Lecture #4: DFA Design and Verification — Part Two
Proof of a Significant Technical Result

The notes for this lecture included the following "significant technical result".

Theorem 1 (Correctness of a DFA)**.** *Let $L \subseteq \Sigma^\star$, for an alphabet Σ, and let*

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

with the same alphabet Σ. Suppose that (after renaming states, if needed)

$$Q = \{q_0, q_1, \ldots, q_{n-1}\}$$

where $n = |Q| \geq 1$. Suppose, as well, that

$$S_0, S_1, \ldots, S_{n-1}$$

are subsets of $\Sigma^\star$ such that the following properties are satisfied.

(a) Every string in $\Sigma^\star$ belongs to **exactly one** *of*

$$S_0, S_1, \ldots, S_{n-1}.$$

(b) $\lambda \in S_0$.

(c) $S_i \subseteq L$ for every integer i such that $0 \leq i \leq n-1$ and $q_i \in F$.

(d) $S_i \cap L = \emptyset$ for every integer i such that $0 \leq i \leq n-1$ and $q_i \notin F$.

(e) The following property is satisfied, for every integer i such that $0 \leq i \leq n-1$ and for every symbol $\sigma \in \Sigma$:

"Suppose that $q_j = \delta(q_i, \sigma)$ (so that $0 \leq j \leq n-1$). Then $\{\omega \cdot \sigma \mid \omega \in S_i\} \subseteq S_j$."

Then $L(M) = L$.

This document provides a proof of this result.

To begin, consider the following claim, which asserts that the "extended transition function" of the DFA models the relationship between the given subsets of $\Sigma^\star$, and states of the DFA, that one would expect.

Lemma 2. *Let $L \subseteq \Sigma^\star$, for an alphabet Σ, and let*

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

with the same alphabet Σ. Suppose that (after renaming states, if needed)

$$Q = \{q_0, q_1, \ldots, q_{n-1}\}$$

where $n = |Q| \geq 1$. Suppose, as well, that

$$S_0, S_1, \ldots, S_{n-1}$$

are subsets of $\Sigma^\star$ such that properties (a), (b), and (e), given in Theorem 1 are satisfied — that is,

(a) Every string in $\Sigma^\star$ belongs to **exactly one** *of*

$$S_0, S_1, \ldots, S_{n-1}.$$

(b) $\lambda \in S_0$.

(e) The following property is satisfied, for every integer i such that $0 \leq i \leq n-1$ and for every symbol $\sigma \in \Sigma$:

"Suppose that $q_j = \delta(q_i, \sigma)$ (so that $0 \leq j \leq n-1$). Then $\{\omega \cdot \sigma \mid \omega \in S_i\} \subseteq S_j$."

Then the following holds, for every string $\omega \in \Sigma^\star$: For every integer j such that $0 \leq j \leq n-1$, $\delta^\star(q_0, \omega) = q_j$ if and only if $\omega \in S_j$.

Proof. The result will be proved ***by induction on the length of the string ω***. The standard form of mathematical induction will be used, and the case that $|\omega| = 0$ will be considered in the basis.

Basis: If $|\omega| = 0$ then $\omega = \lambda$, the empty string. Thus it is necessary and sufficient to prove that, for every integer j such that $0 \leq j \leq n-1$, $\delta^\star(q_0, \lambda) = q_j$ if and only if $\lambda \in S_j$.

Either $j = 0$ or $1 \leq j \leq n-1$. These cases are considered separately, below.

- If $j = 0$ then it follows by the definition of the "extended transition function" that

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

  so that it is now necessary and sufficient to show that $\lambda \in S_j$. Since $j = 0$, $S_j = S_0$, and this follows by property (b), as given above.

- If $1 \leq j \leq n-1$ then it follows, again by the definition of the "extended transition function", that
$$\delta^\star(q_0, \lambda) = q_0 \neq q_j$$
so that it is now necessary and sufficient to show that $\lambda \notin S_j$. Now, as noted above, $\lambda \in S_0$ and it follows by property (a) that λ belongs to *exactly one* of $S_0, S_1, \ldots, S_{n-1}$. Thus λ *does not* belong to S_j (since $j \neq 0$). That is, $\lambda \notin S_j$, as desired.

Thus $\delta^\star(\lambda) = q_j$ if and only if $\lambda \in S_j$, for every integer j such that $0 \leq j \leq n-1$, as required here.

Inductive Step: Let k be an integer such that $k \geq 0$. it is now necessary and sufficient (for the Inductive Step) to use the following "Inductive Hypothesis" to prove the following "Inductive Claim".

> Inductive Hypothesis: The following property is satisfied for every string $\omega \in \Sigma^\star$ such that $|\omega| = k$: For every integer j such that $0 \leq j \leq n-1$, $\delta^\star(q_0, \omega) = q_j$ if and only if $\omega \in S_j$.
>
> Inductive Claim: The following property is satisfied for every string $\omega \in \Sigma^\star$ such that $|\omega| = k+1$: For every integer j such that $0 \leq j \leq n-1$, $\delta^\star(q_0, \omega) = q_j$ if and only if $\omega \in S_j$.

With that noted, let ω be a string in $\Sigma^\star$ such that $|\omega| = k+1$ — so that we now wish to prove (for this string) that, for every integer j such that $0 \leq j \leq n-1$, $\delta^\star(q_0, \omega) = q_j$ if and only if $\omega \in S_j$.

Since $k \geq 0$, $k+1 \geq 1$, so that $|\omega| \geq 1$. Thus
$$\omega = \mu \cdot \sigma$$
for some string $\mu \in \Sigma^\star$ such that $|\mu| = k$, and for some symbol $\sigma \in \Sigma$.

Let ℓ be an integer such that $0 \leq \ell \leq n-1$ and such that
$$\delta^\star(q_0, \mu) = q_\ell. \tag{1}$$

Then — since μ is a string in $\Sigma^\star$ such that $|\mu| = k$ — It follows, ***by the Inductive Hypothesis,*** that $\delta^\star(q_0, \mu) = q_h$ if and only if $\mu \in S_h$, for every integer h such that $0 \leq h \leq n-1$. Thus $\mu \in S_\ell$, by the equation at line (1) and — since property (a) is satisfied — $\mu \notin S_h$ for any integer h such that $0 \leq h \leq n-1$ and $h \neq \ell$.

Let j be an integer such that $0 \leq j \leq n-1$, so that we now wish to prove that $\delta^\star(q_0, \omega) = q_j$ if and only if $\omega \in S_j$. Either $q_j = \delta(q_\ell, \sigma)$ or $q_j \neq \delta(q_\ell, \sigma)$. These cases are considered separately, below.

- If $q_j = \delta(q_\ell, \sigma)$ then

$$\begin{aligned}
\delta^\star(q_0, \omega) &= \delta^\star(q_0, \mu \cdot \sigma) && \text{(since } \omega = \mu \cdot \sigma\text{)} \\
&= \delta(\delta^\star(q_0, \mu), \sigma) && \text{(by the results of Lecture \#2)} \\
&= \delta(q_\ell, \sigma) && \text{(by the equation at line (1)).}
\end{aligned}$$

  Thus $\delta^\star(q_0, \omega) = q_j$, and we now wish to prove that $\omega \in S_j$.

  As noted above, $\mu \in S_\ell$. Since $q_j = \delta(q_\ell, \sigma)$, it follows by property (e) (using ℓ in place of the integer called i, and using μ in place of the string called ω) that

$$\omega = \mu \cdot \sigma \subseteq \{\nu \cdot \sigma \mid \nu \in S_\ell\} \subseteq S_j.$$

  That is, $\omega \in S_j$ as desired.

- If $q_j \neq \delta(q_\ell, \sigma)$ then $\delta^\star(q_0, \omega) \neq q_j$ because $\delta^\star(q_0, \omega) = \delta(q_\ell, \sigma)$, as shown above — and we now wish to prove that $\omega \notin S_j$. Set h to be the integer such that $0 \leq h \leq n-1$ and $\delta(q_\ell, \sigma) = q_h$. Then property (e) can be applied, once again, to argue that

$$\omega = \mu \cdot \sigma \in \{\nu \cdot \sigma \mid \nu \in S_\ell\} \subseteq S_h.$$

  Now, since $q_h = \delta(q_\ell, \sigma) \neq q_j$, $h \neq j$ and it follows by property (a) that $\omega \notin S_j$ (since this property now implies that $S_h \cap S_h = \emptyset$) — as desired.

Thus $\delta^\star(q_0, \omega) = q_j$ if and only if $\omega \in S_j$, for every integer j such that $0 \leq j \leq n-1$. Since ω was an arbitrarily chosen string in $\Sigma^\star$ such that $|\omega| = k+1$, this establishes the Inductive Claim — as needed to complete the Inductive Step.

The claim now follows by induction on the length of ω. $\square$

It remains only to use the above claim, and conditions (c) and (d) (from the statement of Theorem 1) to prove that $L(M) = L$. As is often the case, it easiest to see this if we split this into two tasks, namely, proving that $L(M) \subseteq L$, and proving that $L \subseteq L(M)$.

Lemma 3. *Let $L \subseteq \Sigma^\star$, for an alphabet Σ, and let*

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

with the same alphabet Σ. Suppose that (after renaming states, if needed)

$$Q = \{q_0, q_1, \ldots, q_{n-1}\}$$

where $n = |Q| \geq 1$. Suppose, as well, that

$$S_0, S_1, \ldots, S_{n-1}$$

are subsets of $\Sigma^\star$ such that properties (a), (b), (c) and (e) given in Theorem 1 are satisfied — that is, properties (a), (b), and (e) are satisfied and (since property (c) is satisfied, as well) $S_i \subseteq L$ for every integer i such that $0 \leq i \leq n-1$ and $q_i \in F$. Then $L(M) \subseteq L$.

Proof. Let $\omega \in \Sigma^\star$ such that $\omega \in L(M)$, that is, such that M accepts ω. It is necessary, and sufficient, to prove that $\omega \in L$.

Since M accepts ω, $\delta^\star(q_0, \omega) = q_j$ for some integer j such that $0 \leq j \leq n-1$ and $q_j \in F$. Since properties (a), (b) and (e) are satisfied, it follows by Lemma 2 that $\omega \in S_j$. Since $q_j \in F$, it follows by property (c) that $S_j \subseteq L$. Thus $\omega \in L$, as needed to establish the claim. $\square$

Lemma 4. *Let $L \subseteq \Sigma^\star$, for an alphabet Σ, and let*

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

with the same alphabet Σ. Suppose that (after renaming states, if needed)

$$Q = \{q_0, q_1, \ldots, q_{n-1}\}$$

where $n = |Q| \geq 1$. Suppose, as well, that

$$S_0, S_1, \ldots, S_{n-1}$$

are subsets of $\Sigma^\star$ such that properties (a), (b), (d) and (e) given in Theorem 1 are satisfied — that is, properties (a), (b) and (e) are satisfied and (since property (d) is satisfied, as well) $S_i \cap L = \emptyset$ for every integer i such that $0 \leq i \leq n-1$ and $q_i \notin F$. Then $L \subseteq L(M)$.

Proof. Let $\omega \in \Sigma^\star$ such that $\omega \in L$. It is necessary and sufficient to prove that $L \subseteq L(M)$, that is, M accepts ω.

Suppose, to obtain a contradiction, that M *does not* accept ω — that, is, $\delta^\star(q_0, \omega) = q_j$ for some integer j such that $0 \leq j \leq n-1$ and $q_j \notin F$. Since properties (a), (b) and (e) are satisfied, it follows by Lemma 2 that $\omega \in S_j$. Since $q_j \notin F$, it follows by property (d) that $S_j \cap L = \emptyset$. Thus $\omega \notin L$ and, since ω was chosen to be in L, a ***contradiction*** has been obtained. Our assumption must, therefore be false. That is, M accepts ω, so that $\omega \in L(M)$.

Since ω was arbitrarily chosen from L it follows that $L \subseteq L(M)$, as claimed. $\square$

Proof of Theorem 1. Theorem 1 follows directly from Lemmas 3 and 4, which have now been proved. $\square$