COMPSCI/SFWRENG 2FA3
Discrete Mathematics with Applications II
Winter 2020

Week 07 Exercises

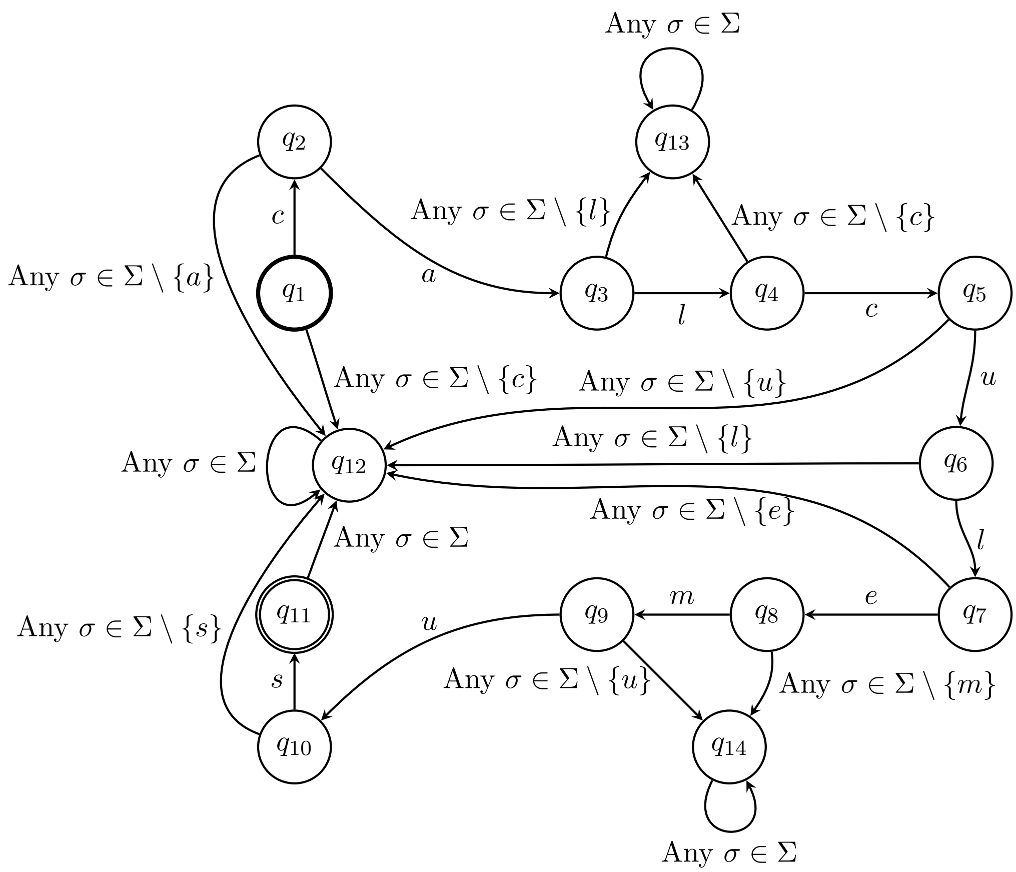
Dr. William M. Farmer
McMaster University

Revised: February 14, 2020

Exercises

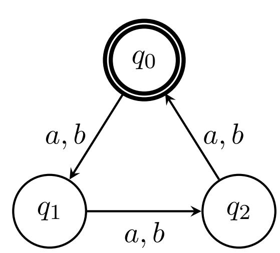
1. Construct deterministic finite automata $M = (Q, \Sigma, \delta, s, F)$ such that:

   a. $\Sigma = \{a, b, \ldots, z\}$ and $L(M)$ contains the single string *calculemus*.
   SOLUTION: Let M be the DFA to match $L(M)$, where δ is illustrated by the below transition diagram:

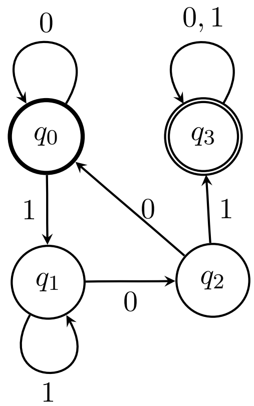


We've used the notation "Any $\sigma \in \Sigma$" to denote any member of the alphabet, to save space. We've also added some extra states (q_{13}, q_{14}), which were unnecessary, but makes the diagram easier to read.

b. $\Sigma = \{a, b\}$ and $L(M) = \{x \in \Sigma^* \mid |x| \equiv 0 \bmod 3\}$.
SOLUTION: Let M be the appropriate DFA with the following transition diagram:

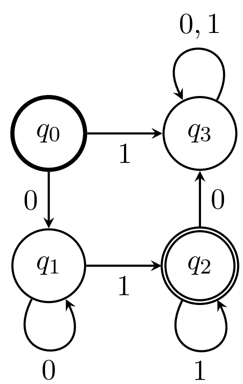


c. $\Sigma = \{0, 1\}$ and $L(M) = \{x \in \Sigma^* \mid x \text{ contains the string } 101\}$
SOLUTION: Let the appropriately defined DFA M have the following transition diagram:



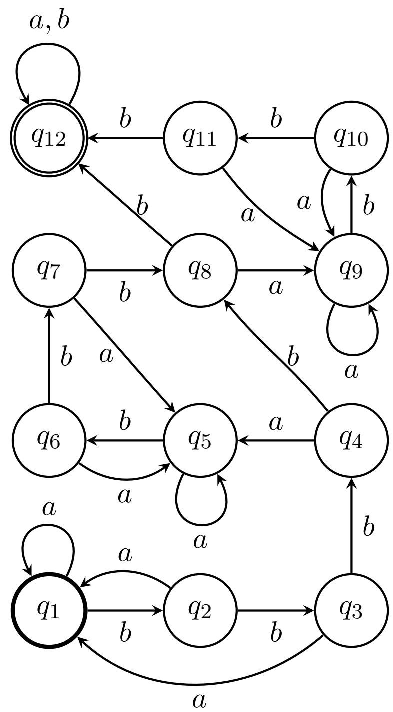
d. $\Sigma = \{0, 1\}$ and $L(M)$ is set of strings in Σ^* of the form $0^m 1^n$ where $m, n \geq 1$.

SOLUTION: Let M be the DFA with the following transition diagram:

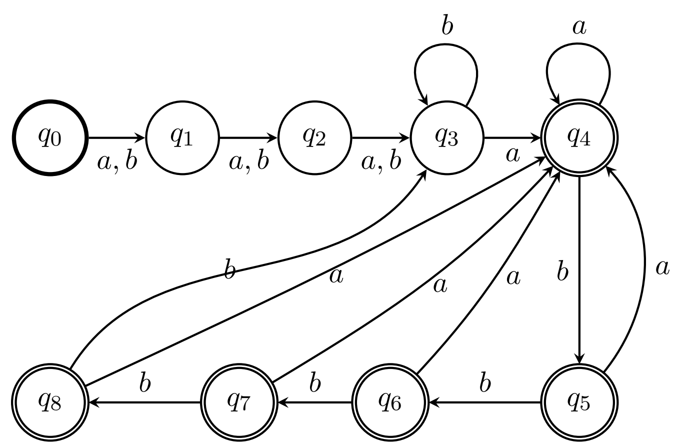


e. $\Sigma = \{a, b\}$ and $L(M)$ is the set of strings in Σ^* that contain at least three occurrences of bbb. Note: Overlapping is permitted so $bbbbb \in L(M)$.

SOLUTION: Let M be the DFA with the following transition diagram:



f. $\Sigma = \{a, b\}$ and $L(M) = \{x_1 a x_2 \mid |x_1| \geq 3 \text{ and } |x_2| \leq 4\}$.
SOLUTION: Let M be the DFA with the following transition diagram:



2. Let $M = (Q, \Sigma, \delta, s, F)$ and $M' = (Q, \Sigma, \delta, s, \{q \in Q \mid q \notin F\})$ be DFAs. Prove that $L(M') = {\sim}L(M)$.

Proof. We begin by noting the definition of the languages:

$$
\begin{aligned}
L(M') &= \{x \in \Sigma^* \mid \hat{\delta}(s, x) \in \{q \in Q \mid q \notin F\}\} \\
{\sim}L(M) &= {\sim}\{x \in \Sigma^* \mid \hat{\delta}(s, x) \in F\}
\end{aligned}
$$

Then, we have

$$\begin{aligned}
L(M') &= \{x \in \Sigma^* \mid \hat{\delta}(s,x) \in \{q \in Q \mid q \notin F\}\} && \langle \text{Definition of } L(M') \rangle \\
&= \{x \in \Sigma^* \mid \hat{\delta}(s,x) \in {\sim}F\} && \langle \text{Set complement} \rangle \\
&= \{x \in \Sigma^* \mid \hat{\delta}(s,x) \notin F\} && \langle \text{Membership of complement} \rangle \\
&= {\sim}\{x \in \Sigma^* \mid \hat{\delta}(s,x) \in F\} && \langle \text{Set complement} \rangle \\
&= {\sim}L(M) && \langle \text{Definition of } {\sim}L(M) \rangle
\end{aligned}$$

as required. □

3. Let Σ be a finite alphabet and $B \subseteq \Sigma^*$. B is *reflexive* if $\epsilon \in B$ and is *transitive* if $BB \subseteq B$. Prove that, if $A \subseteq \Sigma^*$, then A^* is smallest reflexive and transitive set containing A. That is, show that (1) $A \subseteq A^*$, (2) A^* is reflexive, (3) A^* is transitive, and (4) if B is any other reflexive and transitive set containing A, then $A^* \subseteq B$.

   Proof. We begin by noting the definition of A^*:

   $$A^* = \bigcup_{n \geq 0} A^n = A^0 \cup A^1 \cup A^2 \cup \cdots$$

   From this, we know that $A \subseteq A^*$, as A appears in the iterated union of A^*.

   Also, we know that $A^0 = \{\epsilon\}$. Thus, $\epsilon \in A^*$, so A^* is reflexive.

   Since A^* is the set of all possible strings buildable from strings in A, we have that $A^*A^* \subseteq A^*$. We can show this by building an injective map $f : A^*A^* \to A^*$. For any member from the domain (A^*A^*), we can map it to a unique member of the codomain (A^*). The member of the codomain must have the form xy where $x, y \in A^*$. Furthermore, x must come from A^n for some appropriate $n \in \mathbb{N}$. y must similarly come from A^m for some appropriate $m \in \mathbb{N}$. Yet, $xy \in A^{n+m} \subseteq A^*$, so we must have that $A^*A^* \subseteq A^*$, so A^* is transitive.

   We know $A^* \subseteq B$ if for any string $x \in A^*$, we have that $x \in B$. For any $x \in A^*$, we can write it as a concatenation of strings $x_1x_2x_3 \dots x_\ell$ where $x_1, x_2, x_3, \dots x_\ell \in A$. We can do a proof by induction on ℓ to show that $x \in B$.

   Proof. Base case: $\ell = 0$. i.e. $x = \epsilon$. B is reflexive, so $\epsilon \in B$.

   Induction Step: Assume that if $x_1, x_2, \dots, x_\ell \in A^\ell$, then $x_1x_2 \dots x_\ell \in B$. So, for any string $x_1, x_2, \dots, x_{\ell+1} \in A^*$, we know that $x_1, x_2, \dots, x_{\ell+1} \in A^\ell A$. We also know from the induction hypothesis that $A^\ell \subseteq B$ and we know from the question that $A \subseteq B$. Therefore, $x_1, x_2, \dots, x_{\ell+1} \subseteq BB$ □

   Thus, $A^* \subseteq B$, as required. □

4. Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA. Prove by induction on $|y|$ that, for all $x, y \in \Sigma^*$ and $q \in Q$,

$$\hat{\delta}(q, xy) = \hat{\delta}(\hat{\delta}(q, x), y).$$

Proof. Let $P(y) \equiv \hat{\delta}(q, xy) = \hat{\delta}(\hat{\delta}(q, x), y)$. We will prove $P(y)$ by induction over $|y|$, for any state $q \in Q$ and $x \in \Sigma^*$.

Base case: $|y| = 0$, i.e. $y = \epsilon$.

$$\begin{aligned}
P(\epsilon) &\equiv \hat{\delta}(\hat{\delta}(q, x), \epsilon) && \langle \text{Definition of } P \rangle \\
&= \hat{\delta}(q, x) && \langle \text{Definition of } \hat{\delta} \rangle \\
&= \hat{\delta}(q, x\epsilon) && \langle \text{Identity of concatenation} \rangle
\end{aligned}$$

Induction step: Assume $P(y)$. Show that, for any $\sigma \in \Sigma$, we have $P(y\sigma)$.

$$\begin{aligned}
P(y\sigma) &\equiv \hat{\delta}(\hat{\delta}(q, x), y\sigma) && \langle \text{Definition of } P \rangle \\
&= \delta(\hat{\delta}(\hat{\delta}(q, x), y), \sigma) && \langle \text{Definition of } \hat{\delta} \rangle \\
&= \delta(\hat{\delta}(q, xy), \sigma) && \langle \text{Induction hypothesis} \rangle \\
&= \hat{\delta}(q, xy\sigma) && \langle \text{Definition of } \hat{\delta} \rangle
\end{aligned}$$

Thus, by induction over $|y|$, we have that P holds for all $x, y \in \Sigma^*$ and $q \in Q$, as required. $\square$