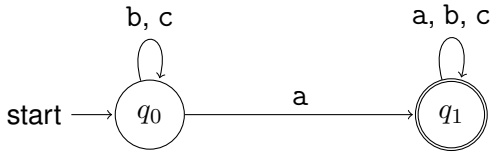
Lecture #4: DFA Design and Verification — Part Two
Completion of Another Example

Problem To Be Solved

Let $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. A supplement for the previous lecture concerned the design of a deterministic finite automaton for the language

$$L = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “a”}\}$$

The following deterministic finite automaton was obtained:



As the rest of this document shows, information that was discovered during the design process, can be used to develop a proof that this DFA has the desired language.

Confirming That We Have a DFA with Alphabet Σ

To begin, let us recall that

$$M = (Q, \Sigma, \delta, q_1, F)$$

where the components of M are as follows.

- $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ — the same ***alphabet*** as used to define the language L.
- $Q = \{q_0, q_1\}$ — a finite, nonempty set of ***states*** such that $Q \cap \Sigma = \{\emptyset\}$.
- The ***start state***, q_0, is a state in Q.
- The set $F = \{q_1\}$ of ***accepting states*** is a subset of Q.
- The ***transition function*** is a well-defined total function $\delta : Q \times \Sigma \to Q$. Indeed, an inspection of the transition function shows that this function can also be described using the following transition table.

(a) Every string in $\Sigma^\star$ belongs to ***exactly one*** of S_0 or S_1 (needed since $Q = \{q_0, q_1\}$, and S_0 and S_1 are the subsets of $\Sigma^\star$ corresponding to q_0 and q_1, respectively).

(b) $\lambda \in S_0$ (needed since S_0 corresponds to the start state, q_0).

(c) $S_1 \subseteq L$ (needed since the state q_1, corresponding to the set S_1, belongs to F).

(d) $S_0 \cap L = \emptyset$ (needed since the state q_0, corresponding to the set S_0, does not belong to F).

(e) The following properties are satisfied.

(i) $\{\omega \cdot \mathtt{a} \mid \omega \in S_0\} \subseteq S_1$ (needed since $\delta(q_0, \mathtt{a}) = q_1$).
(ii) $\{\omega \cdot \mathtt{b} \mid \omega \in S_0\} \subseteq S_0$ (needed since $\delta(q_0, \mathtt{b}) = q_0$).
(iii) $\{\omega \cdot \mathtt{c} \mid \omega \in S_0\} \subseteq S_0$ (needed since $\delta(q_0, \mathtt{c}) = q_0$).
(iv) $\{\omega \cdot \mathtt{a} \mid \omega \in S_1\} \subseteq S_1$ (needed since $\delta(q_1, \mathtt{a}) = q_1$).
(v) $\{\omega \cdot \mathtt{b} \mid \omega \in S_1\} \subseteq S_1$ (needed since $\delta(q_1, \mathtt{b}) = q_1$).
(vi) $\{\omega \cdot \mathtt{c} \mid \omega \in S_1\} \subseteq S_1$ (needed since $\delta(q_1, \mathtt{c}) = q_1$).

Figure 1: Properties Used to Prove That $L(M) = L$

	a	b	c
q_0	q_1	q_0	q_0
q_1	q_1	q_1	q_1

Thus this is a well-defined deterministic finite automaton with alphabet Σ — so its language, $L(M)$, is a subset of $\Sigma^\star$ — just like L is. It remains only to prove that these are the *same* subset of $\Sigma^\star$, that is, $L(M) = L$.

Confirming that $L(M) = L$

Recall that the lecture notes introduced a "key technical claim" that could be used to prove that a deterministic finite automaton has a given language. In order to apply this result, the properties shown in Figure 1, above, must all be shown to hold.

Since the above deterministic finite automaton has only two states — whose corresponding subsets of $\Sigma^\star$ are the language L and its complement —it is easy to show that properties (a)–(d) are satisfied. Proving condition (e) is not quite as straightforward — primarily because it includes quite a few relationships between sets that must be checked.

Lemma 1. *Each of the conditions shown in property (e) (as shown in Figure 1) is satisfied.*

Proof. Each of the claimed relationships can be established by considering the definitions of the subsets of $\Sigma^\star$ that are mentioned in the claims.

- Let $\omega \in \Sigma^\star$ such that $\omega \in S_0$, so that ω does not include an "a".

  The string $\omega \cdot \mathsf{a}$ certainly does include an "a", since it ends with a copy of this symbol, so $\omega \cdot \mathsf{a} \in S_1$. On the other hand, neither of the strings $\omega \cdot \mathsf{b}$ or $\omega \cdot \mathsf{c}$ include an "a", since there are no copies of "a" in ω, so that $\omega \cdot \mathsf{b} \in S_0$ and $\omega \cdot \mathsf{b} \in S_0$. Since the string ω was arbitrarily chosen such that $\omega \in S_0$ it follows that

  $$\{\omega \cdot \mathsf{a} \mid \omega \in S_0\} \subseteq S_1,$$

  $$\{\omega \cdot \mathsf{b} \mid \omega \in S_0\} \subseteq S_0,$$

  and

  $$\{\omega \cdot \mathsf{c} \mid \omega \in S_0\} \subseteq S_0.$$

  That is, conditions (i), (ii) and (iii) are satisfied.

- Let $\omega \in \Sigma^\star$ such that $\omega \in S_1$, so that ω includes at least one "a". Then $\omega \cdot \sigma$ must also include at least one "a", for any symbol $\sigma \in \Sigma$, since ω is a substring of $\omega \cdot \sigma$. Thus $\omega \cdot \sigma \in S_1$, for all $\sigma \in \Sigma$. That is, $\omega \cdot \mathsf{a} \in S_1$, $\omega \cdot \mathsf{b} \in S_1$, and $\omega \cdot \mathsf{c} \in S_1$.

  Since the string ω was arbitrarily chosen such that $\omega \in S_1$, it now follows that

  $$\{\omega \cdot \mathsf{a} \mid \omega \in S_1\} \subseteq S_1,$$

  $$\{\omega \cdot \mathsf{b} \mid \omega \in S_1\} \subseteq S_1,$$

  and

  $$\{\omega \cdot \mathsf{c} \mid \omega \in S_1\} \subseteq S_1.$$

  That is, conditions (iv), (v) and (vi) are satisfied, as needed to establish the claim. □

Theorem 2. $L(M) = L$.

Proof. This result will be established by applying the "Correctness of a DFA" theorem that was introduced in the notes for this lecture. An examination of the statement of that theorem, the language L, and the above DFA confirms that it is necessary, and sufficient, to show that each of the properties that are listed in Figure 1 are satisfied, in order to confirm that $L(M) = L$. "Correctness of a DFA" theorem that was introduced in the notes for this lecture.

- Let $\omega \in \Sigma^\star$. Then either ω does not include a copy of "a", so that $\omega \in S_0$, or ω includes at least one copy of "a", so that $\omega \in S_1$. That is, $\omega \in S_0 \cup S_1$. Since ω was arbitrarily chosen from $\Sigma^\star$, it follows that every string in $\Sigma^\star$ belongs to *at least* one of the sets S_0 or S_1.

  On the other hand, $S_0 \cap S_1 = \emptyset$ — for if ω belonged to both S_0 and S_1 then ω would have to include at least one "a" (since $\omega \in S_1$) and no a's at all (since $\omega \in S_0$) — and both of these conditions cannot be satisfied at the same time. Thus every string in $\Sigma^\star$ belongs to *exactly* one of the subsets S_0 and S_1. That is, property (a) is satisfied.

- Since the empty string, λ does not include any a's, $\lambda \in S_0$ — and property (b) is satisfied.
- Since $S_1 = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one "a"}\} = L$, $S_1 \subseteq L$, and property (c) is satisfied.
- As noted above, $S_0 \cap S_1 = \emptyset$ — so that $S_1 \cap L = \emptyset$, since $S_1 = L$. Thus property (d) is satisfied.
- Lemma 1 implies that property (e) is satisfied.

Since all the properties listed in Figure 1 are satisfied, it now follows by the theorem concerning the "correctness of a DFA", from the lecture notes, that $L(M) = L$, as claimed. □

More About This Example

This example is considerably shorter and simpler than the first one (even though more details are given than is necessary, once again) — because the deterministic finite automaton, being considered, here, has fewer states than the deterministic finite automaton in the first example did.

It is certainly not a mistake to present a different (correct) deterministic finite automaton than the one given as a solution for a problem — but a proof of the correctness of the deterministic finite automaton will generally be longer, and more complicated, for a deterministic finite automaton with lots of states than it is for a deterministic finite automaton with only a few states.