(p,a)]}^T.$$

The matrix $\overline{A}_a$ is well-defined by (5). Let

$$\begin{aligned} \overline{A} &= \sum_{a \in \Sigma} a \cdot \overline{A}_a \\ \overline{u}^T &= u^T Y. \end{aligned}$$

Also, let $\overline{v} \in \{0,1\}^{Q/\equiv}$ be the vector such that

$$e_{[p]}^T \overline{v} = e_p^T v.$$

The vector $\overline{v}$ is well-defined by (6). Note also that

$$e_p^T Y \overline{v} = e_{[p]}^T \overline{v} = e_p^T v,$$

therefore $Y\overline{v} = v$. The automaton $(\overline{u}, \overline{A}, \overline{v})$ is simple and deterministic.

As in the proof of Lemma 0.1, the actions of A and $\overline{A}$ commute with the linear projection Y:

$$AY = Y\overline{A}. \tag{7}$$

To prove (7), observe that for any $p \in Q$,

$$\begin{aligned}
e_p^T A Y &= \sum_{a \in \Sigma} a \cdot e_p^T A_a Y \\
&= \sum_{a \in \Sigma} a \cdot e_{\delta(p,a)}^T Y \\
&= \sum_{a \in \Sigma} a \cdot e_{[\delta(p,a)]}^T \\
&= \sum_{a \in \Sigma} a \cdot e_{[p]}^T \overline{A}_a \\
&= \sum_{a \in \Sigma} a \cdot e_p^T Y \overline{A}_a \\
&= e_p^T Y \overline{A}.
\end{aligned}$$

Now by (7) and (1), we have $A^*Y = Y\overline{A}^*$, therefore

$$\begin{aligned}
\overline{u}^T \overline{A}^* \overline{v} &= u^T Y \overline{A}^* \overline{v} \\
&= u^T A^* Y \overline{v} \\
&= u^T A^* v.
\end{aligned}$$

□

Lemma 0.3 *Let p be an invertible element of a Kleene algebra with inverse p^{-1}. Then*

$$p^{-1}x^*p = (p^{-1}xp)^*.$$

Proof. We have

$$x^*p = (pp^{-1}x)^*p = p(p^{-1}xp)^*$$

by the sliding rule (2). The result follows by multiplying on the left by p^{-1}. □

Theorem 0.4 (Completeness) *Let α and β be two regular expressions over Σ denoting the same regular set. Then $\alpha = \beta$ is a theorem of Kleene algebra.*

Proof. Let $\mathcal{A} = (s, A, t)$ and $\mathcal{B} = (u, B, v)$ be minimal deterministic finite automata over $\mathcal{F}_\Sigma$ such that

$$\begin{aligned}
R_\Sigma(\alpha) &= R_\Sigma(s^T A^* t) \\
R_\Sigma(\beta) &= R_\Sigma(u^T B^* v).
\end{aligned}$$

By Lemmas **??**, 0.1, and 0.2, we have

$$\alpha = s^T A^* t \qquad \beta = u^T B^* v$$

as theorems of Kleene algebra. Since $R_\Sigma(\alpha) = R_\Sigma(\beta)$, by the uniqueness of minimal automata, $\mathcal{A}$ and $\mathcal{B}$ are isomorphic. Let P be a permutation matrix giving this isomorphism. Then

$$\begin{aligned} A &= P^T B P \\ s &= P^T u \\ t &= P^T v. \end{aligned}$$

Using Lemma 0.3, we have

$$\begin{aligned} \alpha &= s^T A^* t \\ &= (P^T u)^T (P^T B P)^* (P^T v) \\ &= u^T P (P^T B P)^* P^T v \\ &= u^T P P^T B^* P P^T v \\ &= u^T B^* v \\ &= \beta. \end{aligned}$$

□

References

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

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

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

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

[5] J. Myhill. Finite automata and the representation of events. Technical Note WADD 57-624, Wright Patterson AFB, 1957.

[6] A. Nerode. Linear automaton transformations. *Proc. Amer. Math. Soc.*, 9:541–544, 1958.

[7] M. O. Rabin and D. S. Scott. Finite automata and their decision problems. *IBM J. Res. Develop.*, 3(2):115–125, 1959.