Exercise 1.

(a)(i) We prove that δ is well defined by a contrapositive proof i.e.

$$\text{if } \exists a \in \Sigma \; [xa] \neq [ya], \text{ then } [x] \neq [y]$$

Suppose $[xa] \neq [ya]$ for $a \in \Sigma$, then by the definition of the equivalence classes of R_L, $(xa, ya) \notin R_L$.

$$(xa, ya) \notin R_L \Leftrightarrow \exists w \in \Sigma^* \; (xaw \in L \wedge yaw \notin L \text{ (or vice versa)})$$

Let $z = aw$, we now have $xz \in L \wedge yz \notin L$ (or vice versa).

$$(xz \in L \wedge yz \notin L) \Leftrightarrow (x, y) \notin R_L \Leftrightarrow [x] \neq [y]$$

Hence, by the contrapositive proof, if $[x] = [y]$, then $[xa] = [ya]$ for all $a \in \Sigma$.

(ii) We prove a more general statement i.e. $\forall x \in \Sigma^* \; \hat{\delta}([\epsilon], x) = [x]$.
This implies $\hat{\delta}([\epsilon], x) \in F$ iff $x \in L$. Since if $x \in L$, then by the definition of F, $[x] = \hat{\delta}([\epsilon], x) \in F$. Conversely, if $\hat{\delta}([\epsilon], x) \in F \Leftrightarrow [x] \in F$, then by the definition of F, $x \in L$.
Now we prove the lemma by an induction on $|x|$.

- **Basis case** $x = \epsilon$. $\delta([\epsilon], \epsilon) = [\epsilon]$ by the definition of the transition function.
- **Step case** Assume that $\hat{\delta}([\epsilon], x) = [x]$ for $|x| < k$. We prove for $w = xa$ where $x \in \Sigma^{k-1}, a \in \Sigma$.

$$\begin{aligned}
\hat{\delta}([\epsilon], xa) &= \delta(\hat{\delta}([\epsilon], x), a) && \text{(definition of } \hat{\delta}) \\
&= \delta([x], a) && \text{(IH)} \\
&= [xa] && \text{(definition of } \delta)
\end{aligned}$$

Hence, we have proven the lemma.
(b). Denote the DFA in part (a) as $D = (Q, \Sigma, \delta, q_0, F)$. We prove that any DFA $A = (Q_A, \Sigma, \delta_A, q_{0_A}, F_A)$ with $L(A) = L$ has at least as many states as D, by constructing a surjective function f from Q_A to Q. We adapted the proof from solutions of Tutorial 2. Define $S(q) = \{w \in \Sigma^* \mid \hat{\delta}(q_{0_A}, w) = q\}$, and f

$$\begin{aligned}
&f : \{q \in Q_A \mid S(q) \neq \emptyset\} \rightarrow \{[x] \mid x \in \Sigma^*\} \\
&f(q) = [x] \text{ with } S(q) \subseteq [x]
\end{aligned}$$

We show that f is well defined, i.e.

- $\forall q \in Q_A$ such that $S(q) \neq \emptyset$, $\exists [x] \in Q$ with $S(q) \subseteq [x]$
  Proof. For $q \in Q_A$, pick $[x] \in Q$ such that $x \in S(q)$. Now for $\forall u, v \in S(q)$, we proved in the tutorial that $(u, v) \in R_L$. Hence for $\forall u \in S(q)$, $(x, u) \in R_L$. Hence, $u \in [x]$, and $S(q) \subseteq [x]$
- if $f(q) = [x]$ and $f(q) = [y]$ for $x \neq y$, then $[x] = [y]$
  Proof. Suppose $f(q) = [x]$ and $f(q) = [y]$, then $S(q) \subseteq [x]$ and $S(q) \subseteq [y]$. Then $u \in S(q) \Rightarrow u \in [x] \Leftrightarrow (x, u) \in R_L$; and $u \in S(q) \Rightarrow u \in [y] \Leftrightarrow (y, u) \in R_L \Leftrightarrow (u, y) \in R_L$. By transitivity, $(x, u) \in R_L \wedge (u, y) \in R_L \Rightarrow (x, y) \in R_L \Leftrightarrow [x] = [y]$

Now, we show that f is surjective. For $[x] \in Q$, we pick $q = \hat{\delta}(q_{0_A}, x) \in Q_A$. $S(q) \neq \emptyset$ since $x \in S(q)$ by definition. We only need to show $S(q) \subseteq [x]$. By the same argument that $\forall u, v \in S(q), (u, v) \in R_L$. $u \in S(q) \Rightarrow (x, u) \in R_L \Leftrightarrow u \in [x]$.
Since f is surjective, then for every state $[x]$ in DFA D, there are corresponding reachable states in DFA A that are mapped to $[x]$, and the cardinality of Q_A exclusive of unreachable states is at least the cardinality of Q. Hence, any DFA that accepts L would have at least as many states as DFA D. Then D is the minimal DFA.

Exercise 2.

(a) Pick n=7. We consider $w = a^j c^k a^l b^m \in L$ with $|w| \geq 7$ in two separate cases.

- $0 \leq j \leq 5$, $k \geq 2$ and $l \neq m$
  Divide $w = xyz$ as $x = a^j c$, $y = c$, and $z = c^{k-2} a^l b^m$. $|xy| = j + 2 \leq 7$ since $0 \leq j \leq 5$, $|y| = 1 > 0$, and by pumping y, we get

  - $xy^0 z = a^j c c^{k-2} a^l b^m = a^j c^{k-1} a^l b^m$
    if $k = 2$, then $k - 1 = 1$, $l \neq m$ still means $xy^0 z \in L$
    if $k > 2$, then $k - 1 \geq 2$, $l \neq m$ still holds, and $xy^0 z \in L$
  - $xy^i z = a^j c c^i c^{k-2} a^l b^m = a^j c^{i+k-1} a^l b^m$ for $i > 1$
    $i + k - 1 > 2$ for $k \geq 2$, $l \neq m$ still holds, so $xy^i z \in L$ for $i > 1$

  Hence, all w when $k \geq 2$ satisfies the pumping lemma.

- $0 \leq j \leq 5$, $k < 2$ and $k, l, m \in \mathbb{N}$
  Note that for $w \in L$ such that $|w| \geq 7$, w should have at least one of l and m not being zero.

  - if $l \neq 0$, then we divide $w = xyz$ such that $x = a^j c^k$, $y = a$, $z = a^{l-1} b^m$. $|xy| = j + k + 1 \leq 7$, $|y| = 1 > 0$,