Exercise 1.1.

(a) Give a recursive algorithm for the following operation:

**Input:** States $p$ and $q$ of the master automaton.

**Output:** State $r$ of the master automaton such that $L(r) = L(p) \cdot L(q)$. 

Observe that the languages $L(p)$ and $L(q)$ can have different lengths. Try to reduce the problem for $p, q$ to the problem for $p^a, q$.

(b) Give a recursive algorithm for the following operation:

**Input:** A state $q$ of the master automaton.

**Output:** State $r$ of the master automaton such that $L(r) = L(q)^R$ where $R$ is the reverse operator.

(c) A **coding** over an alphabet $\Sigma$ is a function $h : \Sigma \mapsto \Sigma$. A coding $h$ can naturally be extended to a function over words, i.e., $h(\epsilon) = \epsilon$ and $h(w) = h(w_1)h(w_2) \cdots h(w_n)$ for every $w \in \Sigma^n$. Give an algorithm for the following operation:

**Input:** A state $q$ of the master automaton and a coding $h$.

**Output:** State $r$ of the master automaton such that $L(r) = \{h(w) : w \in L(q)\}$.

Can you make your algorithm more efficient when $h$ is a permutation?

**Solution.**

(a) Let $L$ and $L'$ be fixed-length languages. The following holds:

\[
L \cdot L' = \begin{cases} 
\emptyset & \text{if } L = \emptyset, \\
L' & \text{if } L = \{\epsilon\}, \\
\bigcup_{a \in \Sigma} \{a\} \cdot L^a \cdot L' & \text{otherwise.}
\end{cases}
\]

These identities give rise to the following algorithm:

(b) Let $L$ be a fixed-length language. The following holds:

\[
L^R = \begin{cases} 
\emptyset & \text{if } L = \emptyset, \\
\{\epsilon\} & \text{if } L = \{\epsilon\}, \\
\bigcup_{a \in \Sigma} (L^a)^R \cdot \{a\} & \text{otherwise.}
\end{cases}
\]

These identities give rise to the following algorithm:

[hard] Note that Lines 11 and 12 are introduced in order to represent the language $\{a_i\}$ in Line 13 as a state $\text{make}(s_1, s_2, ..., s_n)$ of the master automaton. This can be avoided by using the algorithm from Exercise 8.1, namely the state that represents $\{a_i\}$ is $\text{add-lang}\{\{a_i\}\}$. Thus, Lines 11-13 can be replaced just by $r \leftarrow \text{concat}\left(\text{reverse}(q^a), \text{add-lang}(\{a_i\})\right)$.
Input: States $p$ and $q$ of the master automaton.

Output: State $r$ of the master automaton such that $L(r) = L(p) \cdot L(q)$.

1. $\text{concat}(p, q) :$
2. if $G(p, q)$ is not empty then
   3. return $G(p, q)$
4. else if $p = q_0$ then
   5. return $q_0$
6. else if $p = q_\varepsilon$ then
   7. return $q$
7. else
   8. for $a_i \in \Sigma$ do
      9. $s_i \leftarrow \text{concat}(p^{a_i}, q)$
   10. $G(p, q) \leftarrow \text{make}(s_1, s_2, \ldots, s_n)$
   11. return $G(p, q)$

(c) Let $L$ be a fixed-length language and let $h$ be a coding. The following holds:

$$h(L) = \begin{cases} 
\emptyset & \text{if } L = \emptyset, \\
\{\varepsilon\} & \text{if } L = \{\varepsilon\}, \\
\bigcup_{a \in \Sigma} h(a) \cdot h(L^a) & \text{otherwise}. 
\end{cases}$$

These identities give rise to the following algorithm:

The above algorithm makes use of union because the coding may be the same for distinct letters, i.e. $h(a) = h(b)$ for $a \neq b$ is possible. However, if the coding is a permutation, then this is not possible, and thus each letter maps to a unique residual. Therefore, the algorithm can be adapted as follows:

Exercise 1.2.

Let $\Sigma = \{\text{request}, \text{answer}, \text{working}, \text{idle}\}$.

(1) Build a regular expression and an automaton recognizing all words with the property $P_1$: for every occurrence of request there is a later occurrence of answer.

(2) Build an automaton recognizing all words with the property $P_2$: there is an occurrence of answer before which only working and request occur.

(3) Using automata theoretic constructions, prove that all words accepted by the automaton $A$ below satisfy $P_1$, and give a regular expression for all words accepted by the automaton $A$ that violate $P_2$.

![Diagram of automaton](image)

Solution. (1) A possible regular expression is $(\Sigma^*\text{answer})^*(\Sigma\backslash\{\text{request}\})^*$. (Observe that we must also describe the sequences containing no occurrence of request.) A minimal NFA for the property is
Input: A state $q$ of the master automaton.
Output: State $r$ of the master automaton such that $L(r) = L(q)^R$.

1. $\text{reverse}(q)$:
   2. if $G(q)$ is not empty then
      3. return $G(q)$
   4. else if $q = q_0$ then
      5. return $q_0$
   6. else if $q = q_e$ then
      7. return $q_e$
   8. else
      9. $p \leftarrow q_0$
     10. for $a_i \in \Sigma$ do
     11. $s_i \leftarrow q_e$
     12. $s_j \leftarrow q_0$ for every $i \neq j$
     13. $r \leftarrow \text{concat} \left( \text{reverse} (q^{a_i}), \text{make}(s_1, s_2, ..., s_n) \right)$
      14. $p \leftarrow \text{union} (p, r)$
      15. $G(q) \leftarrow p$
      16. return $G(q)$

(3) A minimal NFA for $P_2$ is

(4) Determinizing and complementing the automaton for $P_1$ we get

The intersection of $A$ and the automaton for $P_1$ is empty: indeed, we can only reach a final state of $A$ by executing request, while we can only reach a final state of the automaton for $P_1$ by executing answer. So we cannot simultaneously reach final states in both.
Input: A state $q$ of the master automaton and a coding $h$.

Output: State $r$ of the master automaton such that $L(r) = \{h(w) : w \in L(q)\}$.

1. coding($q, h$):
   2. if $G(q)$ is not empty then
      3. return $G(q)$
   4. else if $q = q_0$ then
      5. return $q_0$
   6. else if $q = q_e$ then
      7. return $q_e$
   8. else
      9. $p \leftarrow q_0$
     10. for $a \in \Sigma$ do
     11.     $r \leftarrow$ coding($q^a, h$)
     12.     $s_h(a) \leftarrow r$
     13.     $s_b \leftarrow q_0$ for every $b \neq h(a)$
     14.     $p \leftarrow \text{union}(p, \text{make}(s))$
     15.     $G(q) \leftarrow p$
     16. return $G(q)$

For the second half, since the automaton for $P_2$ is deterministic, we can complement it by exchanging final and non-final states (and not forgetting that the trap state now becomes an accepting state). We get:

![Diagram](image)

The intersection with $A$ yields

![Diagram](image)

and the regular expression is $(\text{working} + \text{request})^* \text{idle} \Sigma^* \text{answer}$.

Exercise 1.3.

Suppose there are $n$ processes being executed concurrently. Each process has a critical section and a non critical section. At any time, at most one process should be in its critical section. In order to respect this mutual exclusion property, the processes communicate through a channel $c$. Channel $c$ is a queue that can store up to $m$ messages. A process can send a message $x$ to the channel with the instruction $c {!} x$. A process can also consume the first message of the channel with the instruction $c ? x$. If the channel is
Input: A state \( q \) of the master automaton and a coding \( h \) which is a permutation.

Output: State \( r \) of the master automaton such that \( L(r) = \{ h(w) : w \in L(q) \} \).

1. \( \text{coding-permutation}(q, h) : \)
2. if \( G(q) \) is not empty then
3. \hspace{1em} return \( G(q) \)
4. else if \( q = q_\emptyset \) then
5. \hspace{1em} return \( q_\emptyset \)
6. else if \( q = q_\epsilon \) then
7. \hspace{1em} return \( q_\epsilon \)
8. else
9. \hspace{2em} for \( a \in \Sigma \) do
10. \hspace{3em} \( s_{h(a)} \leftarrow \text{coding-permutation}(q^a, h) \)
11. \hspace{2em} \( G(q) \leftarrow \text{make}(s) \)
12. \hspace{1em} return \( G(q) \)

full when executing \( c!x \), then the process blocks and waits until it can send \( x \). When a process executes \( c?x \), it blocks and waits until the first message of the channel becomes \( x \).

Consider the following algorithm. Process \( i \) declares its intention of entering its critical section by sending \( i \) to the channel, and then enters it when the first message of the channel becomes \( i \):

1. \( \text{process}(i) : \)
2. \hspace{1em} while true do
3. \hspace{2em} \( c!i \)
4. \hspace{2em} \( c?i \)
5. \hspace{2em} /* critical section */
6. \hspace{2em} /* non critical section */

(a) Sketch an automaton that models a channel of size \( m > 0 \) where messages are drawn from some finite alphabet \( \Sigma \).

(b) Model the above algorithm, with \( n = 2 \) and \( m = 1 \), as a network of automata. There should be three automata: one for the channel, one for \( \text{process}(0) \) and one for \( \text{process}(1) \).

(c) Construct the asynchronous product of the network obtained in (b).

(d) Use the automaton obtained in (c) to show that the above algorithm violates mutual exclusion, i.e. the two processes can be in their critical sections at the same time.

(e) Design an algorithm that makes use of a channel to achieve mutual exclusion for two processes \( (n = 2) \). You may choose \( m \) as you wish.

(f) Model your algorithm from (e) as a network of automata.

(g) Construct the asynchronous product of the network obtained in (f).
(h) Use the automaton obtained in (g) to show that your algorithm achieves mutual exclusion.

**Solution.**

(a) We construct an automaton $A_{\Sigma, m}$ that stores the content of the channel within its states. For example, the automaton for $\Sigma = \{0, 1\}$ and $m = 2$ is as follows:

More formally, $A_{\Sigma, m} = (Q, \Gamma, \delta, q_0, F)$ is defined as:

\[
Q = \{ w \in (\Sigma \cup \square)^m : (w_i = \square) \implies (w_{i+1} = \square) \text{ for every } 1 \leq i < m \},
\]

\[
\Gamma = \{ c ! \sigma : \sigma \in \Sigma \} \cup \{ c ? \sigma : \sigma \in \Sigma \},
\]

\[
q_0 = \square^m,
\]

\[
F = Q.
\]

Let $\ell : Q \to \{1, 2, \ldots, m\}$ be the function that associates to each state $q$ the position of the last letter of $q$ which is not $\square$. For example, $\ell(abb\square\square) = 3$. The transitions are formally defined as follows:

\[
\delta(q, c ! \sigma) = \begin{cases} q_1q_2\cdots q_\ell(q)\sigma\square^{m-\ell(q)-1} & \text{if } \ell(q) < m, \\ \text{none} & \text{otherwise}, \end{cases}
\]

\[
\delta(q, c ? \sigma) = \begin{cases} q_2q_3\cdots q_m\square & \text{if } q_1 = \sigma, \\ \text{none} & \text{otherwise}. \end{cases}
\]

[hard] Note that $A_{\Sigma, m}$ grows exponentially since $|Q| = \sum_{i=0}^m |\Sigma|^i = (|\Sigma|^{m+1} - 1)/(|\Sigma| - 1)$. 
(b) The automata for the channel, \texttt{process(0)} and \texttt{process(1)} are respectively:

\begin{figure}[h]
\centering
\begin{tikzpicture}
    \node[draw, circle] (0) at (0,0) {$0$};
    \node[draw, circle] (1) at (2,0) {$1$};
    \node[draw, circle] (square) at (1,-1) {$\square$};
    \draw[->] (square) edge[bend right] node[above] {$c!0$} (0);
    \draw[->] (square) edge[bend right] node[below] {$c?0$} (0);
    \draw[->] (square) edge[bend left] node[above] {$c!1$} (1);
    \draw[->] (square) edge[bend left] node[below] {$c?1$} (1);
\end{tikzpicture}
\end{figure}

\begin{figure}[h]
\centering
\begin{tikzpicture}
    \node[draw, circle] (r0) at (0,0) {$r_0$};
    \node[draw, circle] (w0) at (1,0) {$w_0$};
    \node[draw, circle] (c0) at (2,0) {$c_0$};
    \node[draw, circle] (n0) at (2,-1) {$n_0$};
    \node[draw, circle] (r0) at (2,0) {$r_0$};
    \draw[->] (r0) edge node[above] {$c!0$} (w0);
    \draw[->] (w0) edge node[above] {$c?0$} (c0);
    \draw[->] (c0) edge node[above] {$c_0$} (n0);
    \draw[->] (n0) edge node[below] {$n_0$} (r0);
\end{tikzpicture}
\end{figure}

\begin{figure}[h]
\centering
\begin{tikzpicture}
    \node[draw, circle] (r1) at (0,0) {$r_1$};
    \node[draw, circle] (w1) at (1,0) {$w_1$};
    \node[draw, circle] (c1) at (2,0) {$c_1$};
    \node[draw, circle] (n1) at (2,-1) {$n_1$};
    \node[draw, circle] (r1) at (2,0) {$r_1$};
    \draw[->] (r1) edge node[above] {$c!1$} (w1);
    \draw[->] (w1) edge node[above] {$c?1$} (c1);
    \draw[->] (c1) edge node[above] {$c_1$} (n1);
    \draw[->] (n1) edge node[below] {$n_1$} (r1);
\end{tikzpicture}
\end{figure}

(c)
(d) The algorithm violates mutual exclusion since state \((c_0, c_1, \square)\) is reachable in the above automaton.

(e) We initialize a channel \(c\) of size one with message 1. When a process wants to enter its critical section, it simply consumes 1 from the channel and sends it back once it is done:

```
1 process():
2    while true do
3        /* non critical section */
4        c ? 1
5        /* critical section */
6        c ! 1
```

(f) The automata modeling the channel and the two processes are respectively:
Note that we have introduced the new letters $c ! 1$ and $c ? 1$. We could have simply used letters $c ! 1$ and $c ? 1$. However, these new letters will be important when considering the asynchronous product of the network. If the two automata modeling the processes both used $c ! 1$ and $c ? 1$, then the asynchronous product would force them to synchronize on these letters.

In class, we have seen an alternative solution: to simply swap line 4 and 5 of the processes described in #6.2. This also works. You can verify this solution either manually or with Spin.
(h) None of the state of the above automaton is of the form $(c_0, c_1, \sigma)$ where $\sigma \in \{\square, 1\}$. This implies that both processes cannot be in their critical sections at the same time.