# Computer Science 313

## Verification of a Deterministic Finite Automaton

Instructor: Wayne Eberly

Department of Computer Science
University of Calgary

Lecture #4

# Goals for Today

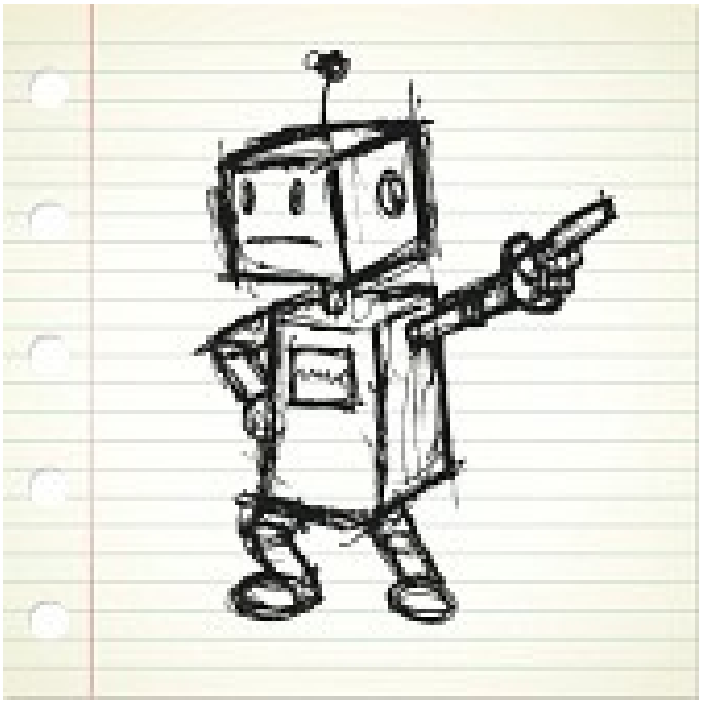
***Goals for Today:***

- Presentation of a technique that can be used to ***prove*** that a given DFA has a given language.
- This will be used to ***prove*** that the one of the deterministic finite automata, developed during the previous lecture, really *does* have the language it is supposed to have.

# Review: A Design Process

The previous lecture included a design process in which you were asked to try to do the following:

## Be the Machine!



# Verification of Correctness of a DFA

***Good News:***

If you followed this design process correctly, in order to design your DFA, then “proving that it is correct” will be pretty easy!

# Verification of Correctness of a DFA

***Not-So-Good News:***

If you “guessed” a DFA or found it by some other means then “proving that is correct” might be difficult (or impossible, because your DFA is actually ***not*** correct).

The easiest way — that I know, to fix this problem — is to ***start again and do this right:*** The “sanity checks” included in the previous lecture are all necessary if you are going to need to prove that your DFA has the language it should.

# Example from the Previous Lecture

In the second example from the previous lecture we considered an alphabet

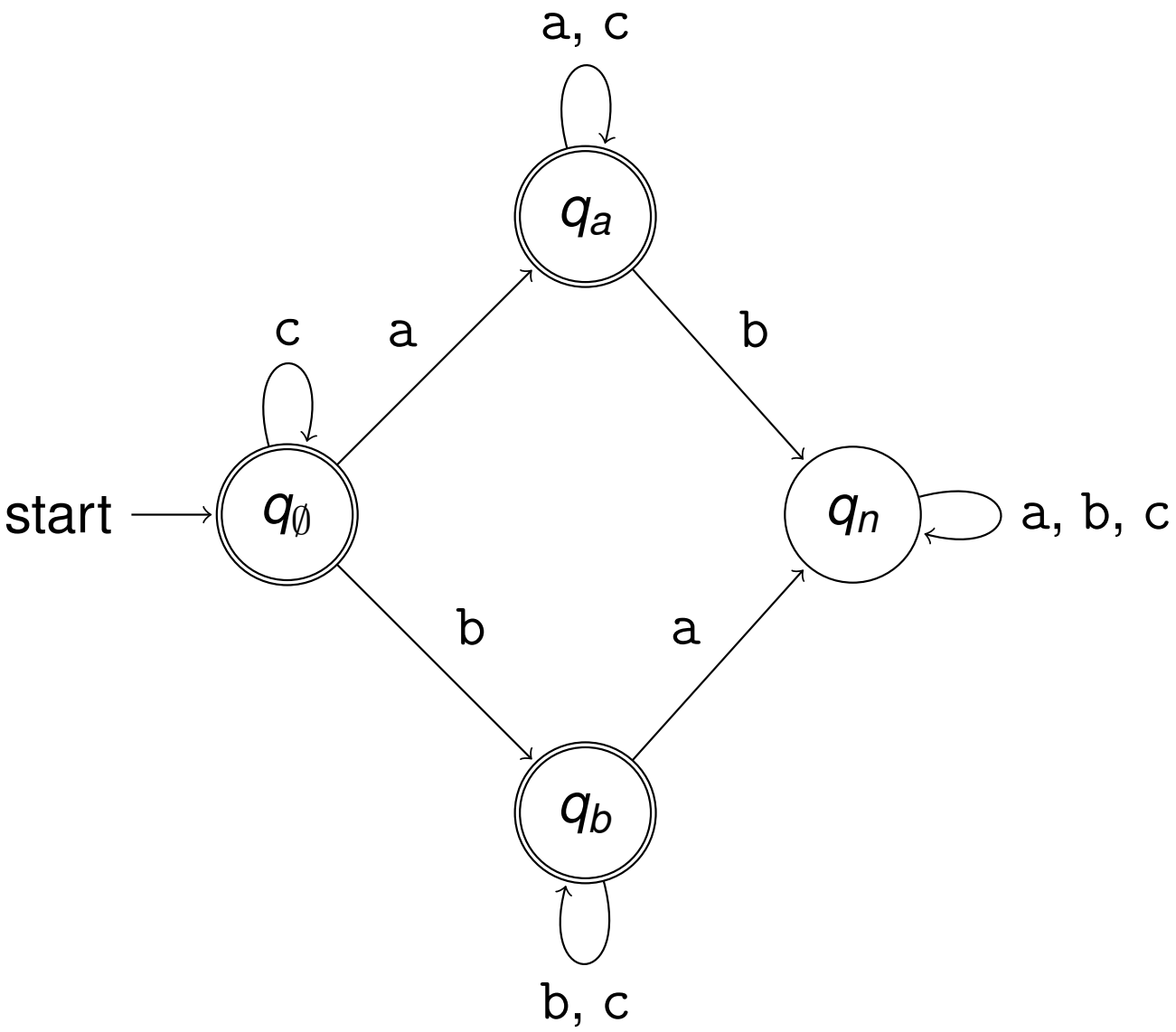
$$\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$$

and the language

$$L_2 = \{\omega \in \Sigma^\star \mid \text{either } \omega \text{ does not include an “a”} \text{ or } \omega \text{ does not include a “b”}\}$$

The DFA, with this this language, developed during the previous lecture is as shown on the following slide.

# Example from the Previous Lecture



# Example from the Previous Lecture

During the design process we identified a subset $S_q \subseteq \Sigma^\star$ with each state $q \in Q$ — in particular, we tried to discover a subset $S_q$ such that, for every string $\omega \in \Sigma^\star$, $\delta^\star(q_0, \omega) = q$ if and only if $\omega \in S_q$.

1. The state $q_\emptyset = q_0$ corresponded to a set $S_\emptyset$. This included all (and only) the strings in $\Sigma^\star$ with no a's or b's, so that

$$S_\emptyset = \{\omega \in \Sigma^\star \mid \omega \text{ only includes c's}\}.$$

2. The state $q_a$ corresponded to the set

$$S_a = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “a” but no b's}\}.$$

# Example from the Previous Lecture

3. The state $q_b$ corresponded to the set

$$S_b = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “b” but no a’s}\}.$$

4. The state $q_n$ corresponded to the set

$$\widehat{S}_{\text{no}} = \{\omega \in \Sigma^\star \mid \omega \text{ includes at least one “a” and at least one “b”}\}.$$

# Step 1: Confirm that *M* is a DFA with the Required Alphabet

This process begins by confirming that *M* really *is* a well-defined deterministic finite automaton whose alphabet is $\Sigma$ — so that the language of *M* is *some* subset of $\Sigma^\star$.

This is part is reasonably easy — but also necessary.

# Step 1: Confirm that $M$ is a DFA with the Required Alphabet

Given a language $L \subseteq \Sigma^\star$ and a deterministic finite automaton

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

1. Confirm that $Q$ is a finite set (of "states").
2. Confirm that $\Sigma$ is another finite set — an "alphabet"' — and that the given language $L$ has been defined to be a subset of $\Sigma^\star$, for the ***same*** alphabet $\Sigma$.
3. Confirm that $q_0 \in Q$.
4. Confirm that $F \subseteq Q$.
5. Confirm that $\delta$ is a ***well-defined total*** function from $Q \times \Sigma$ to $Q$.

Then you may conclude that $M$ *is* a DFA whose language is *some* subset of $\Sigma^\star$.

# Application to the Example

1. One can see by the examination of $M$ (as shown on picture of $M$ given earlier on) that

$$Q = \{q_\emptyset, q_a, q_b, q_n\}$$

   is a finite set (of "states"), as required.
2. One can also see that the alphabet of $M$ is the finite set

$$\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$$

   — and that the language $L$ is defined as a subset of $\Sigma^\star$, for the same alphabet $\Sigma$.

# Application to the Example

3. One can see by an inspection of the picture that the start state, $q_\emptyset$, belongs to the set $Q$ of states that has now been defined.
4. One can also see, by an inspection of the picture of $M$, is that the set $F$ of accepting states is

$$F = \{q_\emptyset, q_a, q_b\}$$

— which is a subset of $Q$.

# Application to the Example

5. Finally, $\delta$ is a well-defined total function from $Q \times \Sigma$ to $Q$. To see that this is the case note (after examining the picture of $M$) that $\delta$ is given by the following table — whose rows are indexed by each of the states in $Q$ and whose columns are indexed by each of the symbols in $\Sigma$. Each cell of this table includes exactly one state in $Q$, as required:

| | a | b | c |
|---|---|---|---|
| $q_\emptyset$ | $q_a$ | $q_b$ | $q_\emptyset$ |
| $q_a$ | $q_a$ | $q_n$ | $q_a$ |
| $q_b$ | $q_n$ | $q_b$ | $q_b$ |
| $q_n$ | $q_n$ | $q_n$ | $q_n$ |

***Conclusion:*** $M$ is a DFA whose a language is a subset of $\Sigma^\star$, and $L$ has been defined as a subset of $\Sigma^\star$ for the same alphabet $\Sigma$.

# Step 2: Complete the Proof of Correctness

The process continues by confirming that this DFA really *does* have the desired language.

- A ***useful result*** — which is stated next and proved in the supplemental document for this lecture — establishes that if you designed this DFA using the design process described in the previous lecture, and confirmed that all of the "sanity checks" included in this process were passed, then most of the hard work has already been done.
- ***This is an advantage of "design processes":*** Following them really can make it easier to confirm that your solution for a problem is correct.

# Step 2: Apply a Useful Result

*If* you have not already done so...

6. Identify a subset $S_q$ of $\Sigma^\star$ for each state $q$ of $Q$.
7. Confirm that every string $\omega \in \Sigma^\star$ belongs to $S_q$ for ***exactly one*** of the states $q \in Q$.
8. Confirm that $\lambda \in S_{q_0}$, where $S_{q_0}$ is the subset of $\Sigma^\star$ corresponding to the start state, $q_0$, of $M$.
9. Confirm that

$$\{\omega \cdot \sigma \mid \omega \in S_q\} \subseteq S_{\delta(q,\sigma)}$$

   for every state $q \in Q$ and for every symbol $\sigma \in \Sigma$.
10. *Apply* the result, shown in the following frame, to conclude that

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

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

# A Useful Result

***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 $\omega \in S_q$.

As previously noted, the proof of this “useful result” is given in the supplemental document for this lecture.

# Application to the Example

6. Consider the following subsets of $\Sigma^\star$ — which correspond to (each one of) the states $q_\emptyset$, $q_a$, $q_b$ and $q_n$ of $Q$:
   - $S_{q_\emptyset} = S_\emptyset = \{\omega \in \Sigma^\star \mid \omega$ only includes c's$\}$
   - $S_{q_a} = S_a = \{\omega \in \Sigma^\star \mid \omega$ includes at least one "a" but no b's$\}$
   - $S_{q_b} = S_b = \{\omega \in \Sigma^\star \mid \omega$ includes at least one "b" but no a's$\}$
   - $S_{q_n} = S_n = \{\omega \in \Sigma^\star \mid$ $\omega$ includes at least one "a" and at least one "b"$\}$
7. Since $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, every string $\omega \in \Sigma^\star$ belongs to exactly one of the above subsets $S_{q_\emptyset}$, $S_{q_a}$, $S_{q_b}$ and $S_{q_n}$.
8. Since the empty string $\lambda$ does not include any a's or b's, $\lambda \in S_{q_\emptyset}$ — as required, since $S_{q_\emptyset}$ corresponds to the start state $q_\emptyset$ of $M$.

# Application to the Example

9. Let $q \in Q$. Then either $q = q_\emptyset$, $q = q_a$, $q = q_b$, or $q = q_n$. These cases will be considered separately.

   *Case:* $q = q_\emptyset$.Then if $\omega \in S_q = S_{q_\emptyset}$ then $\omega$ does not include any a's or b's, so that it only includes c's.

   Now let $\sigma \in \Sigma$. Then either $\sigma = \mathtt{a}$, $\sigma = \mathtt{b}$, or $\sigma = \mathtt{c}$. These will be considered in separate subcases.

   *Subcase:* $\sigma = \mathtt{a}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{a}$. Since $\omega$ does not include any a's or b's, $\omega \cdot \mathtt{a}$ includes an "a" but no b's — so that $\omega \cdot \mathtt{a} \in S_{q_a}$. Since $\delta(q, \sigma) = \delta(q_\emptyset, \mathtt{a}) = q_a$ it follows that $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as claimed.

# Application to the Example

*Subcase:* $\sigma = \mathtt{b}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{b}$. Since $\omega$ does not include any a's or b's, $\omega \cdot \mathtt{b}$ includes a "b" but no a's — so that $\omega \cdot \mathtt{b} \in S_{q_b}$. Since $\delta(q, \sigma) = \delta(q_\emptyset, \mathtt{b}) = q_b$ it follows that $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as claimed.

*Subcase:* $\sigma = \mathtt{c}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{c}$. Since $\omega$ does not include any a's or b's, $\omega \cdot \mathtt{c}$ does not include any a's or b's, either — so that $\omega \cdot \mathtt{c} \in S_{q_\emptyset}$. Since $\delta(q, \sigma) = \delta(q_\emptyset, \mathtt{c}) = q_\emptyset$ it follows that $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as claimed, once again.

# Application to the Example

*Case:* $q = q_a$. Then if $\omega \in S_q = S_{q_a}$ then $\omega$ includes at least one "a" but no b's.

Let $\sigma \in \Sigma$. Then, once again, either $\sigma = \mathtt{a}$, $\sigma = \mathtt{b}$, or $\sigma = \mathtt{c}$. Once again, each is considered as a separate subcase.

*Subcase:* $\sigma = \mathtt{a}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{a}$, so that $\omega \cdot \sigma$ also includes at least one "a" but no b's, so that $\omega \cdot \sigma \in S_{q_a}$ as well. Since $\delta(q, \sigma) = \delta(q_a, \mathtt{a}) = q_a$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as required.

# Application to the Example

*Subcase:* $\sigma = \mathtt{b}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{b}$, so that $\omega \cdot \sigma$ includes both an "a" and a "b", and $\omega \cdot \sigma \in S_{q_n}$. Since $\delta(q, \sigma) = \delta(q_a, \mathtt{b}) = q_n$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as required.

*Subcase:* $\sigma = \mathtt{c}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{c}$, so that $\omega \cdot \sigma$ also includes at least one "a" but no b's, and thus $\omega \cdot \sigma \in S_{q_a}$. Since $\delta(q, \sigma) = \delta(q_a, \mathtt{c}) = q_a$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, once again.

# Application to the Example

*Case:* $q = q_b$. Then if $\omega \in S_q = S_{q_b}$ then $\omega$ includes at least one "b" but no a's.

Let $\sigma \in \Sigma$. Then, once again, either $\sigma = \mathtt{a}$, $\sigma = \mathtt{b}$, or $\sigma = \mathtt{c}$. Once again, each is considered as a separate subcase.

*Subcase:* $\sigma = \mathtt{a}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{a}$, so that $\omega \cdot \sigma$ includes both an "a" and a "b", and $\omega \cdot \sigma \in S_{q_n}$. Since $\delta(q, \sigma) = \delta(q_b, \mathtt{a}) = q_n$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as required.

# Application to the Example

*Subcase:* $\sigma = \mathtt{b}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{b}$, so that $\omega \cdot \sigma$ also includes at least one "b" but no a's, so that $\omega \cdot \sigma \in S_{q_b}$ as well. Since $\delta(q, \sigma) = \delta(q_b, \mathtt{b}) = q_b$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, as required.

*Subcase:* $\sigma = \mathtt{c}$. Then $\omega \cdot \sigma = \omega \cdot \mathtt{c}$, so that $\omega \cdot \sigma$ also includes at least one "b" but no a's, and thus $\omega \cdot \sigma \in S_{q_b}$. Since $\delta(q, \sigma) = \delta(q_b, \mathtt{c}) = q_b$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case, once again.

# Application to the Example

*Case:* $q = q_n$. Then if $\omega \in S_q = S_{q_n}$ then $\omega$ includes at least one "a" and at least one "b".

Let $\sigma \in \Sigma$. Then $\omega \cdot \sigma$ also includes at least one "a" and at least one "b", so that $\omega \cdot \sigma \in S_{q_n}$. Since $\delta(q_n, \sigma) = q_n$, it follows that $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$ in this case too.

It follows that for every state $q \in Q$, every string $\omega \in S_q$ and every symbol $\sigma \in \Sigma$, $\omega \cdot \sigma \in S_{\delta(q,\sigma)}$. In other words

$$\{\omega \cdot \sigma \mid \omega \in S_q\} \subseteq S_{\delta(q,\sigma)}$$

for every state $q \in Q$ and every symbol $\sigma \in \Sigma$, as desired.

# Application to the Example

10. All the conditions included in Theorem #1 have now been verified. It now follows by an application of this result that
    - $\delta^\star(q_\emptyset, \omega) = q_\emptyset$ for every string $\omega \in S_{q_\emptyset} = S_\emptyset$,
    - $\delta^\star(q_\emptyset, \omega) = q_a$ for every string $\omega \in S_{q_a} = S_a$,
    - $\delta^\star(q_\emptyset, \omega) = q_b$ for every string $\omega \in S_{q_b} = S_b$, and
    - $\delta^\star(q_\emptyset, \omega) = q_n$ for every string $\omega \in S_{q_n} = S_n$.

# Step 3: Compare the Languages That Have Now Been Identified

11. Finally, confirm that

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

You may then conclude that the language of $M$ is $L$ — for you have now ***proved*** this.

# Application to the Example

11. Since $F = \{q_\emptyset, q_a, q_b\}$, the set

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

is equal to the union of the sets

- $S_{q_\emptyset} = S_\emptyset = \{\omega \in \Sigma^\star \mid$ $\omega$ does not include any a's or b's$\}$,
- $S_{q_a} = S_a = \{\omega \in \Sigma^\star \mid$ $\omega$ includes at least one "a" but no b's$\}$, and
- $S_{q_b} = S_b = \{\omega \in \Sigma^\star \mid$ $\omega$ includes at least one "b" but no a's$\}$.

This set is equal to the language

$$L_2 = \{\omega \in \Sigma^\star \mid \text{either } \omega \text{ does not include an "a" or } \omega \text{ does not include a "b"}\}$$

Therefore, $L(M) = L_2$, as desired.