CPSC 313 — Supplemental Material for Lecture #4
Correctness of a DFA — Proof of a Useful Result

The goal of this document is to present a proof of the following result, which can be used to prove that a deterministic finite automaton is "correct," that is, has the language that is claimed.

Theorem 1. *Let*

$$M = (Q, \Sigma, \delta, q_0, F)$$

be a deterministic finite automaton and let S_q be a subset of $\Sigma^\star$ associated with q, for each state $q \in Q$. Suppose that the following properties are satisfied.

(a) *Every string $\omega \in \Sigma^\star$ belongs to S_q for* ***exactly one*** *of the states $q \in Q$.*

(b) *$\lambda \in S_{q_0}$, where S_{q_0} is the subset of $\Sigma^\star$ corresponding to the start state q_0 of Q.*

(c) *$\{\omega \cdot \sigma \mid \omega \in S_q\} \subseteq S_{\delta(q.\sigma)}$ for every state $q \in Q$ and for every symbol $\sigma \in \Sigma$.*

Then

$$\delta^\star(q_0, \omega) = q$$

for every state $q \in Q$ and for every string $\omega \in S_q$.

Proof. Suppose $M = (Q, \Sigma, \delta, q_0, F)$ is a deterministic finite automaton, that a subset S_q of Q is associated with each state q of Q, and that the above properties (a)–(c) are satisfied. Then it will be proved that

$$\delta^\star(q_0, \omega) = q \tag{1}$$

for every state $q \in Q$ and for every string $\omega \in S_q$, using ***mathematical induction on the length of the string ω***. The standard form of mathematical induction will be used.

Basis: It is necessary and sufficient to show that

$$\delta^\star(q_0, \omega) = q_0$$

for every state $q \in Q$ and for every string $\omega \in S_q$ whose length is zero.

Suppose, therefore, that ω is a string in S_q with length zero. Then $\omega = \lambda$, the empty string (since no other strings in $\Sigma^\star$ with length zero exist), and it follows by property (b), above, that $\lambda \in S_{q_0}$, the subset of $\Sigma^\star$ corresponding to the start state q_0 of M. It is therefore necessary and sufficient to show that

$$\delta^\star(q_0, \lambda) = q_0.$$

However, this follows directly from the definition of extended transition function $\delta^\star : Q \times \Sigma^\star \to Q$ (as given in Lecture #2).

Inductive Step: Let k be an integer such that $k \geq 0$. It is necessary and sufficient to use the following

> Inductive Hypothesis: $\delta^\star(q_0, \omega) = q$ for every state $q \in Q$ and for every string $\omega \in S_q$ whose length is k.

to prove the following

> Inductive Claim: $\delta^\star(q_0, \omega) = q$ for every state $q \in Q$ and for every string $\omega \in S_q$ whose length is $k+1$.

With that noted, let $q \in Q$ and let ν be a string in S_q whose length is $k+1$. Then, since $k+1 \geq 1$, ν has positive length and there exists a string $\mu \in \Sigma^\star$ and a symbol $\sigma \in Q$ such that

$$\nu = \mu \cdot \sigma. \tag{2}$$

Now, the length of μ is one less than the length of ν, so that μ is a string in $\Sigma^\star$ with length k.

Property (a), above, implies that there exists exactly one state $r \in Q$ such that $\mu \in S_r$, the subset corresponding to r. Now, since $r \in Q$ and μ is a string with length k in S_r, it follows by the ***inductive hypothesis*** that

$$\delta^\star(q_0, \mu) = r. \tag{3}$$

Notice that

$$\nu = \mu \cdot \sigma \subseteq \{\omega \cdot \sigma \mid \omega \in S_r\},$$

and that property (c), above, implies that

$$\{\omega \cdot \sigma \mid \omega \in S_r\} \subseteq S_{\delta(r,\sigma)},$$

where $S_{\delta(r,\sigma)}$ is the subset of $\Sigma^\star$ corresponding to the state $\delta(r, \sigma)$. It follows that

$$\nu \in S_{\delta(r,\sigma)}.$$

However, ν was chosen from S_q and it now follows that

$$\delta(r, \sigma) = q \tag{4}$$

— for, otherwise, ν would belong to subsets of $\Sigma^\star$ corresponding to at least *two* of the states in Q. This would contradict property (a) from the statement of the claim.

It now follows that

$$\begin{aligned}
\delta^\star(q_0, \nu) &= \delta^\star(q_0, \mu \cdot \sigma) && \text{(since } \nu = \mu \cdot \sigma \text{ as shown at line (2), above)} \\
&= \delta(\delta^\star(q_0, \mu), \sigma) && \text{(by the definition of the extended transition function } \delta^\star) \\
&= \delta(r, \sigma) && \text{(since } \delta^\star(q_0, \mu) = r\text{, as shown at line (3), above)} \\
&= q && \text{(as shown at line (4), above).}
\end{aligned}$$

Now, since q was an arbitrarily chosen state in Q, and since ν was an arbitrarily chosen string with length $k+1$ in S_q, it follows that

$$\delta^\star(q_0, \omega) = q$$

for every state $q \in Q$ and for every string ω with length $k+1$ in S_q — establishing the inductive claim, and completing the inductive step.

The claim now follows by induction on the length of the string ω. ☐

Corollary 2. *Let*

$$M = (Q, \Sigma, \delta, q_0, F)$$

be a deterministic finite automaton and let S_q be a subset of $\Sigma^\star$ associated with q for each state $q \in Q$. Suppose that properties (a)–(c) from the statement of Theorem 1 are satisfied. Then the language $L(M)$ of the automaton M is

$$\bigcup_{q \in F} S_q.$$

Proof. Suppose first that

$$\omega \in \bigcup_{q \in F} S_q.$$

Then $\omega \in S_q$ for some state $q \in F$. It follows by Theorem 1 that

$$\delta^\star(q_0, \omega) = q \in F,$$

so that M accepts ω — and $\omega \in L(M)$. Since ω was arbitrarily chosen, this implies that

$$\bigcup_{q \in F} S_q \subseteq L(M). \tag{5}$$

Suppose next that $\omega \in \Sigma^\star$ but

$$\omega \notin \bigcup_{q \in F} S_q.$$

Then $\omega \notin S_q$ for any state $q \in F$, and it follows by property (a) (from the statement of Theorem 1) that $\omega \in S_r$ for some state $r \in Q$ such that $r \notin F$. It follows by another application of Theorem 1 that

$$\delta^\star(q_0, \omega) = r \notin F,$$

so that M rejects ω — and $\omega \notin L(M)$. Since ω was arbitrarily chosen, this implies that if $\omega \notin \bigcup_{q \in F} S_q$ then $\omega \notin L(M)$, for all $\omega \in \Sigma^\star$, so that

$$L(M) \subseteq \bigcup_{q \in F} S_q. \tag{6}$$

The containments shown at lines (5) and (6), above, establish that

$$\bigcup_{q \in F} S_q = L(M),$$

as claimed. □