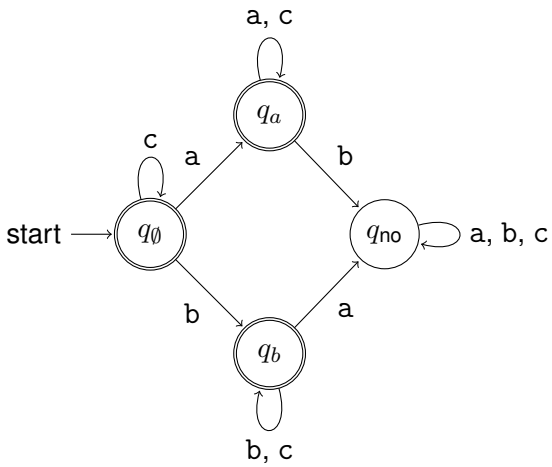
Lecture #4: DFA Design and Verification — Part Two
Completion of Example

Recall that the lecture example concerned the language $L \subseteq \Sigma^\star$ for the alphabet $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, and for

$$L = \{\omega \in \Sigma^\star \mid \text{either } \omega \text{ does not include an “a” or } \omega \text{ does not include a “b”}\}.$$

The designed process, introduced in this lecture, was used to produce a deterministic finite automaton M with the following transition diagram



along with the following subsets of $\Sigma^\star$:

- The set $S_\emptyset = \{\omega \in \Sigma^\star \mid \omega \text{ only includes c's}\}$ corresponds to the state q_0.
- The set $S_a = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “a” but no b's}\}$ corresponds to the state q_a.
- The set $S_b = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “b” but no a's}\}$ corresponds to the state q_a.
- The set $S_{\mathsf{no}} = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “a” and at least one “b”}\}$ corresponds to the state q_{no}.

The goal of this document is to complete the ongoing example by providing a ***proof*** that $L(M) = L$ — establishing that the DFA is "correct" (when considered as a solution for this design problem).

Confirming That We Have a DFA with Alphabet Σ

To begin, let us note that — as shown above —

$$M = (Q, \Sigma, \delta, q_\emptyset, F)$$

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.
- $Q = \{q_\emptyset, q_a, q_b, q_{\mathsf{no}}\}$ — a finite, nonempty set of ***states*** such that $Q \cap \Sigma = \emptyset$.
- The ***start state***, $q_\emptyset$, is a state in Q.
- The set $F = \{q_\emptyset, q_a, q_b\}$ 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.[1]

	a	b	c
$q_\emptyset$	q_a	q_b	$q_\emptyset$
q_a	q_a	q_{no}	q_a
q_b	q_{no}	q_b	q_b
q_{no}	q_{no}	q_{no}	q_{no}

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, on page 3, must all be shown to hold.

[1] This table has a row for every state in Q, and a column for every symbol in Σ. It is consistent with the given transition diagram and every cell of this table stores exactly one state in Q — so it represents a total function from $Q \times \Sigma$ to Q, as required.

(a) Every string in $\Sigma^\star$ belongs to ***exactly one*** of $S_\emptyset$, S_a, S_b, or S_{no}. (needed since $Q = \{q_\emptyset, q_a, q_b, q_{\mathsf{no}}\}$ and $S_\emptyset$, S_a, S_b and S_{no} are subsets of $\Sigma^\star$ corresponding to the states $q_\emptyset$, q_a, q_b and q_{no}, respectively).

(b) $\lambda \in S_\emptyset$ (needed since $S_\emptyset$ corresponds to the start state, $q_\emptyset$).

(c) $S_\emptyset \subseteq L$, $S_a \subseteq L$, and $S_b \subseteq L$ (needed since the states $q_\emptyset$, q_a and q_b, corresponding to the sets $S_\emptyset$, S_a and S_b, respectively, are all in F).

(d) $S_{\mathsf{no}} \cap L = \emptyset$ (needed since the state q_{no}, corresponding to the set S_{no}, is not in F).

(e) The following properties are satisfied.

(i) $\{\omega \cdot \mathsf{a} \mid \omega \in S_\emptyset\} \subseteq S_a$ (needed since $\delta(q_\emptyset, \mathsf{a}) = q_a$).
(ii) $\{\omega \cdot \mathsf{b} \mid \omega \in S_\emptyset\} \subseteq S_b$ (needed since $\delta(q_\emptyset, \mathsf{b}) = q_b$).
(iii) $\{\omega \cdot \mathsf{c} \mid \omega \in S_\emptyset\} \subseteq S_\emptyset$ (needed since $\delta(q_\emptyset, \mathsf{c}) = q_\emptyset$).
(iv) $\{\omega \cdot \mathsf{a} \mid \omega \in S_a\} \subseteq S_a$ (needed since $\delta(q_a, \mathsf{a}) = q_a$).
(v) $\{\omega \cdot \mathsf{b} \mid \omega \in S_a\} \subseteq S_{\mathsf{no}}$ (needed since $\delta(q_a, \mathsf{b}) = q_{\mathsf{no}}$).
(vi) $\{\omega \cdot \mathsf{c} \mid \omega \in S_a\} \subseteq S_a$ (needed since $\delta(q_a, \mathsf{c}) = q_a$).
(vii) $\{\omega \cdot \mathsf{a} \mid \omega \in S_b\} \subseteq S_{\mathsf{no}}$ (needed since $\delta(q_b, \mathsf{a}) = q_{\mathsf{no}}$).
(viii) $\{\omega \cdot \mathsf{b} \mid \omega \in S_b\} \subseteq S_b$ (needed since $\delta(q_b, \mathsf{b}) = q_b$).
(ix) $\{\omega \cdot \mathsf{c} \mid \omega \in S_b\} \subseteq S_b$ (needed since $\delta(q_b, \mathsf{c}) = q_b$).
(x) $\{\omega \cdot \mathsf{a} \mid \omega \in S_{\mathsf{no}}\} \subseteq S_{\mathsf{no}}$ (needed since $\delta(q_{\mathsf{no}}, \mathsf{a}) = q_{\mathsf{no}}$).
(xi) $\{\omega \cdot \mathsf{b} \mid \omega \in S_{\mathsf{no}}\} \subseteq S_{\mathsf{no}}$ (needed since $\delta(q_{\mathsf{no}}, \mathsf{b}) = q_{\mathsf{no}}$).
(xii) $\{\omega \cdot \mathsf{c} \mid \omega \in S_{\mathsf{no}}\} \subseteq S_{\mathsf{no}}$ (needed since $\delta(q_{\mathsf{no}}, \mathsf{c}) = q_{\mathsf{no}}$).

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

Checking That Every String in $\Sigma^\star$ Belong to Exactly One Subset

Let us begin by showing that property (a) is satisfied.

Lemma 1. *Every string in $\Sigma^\star$ belongs to exactly one of the subsets $S_\emptyset$, S_a, S_b and S_{no}.*

Proof. Let us first show that every string in $\Sigma^\star$ belongs to *at least* one of the sets $S_\emptyset$, S_a, S_b and S_{no}, that is

$$S_\emptyset \cup S_a \cup S_b \cup S_{\mathsf{no}} = \Sigma^\star.$$

Let $\omega \in \Sigma^\star$. Then either ω does not include any a's, or ω includes at least one "a". These cases are considered separately, below.

- If ω does not include any a's, then either ω does not include b's, or ω includes at least one "b". These subcases are considered separately, below.

  - If ω does not include any b's, then $\omega \in S_\emptyset \subseteq S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$, as desired.
  - If ω includes at least one "b", then $\omega \in S_b \subseteq S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$, as desired.

  Since both possible cases have been considered, it now follows that if $\omega \in \Sigma^\star$ such that ω does not include any a's, then $\omega \in S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$.

- If ω includes at least one "a", then either ω does not include b's, or ω includes at least one "b". These subcases are considered separately, below.

  - If ω does not include any b's, then $\omega \in S_a \subseteq S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$, as desired.
  - If ω includes at least one "b", then $\omega \in S_{\text{no}} \subseteq S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$, as desired.

  Since both possible cases have been considered, it now follows that if $\omega \in \Sigma^\star$ such that ω includes at least one "a", then $\omega \in S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$, as desired.

Since both possible cases have now been considered, it now follows that if $\omega \in \Sigma^\star$, then $\omega \in S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}$. That is,

$$\Sigma^\star \subseteq S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}}.$$

On the other hand, since $S_\emptyset \subseteq \Sigma^\star$, $S_a \subseteq \Sigma^\star$, $S_b \subseteq \Sigma^\star$, and $S_{\text{no}} \subseteq \Sigma^\star$, it is certainly true that

$$S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}} \subseteq \Sigma^\star$$

as well. Thus

$$S_\emptyset \cup S_a \cup S_b \cup S_{\text{no}} = \Sigma^\star,$$

and every string in $\Sigma^\star$ belongs to at least one of $S_\emptyset$, S_a, S_b, or S_{no}.

It remains only to show that every string in $\Sigma^\star$ belongs to *at most* one of $S_\emptyset$, S_a, S_b, or S_{no}. This can be proved by establishing each of the following, for every string $\omega \in \Sigma^\star$.

(a) If $\omega \in S_\emptyset$ then ω does not belong to any of S_a, S_b, or S_{no}.

(b) If $\omega \in S_a$ then ω does not belong to any of $S_\emptyset$, S_b, or S_{no}.

(c) If $\omega \in S_b$ then ω does not belong to any of $S_\emptyset$, S_a, or S_{no}.

(d) If $\omega \in S_{\text{no}}$ then ω does not belong to any of S_a, S_b, or S_{no}.

Each of these is proved separately, below.

(a) Let $\omega \in S_\emptyset$, so that ω does not include any a's or b's. Then $\omega \notin S_a$, since every string in S_a includes at least one "a"; $\omega \notin S_b$, since every string in S_b includes at least one "b"; and $\omega \notin S_{\text{no}}$ since every string in S_{no} includes at least one "a". Thus

$$S_\emptyset \cap S_a = S_\emptyset \cap S_b = S_\emptyset \cap S_{\text{no}} = \emptyset,$$

that is, no string in $S_\emptyset$ belongs to any of S_a, S_b, or S_{no}.

(b) Let $\omega \in S_a$, so that ω includes at least one "a" but does not include any b's. Then $\omega \notin S_\emptyset$, since $S_\emptyset \cap S_a = \emptyset$, as noted in the proof of the above condition (a); $\omega \notin S_b$ and $\omega \notin S_{\text{no}}$, since every string in either S_b or S_{no} must include at least one "b". Thus

$$S_a \cap S_\emptyset = S_a \cap S_b = S_a \cap S_{\text{no}} = \emptyset,$$

that is, no string in S_a belongs to any of $S_\emptyset$, S_b, or S_{no}.

(c) Let $\omega \in S_b$, so that ω includes at least one "b" but does not include any a's. Then $\omega \notin S_\emptyset$, since $S_\emptyset \cap S_b = \emptyset$, as noted in the proof of the above condition (a); $\omega \notin S_a$, since $S_a \cap S_b = \emptyset$, as noted in the proof of the above condition (b); and $\omega \notin S_{\text{no}}$, since every string in S_{no} must include at least one "a". Thus

$$S_b \cap S_\emptyset = S_b \cap S_a = S_b \cap S_{\text{no}} = \emptyset,$$

that is, no string in S_b belongs to any of $S_\emptyset$, S_a or S_{no}.

(d) Let $\omega \in S_{\text{no}}$, so that ω includes at least one "a" and at least one "b". Then $\omega \notin S_\emptyset$, since $S_\emptyset \cap S_{\text{no}} = \emptyset$, as noted in the proof of the above condition (a); $\omega \notin S_a$, since $S_a \cap S_{\text{no}} = \emptyset$, as noted in the proof of the above condition (b), and $\omega \notin S_b$, since $S_b \cap S_{\text{no}} = \emptyset$, as noted in the proof of the above condition (c). Thus

$$S_{\text{no}} \cap S_\emptyset = S_{\text{no}} \cap S_a = S_{\text{no}} \cap S_b = \emptyset,$$

that is, no string in S_{no} belongs to any of $S_\emptyset$, S_a, or S_b.

It follows by the above that no string in $\Sigma^\star$ belongs to more than one of $S_\emptyset$, S_a, S_b or S_{no}.

Thus every string in $\Sigma^\star$ belongs to *exactly one* of $S_\emptyset$, S_a, S_b or S_{no}, as claimed. □

Property (b) is easily established by an examination of the set $S_\emptyset$ As shown below, properties (c) and (d) are also reasonably easy to establish.

Lemma 2. *$S_\emptyset \subseteq L$, $S_a \subseteq L$, $S_b \subseteq L$, and $S_{no} \cap L = \emptyset$.*

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 $\omega \in S_\emptyset$. Then it follows by the definition of $S_\emptyset$ that is a string in $\Sigma^\star$ that does not include any a's or b's (so that it is a sequence of zero or more c's). Since

  $$L = \{\omega \in \Sigma^\star \mid \text{either } \omega \text{ does not include an "a" or } \omega \text{ does not include a "b"}\},$$

  and this language includes all the strings in $\Sigma^\star$ that do not include any a's or b's at all, $\omega \in L$. Since ω was arbitrarily chosen from $S_\emptyset$, it follows that $S_\emptyset \subseteq L$.

- Let $\omega \in S_a$. Then it follows by the definition of S_a that ω is a string in $\Sigma^\star$ that does not include any $\mathtt{b}$'s and, once again, this implies that ω is a string in the above language L. Since ω was arbitrarily chosen from S_a it follows that $S_a \subseteq L$.
- The proof that $S_b \subseteq L$ is virtually identical to the proof that $S_a \subseteq L$ — all that is needed is to exchange the roles of the symbols "a" and "b" (and the sets S_a and S_b) in the above argument.
- Finally, let $\omega \in S_{\mathsf{no}}$. Then it follows by the definition of S_{no} that ω includes both an "a" and a "b", and this implies that $\omega \notin L$. Since ω was arbitrarily chosen from S_{no}, it follows that $\omega \notin L$ *for all* $\omega \in S_{\mathsf{no}}$ — that is, $S_{\mathsf{no}} \cap L = \emptyset$, as claimed. □

The proof of property (e) is also straightforward, but somewhat long (because so many relationships must be checked):

Lemma 3. *Each of the conditions included 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 $\omega \in S_\emptyset$ — so that ω does not include any $\mathtt{a}$'s or any $\mathtt{b}$'s. Then the string $\omega \cdot \mathtt{a}$ includes at least one "a" (since it ends with one) but it does not include any $\mathtt{b}$'s; that is, $\omega \cdot \mathtt{a} \in S_a$. Exchanging the role of "a" and "b" in this argument one can see that $\omega \cdot \mathtt{b} \in S_b$. The string $\omega \cdot \mathtt{c}$ does not include any $\mathtt{a}$'s or $\mathtt{b}$'s, since ω does not, so that $\omega \cdot \mathtt{c} \in S_\emptyset$.

  Since ω was arbitrarily chosen from $S_\emptyset$ it follows that

  $$\{\omega \cdot \mathtt{a} \mid \omega \in S_\emptyset\} \subseteq S_a,$$

  $$\{\omega \cdot \mathtt{b} \mid \omega \in S_\emptyset\} \subseteq S_b,$$

  and

  $$\{\omega \cdot \mathtt{c} \mid \omega \in S_\emptyset\} \subseteq S_\emptyset.$$

  That is, conditions (i), (ii) and (iii) all hold.
- Let $\omega \in \Sigma^\star$ such that $\omega \in S_a$ — so that ω includes at least one "a" but ω does not include any $\mathtt{b}$'s. Then the string $\omega \cdot \mathtt{a}$ certainly includes at least one "a" as well, but it does not include any $\mathtt{b}$'s, since ω does not: $\omega \cdot \mathtt{a} \in S_a$. Similarly, the string $\omega \cdot \mathtt{c}$ includes at least one "a" but no $\mathtt{c}$'s, since this is true for ω: $\omega \cdot \mathtt{c} \in S_a$ as well. On the other hand, $\omega \cdot \mathtt{b}$ includes at least one "a", since ω does, and it includes at least one "b" because it ends with this symbol: $\omega \cdot \mathtt{b} \in S_{\mathsf{no}}$.

Since ω was arbitrarily chosen from S_a, it follows that

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

$$\{\omega \cdot \mathsf{b} \mid \omega \in S_a\} \subseteq S_{\mathsf{no}},$$

and

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

That is, conditions (iv), (v) and (vi) are satisfied.

- Applying the above argument again, with the roles of the symbols "a" and "b" (and the sets S_a and S_b) reversed, one can also show that

$$\{\omega \cdot \mathsf{a} \mid \omega \in S_b\} \subseteq S_{\mathsf{no}},$$

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

and

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

That is, conditions (vii), (viii), and (ix) are satisfied

- Let $\omega \in S_{\mathsf{no}}$, so that $\omega \in \Sigma^\star$ and ω includes both an "a" and a "b". Then $\omega \cdot \sigma$ also includes both an "a" and a "b", so that $\omega \cdot \sigma \in S_{\mathsf{no}}$ as well, for any symbol $\sigma \in \Sigma$. Thus $\omega \cdot \mathsf{a} \in S_{\mathsf{no}}$, $\omega \cdot \mathsf{b} \in S_{\mathsf{no}}$, and $\omega \cdot \mathsf{c} \in S_{\mathsf{no}}$. Since ω was arbitrarily chosen from S_{no}, it follows that

$$\{\omega \cdot \mathsf{a} \mid \omega \in S_{\mathsf{no}}\} \subseteq S_{\mathsf{no}},$$

$$\{\omega \cdot \mathsf{b} \mid \omega \in S_{\mathsf{no}}\} \subseteq S_{\mathsf{no}},$$

and

$$\{\omega \cdot \mathsf{c} \mid \omega \in S_{\mathsf{no}}\} \subseteq S_{\mathsf{no}}.$$

That is, conditions (x), (xi) and (xii) are also satisfied, as needed to establish the claim. □

Theorem 4. $L(M) = L$.

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 $L(M) = L$.

- It follows by Lemma 1, above, that property (a) is satisfied.

- Since the empty string λ, does not include any a's or b's (since it has length zero, and does not include any symbols at all), $\lambda \in S_\emptyset$, and property (b) is satisfied.
- Lemma 2 implies that properties (c) and (d) are satisfied.
- Lemma 3 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. □

About This Example

If the "design" part of this exercise was carried out in detail then almost none of the information included in the proof of Theorem 4, or the proofs of the lemmas this proof used, would be new — so that the task of writing the proof is, largely, a task of re-organizing material that has already been obtained, in order to make it is easy as possible for reader to follow the argument that is being presented.[2] Generally, moving from what you know, to what you wish to prove (possibly identifying intermediate goals and working to establish then along the way) is generally advisable.

There is often more than one effective way to organize material, when writing.

It is not always clear *how much* information can be given — what can you safely assume that the reader already knows (so that you do not need to included it)? This is a matter of judgment and depends on who it is you are writing for. I typically give more detail than is strictly necessary, when writing for a large class — because I frequently get asked to supply details, later on, if I initially leave them out.

Every once in a while, a student will write more than is necessary (or is helpful). ***It happens much more frequently that students don't write enough.***

[2] Writing advice that will possibly be given repeatedly, in this course, is as follows: You should always remember that you are writing for another person or group of people — your reader(s). Whenever you can, you should try to consider their needs as you organize the material you are writing.