- Start as early as possible, and contact the instructor if you get stuck.
- See the course outline for details about the course's marking policy and rules on collaboration.
- Submit your completed solutions to **Crowdmark**.

1. **Definition 1** *Let X and Y be sets. Then the* ***intersection of X and Y, denoted*** *$X \cap Y$, is the set of elements of both X and Y:*

$$X \cap Y = \{z \mid z \in X \text{ and } z \in Y\}.$$

Definition 2 *Let X and Y be sets. Then the* ***union of X and Y, denoted*** *$X \cup Y$, is the set of elements of either X or Y (or both):*

$$X \cup Y = \{z \mid z \in X \text{ or } z \in Y, \text{ or both}\}.$$

Definition 3 *Let X and Y be sets. Then Y* ***is a subset of X, denoted*** *$Y \subseteq X$, if and only if every element of Y is also an element of X.*

Definition 4 *Let X be a set. Then the* ***power set of X, denoted*** *$P(X)$, is defined to be the set of subsets of X. In other words, $Y \in P(X)$ if and only if $Y \subseteq X$.*

[6] (a) Let E and F be sets. Prove that $P(E) \cap P(F) = P(E \cap F)$.

If we assume

$$A \in P(E \cap F)$$

by the **power set** and **intersection** definitions,

$$\begin{aligned} &A \subseteq E \cap F \\ &A \subseteq E \wedge A \subseteq F \\ &A \in P(E) \wedge A \in P(F) \\ &A \in P(E) \cap P(F) \end{aligned} \tag{1}$$

Since we assumed $A \in P(E \cap F)$ and have shown $A \in P(E) \cap P(F)$

$$P(E \cap F) \subseteq P(E) \cap P(F)$$

Using the same method we now assume,

$$A \in P(E) \cap P(F)$$

Then,

$$\begin{aligned} &A \in P(E) \wedge A \in P(F) \\ &A \subseteq E \wedge A \subseteq F \\ &A \subseteq E \cap F \\ &A \in P(E \cap F) \end{aligned} \tag{2}$$

Which shows that $P(E) \cap P(F) \subseteq P(E \cap F)$. Since we have already shown $P(E \cap F) \subseteq P(E) \cap P(F)$ we now have proven,

$$P(E) \cap P(F) = P(E \cap F)$$

  rdmoroun@uwaterloo.ca

[3] (b) Let E and F be sets. Prove that $P(E) \cup P(F) \subseteq P(E \cup F)$.

Let $G \in P(E) \cup P(F)$ then using the **power set** and **union** definitions we need to show $G \in P(E \cup F)$.

$$\begin{aligned} &G \in P(E) \cup P(F) \\ &G \subseteq E \vee G \subseteq F \\ &G \subseteq E \cup G \\ &G \in P(E \cup F) \end{aligned} \tag{3}$$

Since we have shown that for an arbitrary $G \in P(E) \cup P(F)$ and G is also an element of $P(E \cup F)$. We have proven $P(E) \cup P(F) \subseteq P(E \cup F)$.

[3] (c) Give an example of finite sets E and F such that $P(E \cup F) \not\subseteq P(E) \cup P(F)$. Briefly explain why your choice of E and F is correct.

Proof by counter-example

$$\begin{aligned}
\text{Let} \quad E &= \{a\} \\
F &= \{b\} \\
\text{Then,} \quad P(E) &= \{\emptyset, \{a\}\} \\
P(F) &= \{\emptyset, \{b\}\} \\
P(E \cup F) &= \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \\
P(E) \cup P(F) &= \{\emptyset, \{a\}, \{b\}\} \\
\because P(E) \cup P(F) &\neq P(E \cup F) \\
\therefore P(E \cup F) &\not\subseteq P(E) \cup P(F)
\end{aligned} \tag{4}$$

[3] 2. Let $\Sigma^* = \{0, 1\}$. Let L be the language, over Σ^*, or words having at least two different substrings, each of length 2. For example,

- $010 \in L$, because it contains the substrings 01 and 10, and
- $000 \notin L$, because its only substring of length 2 is 00.

Describe L by writing a sentence of the form

$$L = \{w \in \Sigma^* \quad | \quad P(w)\},$$

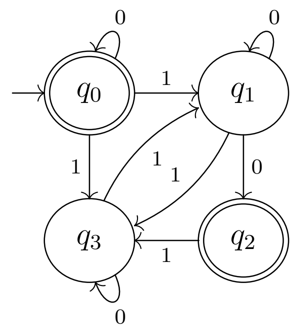
where $P(w)$ is a first-order logic formula. In $P(w)$, you may use the notation

- $|x|$ to return the length of any string x,
- standard arithmetic relations $=, \neq, <, \leq$, etc.,
- standard arithmetic constants $0, 1, 2$, etc., and
- the relation $Substr(u, v)$, which is true if and only if u is a substring of v.

$$L = \{w \in \Sigma^* \quad | \quad P(w)\},$$

$$\begin{aligned} P(w) \to \exists x \exists y \ &: |x| = 2 \\ &\wedge |y| = 2 \\ &\wedge Substr(x, w) \\ &\wedge Substr(y, w) \\ &\wedge x \neq y \end{aligned} \tag{5}$$

3. Consider the NFA, M, having alphabet $\Sigma^* = \{0, 1\}$ and defined by the following diagram.



For each choice of input word w given below, determine whether or not $w \in L(M)$. Briefly justify each answer.

[3] (a) $w = 101$

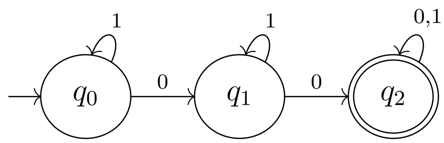
$$\begin{aligned}
w \in L(M) &\implies \hat{\delta}(q_0, w) \cap F \neq \emptyset \\
\hat{\delta}(q_0, w) &= \hat{\delta}(q_0, 101) \\
&= \delta(\hat{\delta}(q_0, 10), 1) \\
&= \delta(\delta(\delta(q_0, 1), 0), 0) \\
\delta(q_0, 1) &= \{q_1, q_3\} \\
\delta(\{q_1, q_3\}, 0) &= \delta(q_1, 0) \cup \delta(q_3, 0) \\
\delta(q_1, 0) &= \{q_1, q_2\} \\
\delta(q_3, 0) &= \{q_3\} \\
\delta(\{q_1, q_3\}, 0) &= \{q_1, q_2, q_3\} \\
\delta(\{q_1, q_2, q_3\}, 1) &= \delta(q_1, 1) \cup \delta(q_2, 1) \cup \delta(q_3, 1) \\
\delta(q_1, 1) &= \{q_3\} \\
\delta(q_2, 1) &= \{q_3\} \\
\delta(q_3, 1) &= \{q_1\} \\
\delta(\{q_1, q_2, q_3\}, 1) &= \{q_1, q_3\} \\
\hat{\delta}(q_0, 101) &= \{q_1, q_3\} \\
F &= \{q_0, q_2\} \\
&\because \hat{\delta}(q_0, 101) \cap F = \emptyset \\
&\therefore w \notin L(M)
\end{aligned} \tag{6}$$

[3] (b) $w = 1010$

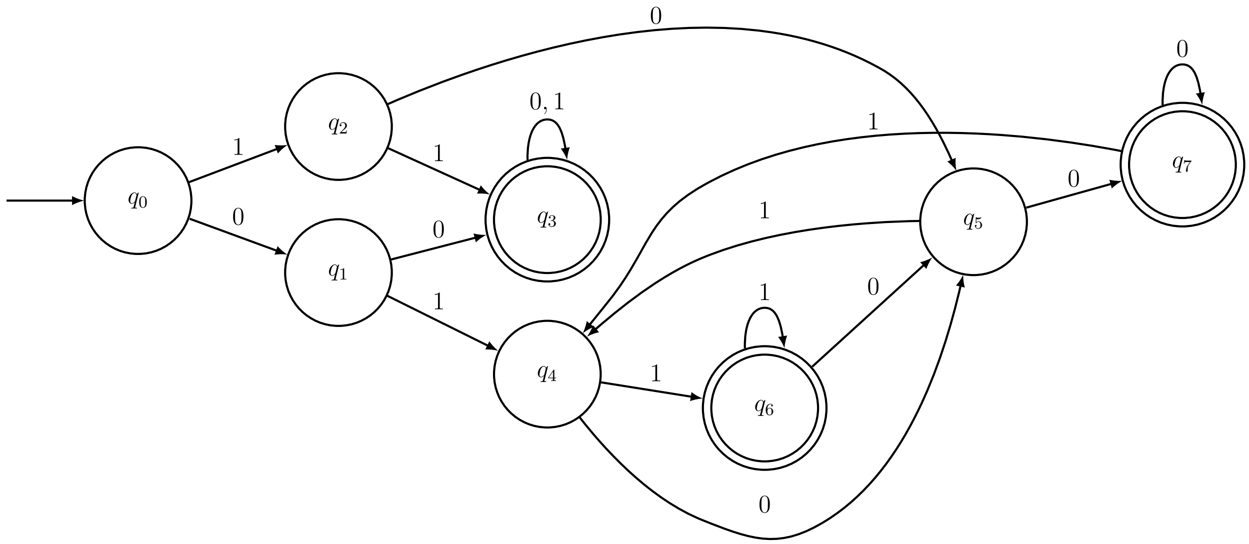
$$\begin{aligned} w \in L(M) &\implies \hat{\delta}(q_0, w) \cap F \neq \emptyset \\ \hat{\delta}(q_0, w) &= \hat{\delta}(q_0, 1010) \\ &= \delta(\hat{\delta}(q_0, 101), 0) \\ \hat{\delta}(q_0, 101) &= \{q_1, q_3\} \quad \text{FROM PART (a)} \\ \delta(\{q_1, q_3\}, 0) &= \delta(q_1, 0) \cup \delta(q_3, 0) \\ \delta(q_1, 0) &= \{q_1, q_2\} \\ \delta(q_3, 0) &= \{q_3\} \\ \delta(\{q_1, q_3\}, 0) &= \{q_1, q_2, q_3\} \\ &\because \hat{\delta}(q_0, 1010) \cap F = \{q_2\} \\ &\therefore w \in L(M) \end{aligned} \tag{7}$$

4. Draw the diagram of a DFA, NFA or ε-NFA which accepts each of the following languages over $\Sigma^* = \{0, 1\}$, and argue informally why your automaton accepts exactly the language given.

[4] (a) $L_a = \{w \in \Sigma^* \mid n_0(w) \geq 2\}$. Recall that $n_0(w)$ denotes the number of occurrences of the symbol 0 in the string w.



Letting $w = \epsilon$ we begin at state q_0. From state q_0 we can see $\delta(q_0, 1) = q_0$ and $\delta(q_0, 0) = q_1$ so any addition of a 1 to w will keep us in this state where $n_0(w) = 0$. Only by adding a 0 to w can we move to state q_1. Once in q_1 we have $n_0(w) = 1$ and once again adding any additional 1 symbols to w keeps us in state q_1 as seen by $\delta(q_1, 1) = q_1$. Similarly, only by adding a 0 symbol to w can we progress to the final state q_2. $\delta(q_1, 0) = q_2$. Once in state q_2 we are at the point where $n_0(w) = 2$ since only the 2 additions of 0 symbols to $w = \epsilon$ could bring us to this state. In state q_2, $\delta(q_2, 0) = q_2$ and $\delta(q_2, 1) = q_2$. Since we know there are at least 2 0 symbols at state q_2 and any addition of 0s keeps us in q_2 we see $n_0(w) \geq 2$ in state q_2. Because $q_2 \in F$ we can be confident that the above diagram accepts exactly the language $L_a = \{w \in \Sigma^* \mid n_0(w) \geq 2\}$.



[4] (b) $L_b = \{w \in \Sigma^* \mid w \text{ begins or ends with 00 or 11}\}$.

To argue the above diagram accepts exactly the language described by L_b we first consider the case where w either starts with 00 or with 11. When w starts with 00 $\hat{\delta}(q_0, 00) = \delta(\delta(q_0, 0), 0) = q_3$ Similarly for w starting with 11 $\hat{\delta}(q_0, 11) = \delta(\delta(q_1, 1), 1) = q_3$

At q_3 any additional symbol additions will keep L_b in q_3 which is correct since $q_3 \in F$.

Next we consider the case where w does not start with 00 or 11. This means that either w starts with 01 or 10.
For w =01 $\hat{\delta}(q_0, 01) = \delta(\delta(q_0, 0), 1) = q_4$. Then for w =10 $\hat{\delta}(q_0, 10) = \delta(\delta(q_0, 1), 0) = q_5$.

From q_4 or q_5 there is no path to q_3 so the final cases must be considered where w ends with either 00 or 01.

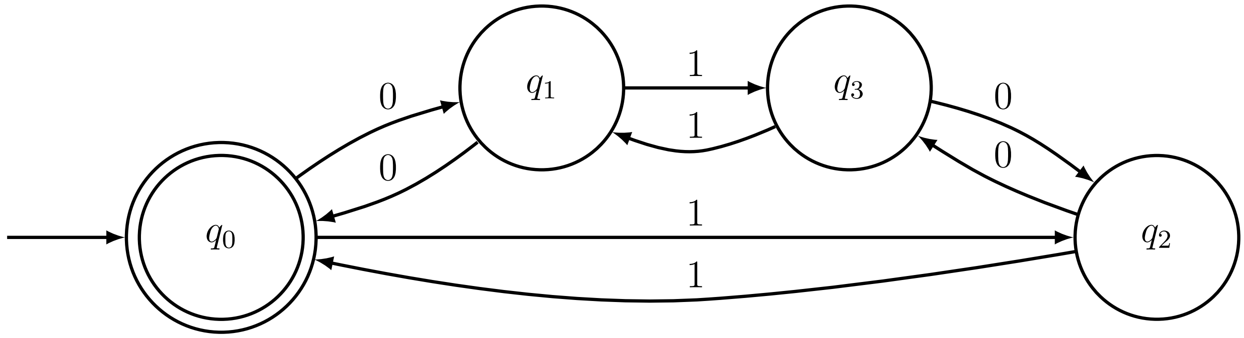
At state q_4 we have just read a 1 so an additional 1 will give us a string with a potential 11 ending $\delta(q_4, 1) = q_6$. Conversely, reading a 0 will take us to state q_5.

At state q_5 we have just read a 0 so an additional 0 will give us a string with a potential 00 ending $\delta(q_4, 1) = q_6$. Conversely, reading a 1 will take us to state q_4 (discussed above).

At state q_6 we have just read two consecutive 1s. Any additional 1s read in this state will not change the state and $q_6 \in F$. However the addition of a 0 will take us to state q_5 which we have discussed above.

At state q_7 we have just read two consecutive 0s. Any additional 0s read in this state will not change the state and $q_7 \in F$. However the addition of a 1 will take us to state q_4 which we have discussed above.

As we cycle through the 8 states of the diagram it is clear that only in states:
q_3 The string must start with a 00 or a 11.
q_6 The string must end with a 11.
q_7 The string must end with a 00.
Since $F = \{q_3, q_6, q_7\}$ the language defined as L_b exactly accepts strings which begin or end with 00 or 11.



[4] (c) $L_c = \{w \in \Sigma^* \mid n_0(w) \equiv 0 \bmod 2 \text{ and } n_1(w) \equiv 0 \bmod 2\}$.

Given the predicate $n_0(w) \equiv 0 \bmod 2$ and $n_1(w) \equiv 0 \bmod 2$ combined with the fact $|\Sigma| = 2$ we can surmise that the addition of any symbol from Σ to w can lead to $2^2 = 4$ possible states:

q_0 Where, $n_0(w) \equiv 0 \bmod 2$ and $n_1(w) \equiv 0 \bmod 2$
q_1 Where, $n_0(w) \equiv 1 \bmod 2$ and $n_1(w) \equiv 0 \bmod 2$
q_2 Where, $n_0(w) \equiv 0 \bmod 2$ and $n_1(w) \equiv 1 \bmod 2$
q_3 Where, $n_0(w) \equiv 1 \bmod 2$ and $n_1(w) \equiv 1 \bmod 2$

Because $|\Sigma| = 2$ and the above diagram is a DFA each state has 2 transitions $\delta(q, 0)$ and $\delta(q, 1)$ for some $q \in Q$.

q_0 When a 0 is read $n_0(w) mod 2$ changes from 0 to 1 $\delta(q_0, 0) = q_1$
q_0 When a 1 is read $n_1(w) mod 2$ changes from 0 to 1 $\delta(q_0, 1) = q_2$
q_1 When a 0 is read $n_0(w) mod 2$ changes from 1 to 0 $\delta(q_1, 0) = q_0$
q_1 When a 1 is read $n_1(w) mod 2$ changes from 0 to 1 $\delta(q_1, 1) = q_3$
q_2 When a 0 is read $n_0(w) mod 2$ changes from 0 to 1 $\delta(q_2, 0) = q_3$
q_2 When a 1 is read $n_1(w) mod 2$ changes from 1 to 0 $\delta(q_2, 1) = q_0$
q_3 When a 0 is read $n_0(w) mod 2$ changes from 1 to 0 $\delta(q_3, 0) = q_2$
q_3 When a 1 is read $n_1(w) mod 2$ changes from 1 to 0 $\delta(q_3, 1) = q_1$

Then to show the above diagram accepts exactly the language we start with $w = \epsilon$ at q_0. Since $n_{0,1}(w) = 0$, $0 \bmod 2 \equiv 0$ and $q_0 \in F$ the predicate holds. We have shown that every transition leads to a state that corresponds with our 4 states above and only in q_0 does the predicate $n_0(w) \equiv 0 \bmod 2$ and $n_1(w) \equiv 0 \bmod 2$ hold. We have shown our diagram accepts exactly the language described.

5. Let $M = (Q, \Sigma^*, \delta, q_0, F)$ be a DFA. let $\hat{\delta}$ denote the extended transition function of M, as defined in the lecture slides.

[4] (a) Prove that, for any $x, y \in \Sigma^*$, and any $q \in Q$, we have

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

Proof by induction on $|y|$. **Base Case**:

$$|y| = 0 \implies y = \epsilon$$

Then

$$\begin{aligned} \hat{\delta}(q, xy) &= \hat{\delta}(q, x\epsilon) \\ &= \hat{\delta}(\hat{\delta}(q, x), \epsilon) \end{aligned} \tag{8}$$

Since the base case holds. For our **Induction Hypothesis:** We assume

$$\hat{\delta}(q, xz) = \hat{\delta}(\hat{\delta}(q, x), z) \quad | \quad z \in \Sigma^* \quad \text{and} \quad |z| \geq 0$$

For our **Inductive Step:** we let $z = ya$ where $a \in \Sigma$, $|a| = 1$ and $y \in \Sigma^*$, $|y| \geq 0$ Then,

$$\begin{aligned} \hat{\delta}(q, xz) &= \hat{\delta}(q, xya) \\ &= \delta(\hat{\delta}(q, xy), a) \\ &= \delta(\hat{\delta}(\hat{\delta}(q, x), y), a) \\ &= \hat{\delta}(\hat{\delta}(q, x), ya) \\ &= \hat{\delta}(\hat{\delta}(q, x), z) \end{aligned} \tag{9}$$

By the principle of induction we have shown $\hat{\delta}(q, xy) = \hat{\delta}(\hat{\delta}(q, x), y)$ for all $x, y \in \Sigma^*$ and some $q \in Q$.

[4] (b) Assume that for some state $q \in Q$, and for every $a \in \Sigma^*$, we have $\delta(q, a) = q$. Prove that $\hat{\delta}(q, x) = q$ holds for every $x \in \Sigma^*$.

Proof by induction on $|x|$ with **Base Case**:

$$|x| = 0 \quad \rightarrow \quad x = \epsilon$$

Then,

$$\hat{\delta}(q, \epsilon) = q$$

Induction Hypothesis: Assume,

$$\hat{\delta}(q, k) = q \quad \forall k \in \Sigma^*, |k| \geq 1$$

Inductive Step:
Let $\omega = ak$ where $x \in \Sigma^*$, $|k| \geq 1$ and $a \in \Sigma^*$, $|a| = 1$ then,

$$\begin{aligned} \hat{\delta}(q, \omega) &= \hat{\delta}(q, ak) \\ &= \hat{\delta}(\delta(q, a), k) \\ &= \hat{\delta}(q, k) \\ &= q \end{aligned} \tag{10}$$

Since $\hat{\delta}(q, \omega) = q$ our inductive hypothesis holds and we have shown

$$\hat{\delta}(q, x) = q \quad \forall x \in \Sigma^*$$

[4] (c) Assume that for some state $q \in Q$, and some string $x \in \Sigma^*$, we have $\hat{\delta}(q, x) = q$. Prove that, for every $n \geq 0$, we have $\hat{\delta}(q, x^n) = q$.

Proof by induction on n with **Base Case:**

$$n = 0$$

Then,

$$\hat{\delta}(q, x^0) = \hat{\delta}(q, \epsilon) = q$$

Induction Hypothesis: Assume,

$$\hat{\delta}(q, x^k) = q \quad \forall k \in \mathbb{Z} \quad | \quad k \geq 0$$

Inductive Step: Show true for $k + 1$.

$$\begin{aligned} \hat{\delta}(q, x^{k+1}) &= \hat{\delta}(q, xx^k) \\ &= \hat{\delta}(\hat{\delta}(q, x), x^k) \\ &= \hat{\delta}(q, x^k) \\ &= q \end{aligned} \tag{11}$$

Since $\hat{\delta}(q, x^{k+1}) = q$ our induction hypothesis holds and we have shown:

$$\hat{\delta}(q, x^n) = q, \quad \forall n \in \mathbb{Z} \quad | \quad n \geq 0$$