These exercises are intended to give you some practice devising deterministic finite state automata (DFAs).

1. Let \( L_1 = \{ x \in \{a,b\}^* \mid \text{the number of } a \text{ in } x \text{ is even} \} \), and let \( L_2 = \{ z \in \{a,b\}^* \mid |z| \equiv 0 \mod 3 \} \). Build DFAs that accept \( L_1 \) and \( L_2 \), and use the product procedure to build a DFA that accepts \( L_1 \cap L_2 \).

Sample solution: Here is my specification for \( M_1 = \{Q, \Sigma, \delta, q_0, F\} \) that accepts \( L_1 \):

\[
\{Q = \{E, O\}, \\
\Sigma = \{a, b\}, \\
\delta = \begin{array}{c|ccc}
\delta & E & O \\
\hline
a & O & E \\
b & E & O
\end{array}, \\
q_0 = E, \\
F = \{E\}
\]

Here is my specification for \( M_2 = \{Q, \Sigma, \delta, q_0, F\} \) that accepts \( L_2 \):

\[
\{Q = \{0, 1, 2\}, \\
\Sigma = \{a, b\}, \\
\delta = \begin{array}{c|ccc}
\delta & 0 & 1 & 2 \\
\hline
a & 1 & 2 & 0 \\
b & 1 & 2 & 0
\end{array}, \\
s = q_0 = 0, \\
F = \{0\}
\]
Here is my specification for the product machine $M_{1 \land 2}$ that accepts $L_1 \cap L_2$:

$$Q = \{(E, 0), (E, 1), (E, 2), (O, 0), (O, 1), (O, 2)\},$$
$$\Sigma = \{a, b\},$$

<table>
<thead>
<tr>
<th>$\delta$</th>
<th>$(E, 0)$</th>
<th>$(E, 1)$</th>
<th>$(E, 2)$</th>
<th>$(O, 0)$</th>
<th>$(O, 1)$</th>
<th>$(O, 2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$(O, 1)$</td>
<td>$(O, 2)$</td>
<td>$(O, 0)$</td>
<td>$(E, 1)$</td>
<td>$(E, 2)$</td>
<td>$(E, 0)$</td>
</tr>
<tr>
<td>$b$</td>
<td>$(E, 1)$</td>
<td>$(E, 2)$</td>
<td>$(E, 0)$</td>
<td>$(O, 1)$</td>
<td>$(O, 2)$</td>
<td>$(O, 0)$</td>
</tr>
</tbody>
</table>

$s = q_0 = (E, 0),$  
$F = \{(E, 0)\}$

2. Use structural induction to prove that the DFAs you propose accept $L_1$ and $L_2$. Without any further induction, prove that your product machine accepts $L_1 \cap L_2$ by constructing a state invariant consisting of conjunctions of the state invariants of the other two machines, and then using your earlier proofs to show that this new state invariant is correct.

**Sample solution:** First, define $\Sigma^*$ as the smallest set such that:

(a) $\epsilon \in \Sigma^*$
(b) $s \in \Sigma^* \Rightarrow sa \in \Sigma^* \land sb \in \Sigma^*$

prove that $M_1$ accepts $L_1$: Define $P(s)$ as:

$$P(s) : \delta^*(E, s) = \begin{cases} E & \text{if } s \text{ has an even number of } a \\ O & \text{if } s \text{ has an odd number of } a \end{cases}$$

I prove $\forall s \in \Sigma^*, P(s)$ by structural induction.

basis case: $|s| = 0$, an even number, and $\delta^*(E, \epsilon) = E$ so the implication in the first line of the invariant is true in this case. Also, since $|\epsilon|$ is not odd, the implication in the second line of the invariant is vacuously true. So $P(\epsilon)$ holds.

inductive step: Let $s \in \Sigma^*$ and assume $P(s)$. I will show that $P(sa)$ and $P(sb)$ follow. There are two cases to consider:

case sa: Then

$$\delta^*(E, sa) = \delta(\delta^*(E, s), a) = \begin{cases} \delta(E, a) & \text{if } s \text{ has even number of } a \\ \delta(O, a) & \text{if } s \text{ has odd number of } a \end{cases} \quad \# \text{ by } P(s)$$

$$= \begin{cases} O & \text{if } sa \text{ has odd number of } a \\ E & \text{if } sa \text{ has even number of } a \end{cases} \quad \# \text{ one more } a$$

case sb: Then

$$\delta^*(E, sb) = \delta(\delta^*(E, s), b) = \begin{cases} \delta(E, b) & \text{if } s \text{ has even number of } a \\ \delta(O, b) & \text{if } s \text{ has odd number of } a \end{cases} \quad \# \text{ by } P(s)$$

$$= \begin{cases} E & \text{if } sb \text{ has even number of } a \\ O & \text{if } sb \text{ has odd number of } a \end{cases} \quad \# \text{ same number of } a$$
So $P(sa)$ and $P(sb)$ follow.

The first line of the invariant ensures that all strings with an even number of $a$s are accepted. The contrapositive of the second line of the invariant ensures that any string that does not drive the machine to state $O$ does not have an odd number of $a$s, in other words all strings that drive the machine to state $E$ have an even number of $a$s. So $M_1$ accepts $L_1$.

**prove that $M_2$ accepts $L_2$:** Define $P(s)$ as:

$$P(s) : \delta^*(0,s) = \begin{cases} 0 & \text{if } |s| \equiv 0 \text{ mod } 3 \\
1 & \text{if } |s| \equiv 1 \text{ mod } 3 \\
2 & \text{if } |s| \equiv 2 \text{ mod } 3 \end{cases}$$

I prove $\forall s \in \Sigma^*, P(s)$ by structural induction.

**basis case:** $|s| = 0$, a multiple of 3, and $\delta^*(0,e) = 0$, so the implication in the first line of the invariant is true in this case. Since $|s|$ leaves a remainder of neither 1 nor 2 when divided by 3, the implications on the second and third lines of the invariant are vacuously true. So $P(e)$ holds.

**induction step:** Let $s \in \Sigma^*$ and assume $P(s)$. Let $c \in \{a,b\}$. I will prove that $P(sc)$ follows.

$$\delta^*(0,sc) = \delta(\delta^*(0,s),c) = \begin{cases} \delta(0,c) & \text{if } |s| \equiv 0 \text{ mod } 3 \\
\delta(1,c) & \text{if } |s| \equiv 1 \text{ mod } 3 \# \text{ by } P(s) \\
\delta(2,c) & \text{if } |s| \equiv 2 \text{ mod } 3 \\
1 & \text{if } |sc| \equiv 1 \text{ mod } 3 \\
2 & \text{if } |sc| \equiv 2 \text{ mod } 3 \# \text{ one more character} \\
0 & \text{if } |sc| \equiv 0 \text{ mod } 3 \end{cases}$$

so $P(sc)$ follows.

The invariant ensures that all strings with a multiple of 3 characters drive the machine to state 0. The contrapositives of the second and third lines ensure that any string that does not drive the machine to state 1 does not have a length equivalent to 1 mod 3, and any string that does not drive the machine to state 2 does not have a length equivalent to 2 mod 3, so any strings that drive the machine to state 0 have lengths equivalent to 0 mod 3. Hence $M_2$ accepts $L_2$.

**prove $M_{1\wedge2}$ accepts $L_1 \cap L_2$:** Denote the states for $M_1$ as $Q_1$, the states for $M_2$ as $Q_2$, their respective transition functions as $\delta_1$ and $\delta_2$, and the transition function for $M_{1\wedge2}$ as $\delta_{1\wedge2}$. Inspection of $\delta_{1\wedge2}$ shows that if $(q_1,q_2,c) \in Q_1 \times Q_2 \times \Sigma$, then $\delta_{1\wedge2}((q_1,q_2),c) = (\delta_1(q_1,c),\delta_2(q_2,c))$. Thus the following invariant follows by simply taking conjunctions of the invariants of the component machines, for any $s \in \Sigma^*$

$$P(s) : \delta^*((E,0),s) = \begin{cases} (E,0) & \text{if } s \text{ has an even number of } a \text{ and } |s| \equiv 0 \text{ mod } 3 \\
(E,1) & \text{if } s \text{ has an even number of } a \text{ and } |s| \equiv 1 \text{ mod } 3 \\
(E,2) & \text{if } s \text{ has an even number of } a \text{ and } |s| \equiv 2 \text{ mod } 3 \\
(O,0) & \text{if } s \text{ has an odd number of } a \text{ and } |s| \equiv 0 \text{ mod } 3 \\
(O,1) & \text{if } s \text{ has an odd number of } a \text{ and } |s| \equiv 1 \text{ mod } 3 \\
(O,2) & \text{if } s \text{ has an odd number of } a \text{ and } |s| \equiv 2 \text{ mod } 3 \end{cases}$$

The implication on the first line ensures that all strings with an even number of $a$s and a length that is a multiple of 3 end up in state $(E,0)$. The contrapositive of the implications on the other
lines ensure that any string that does not drive the machines to one of those 5 states must have an even number of $a$s and a length that is a multiple of 3. Hence $M_{1 \land 2}$ accepts $L_1 \cap L_2$. 
