FORMAL LANGUAGES & AUTOMATA

VICKY G

We are going to study the relationship between a special kind of machine (automata), languages and a special kind of algebra (monoids).

Automata \(\leftrightarrow\) Regular Languages \(\leftrightarrow\) Monoids

1. MONOIDS AND LANGUAGES

A monoid is a set \(M\) together with an associative binary operation, which has an identity.

Thus, a monoid has the following algebraic relations

\[
\forall a, b \in M \quad \exists ab \in M, \\
\forall a, b, c \in M \quad a(bc) = (ab)c, \\
\exists 1 \in M \text{ such that } 1a = a = a1 \quad \forall a \in M.
\]

Note. The identity of \(M\) is unique.

1.1. Alphabets, Words and Languages

Study (sets of) sequences of symbols.

Definition: An alphabet is a finite non-empty set \(A\). A letter is an element of \(A\) and a word (or string) over \(A\) is a finite sequence of elements of \(A\).

Example 1.1. If we have the alphabet \(A = \{0, 1\}\) then the following are words over \(A\): 0, 10, 011. If \(A = \{a, b\}\) then \(a, b, ab, ba, a aa, a ab, \ldots\) are all words over \(A\). If \(A\) is the standard alphabet \(\{a, b, \ldots, z\}\) then \(cat\) and \(atz\) are words over \(A\).

Note. If \(a_1, a_2, \ldots, a_n, a'_1, a'_2, \ldots, a'_m \in A\) then \(a_1a_2\ldots a_n = a'_1a'_2\ldots a'_m \iff n = m\) and \(a_i = a'_i\) for \(1 \leq i \leq n\).

We define \(A^+=\{a_1a_2\ldots a_n \mid n \in \mathbb{N}, a_i \in A, 1 \leq i \leq n\}\) to be the set of all non-empty words over \(A\). Also, introduce the empty word \(\varepsilon\) (in some books denoted 1 or \(\lambda\)). Now, \(A^* = A^+ \cup \{\varepsilon\}\) is the set of all words over \(A\). A language (over \(A\)) is a subset of \(A^*\).

Definition: A language \(L\) is finite if \(|L| < \infty\). A language is cofinite if \(L^c = A^* \setminus L\)

Example 1.2. \(\emptyset, \{\varepsilon\}, \{a, b, ba\}\) are finite languages.
Length of Words
We have that the empty words has no letters and so $|\varepsilon| = 0$. Also, 

$$|a_1a_2\ldots a_n| = n.$$  

Note. $|xy| = |x| + |y|$  

Example 1.3. $|abab| = 4$, $|a| = 1$ and $|aa| = |ab| = 2$.

Let us take the language $L = \{w \in A^* \mid |w| \geq 2\}$, then this is cofinite. This is because $L^c = \{\varepsilon\} \cup A$ is finite.

Concatenation of Words
Take $x, y \in A^*$ then we form a new word $xy$ by putting $x$ and $y$ together, end to end.

Example 1.4. Let $x = ab$ and $y = bca$ then by $xy$ we refer to $abca$.

Note. \(\varepsilon x = x = x\varepsilon\) for all $x \in A^*$. Also $(xy)z = x(yz)$ for all $x, y, z \in A^*$. Hence $A^*$ is a monoid with identity element $\varepsilon$, called the free monoid on $A$. We note that $A^*$ is not a group as only $\varepsilon$ has an inverse element. This is because given any $x$ there can never be a $y$ such that $xy = \varepsilon$.

For $a \in A$, $a^n$ ($n \geq 0$) is the word consisting of $n$ $a$’s, i.e. $a^0 = \varepsilon$, $a^1 = a$, $a^2 = aa$, $a^3 = aaa$, etc.

Note. \(\{a\}^* = \{\varepsilon, a, aa, aaa, \ldots\}\) = \(\{\varepsilon, a, a^2, a^3, \ldots\}\) = \(\{a^n \mid n \geq 0\}\).

For any $x \in A^*$

$$x^n = \underbrace{xx\ldots x}_{n \text{ times}}.$$  

Example 1.5. $x^0 = \varepsilon$ if $x = ab$ then $x^3 = ababab$.

Clearly $x^nx^m = x^{n+m}$ and $(x^n)^m = x^{nm}$ for all $n, m \geq 0$, i.e. the index laws hold.

Letter Count
If $a \in A$ and $x \in A^*$, then $|x|_a$ = the number of occurrences of $a$ in $x$.

Example 1.6. If $A = \{a, b, c\}$ then $|abca|_a = 2$, $|\varepsilon|_b = 0$, $|accac|_b = |ac^2ac|_b = 0$ and $|ac^2ac|_c = 3$.

Prefix
$y$ is a prefix of a word $x \in A^*$ if $x = yz$ for some $z \in A^*$. We note that $\varepsilon$ is a prefix of $x$ for any $x \in A^*$ as $x = \varepsilon x$. Also, any word $x \in A^*$ is a prefix of itself because $x = x\varepsilon$. If $x = a^2b$, then the prefixes of $x$ are $\varepsilon, a, a^2, a^2b$. 
1.2. Operations on Languages

Recall that a *language* over $A$ is a subset of $A^*$. We have that $\emptyset$, $A^*$ are languages over $A$ and $\emptyset \subseteq L \subseteq A^*$ for any language $L$.

**Boolean Operations**

If $L,K$ are languages then $L \cup K$, $L \cap K$, $L \setminus K$ and $L^c = A^* \setminus L$ are also languages.

**Product:** Let $L,K \subseteq A^*$ then we define $LK = \{xy \mid x \in L, y \in K\}$.

**Example 1.7.** If we have $\{a,ab\}$ and $\{b,bc\}$ are languages then $\{a,ab\}\{b,bc\} = \{ab,abc,abb,abbc\}$.

As an exercise show that $(KL)M = K(LM)$. For $w \in A^*$ and $L \subseteq A^*$, usually write $wL$ for $\{w\}L$ and $Lw$ for $L\{w\}$, etc. So $wL = \{wv \mid v \in L\}$ and $KwL = K\{w\}L = \{uwv \mid \in K, v \in L\}$. As usual, $L^n$ denotes $\underbrace{L \cdots L}_{n \text{ times}}$.

So $L^1 = L$, $L^2 = LL$, $L^3 = LLL$, $\ldots$, $L^{n+1} = L^nL$, $L^0 = \{\varepsilon\}$.

**The (Kleene) Star:** of $L \subseteq A^*$ is $L^* = \{x_1x_2\ldots x_n \mid n \geq 0 \text{ and } x_i \in L, 1 \leq i \leq n\}$

$= L^0 \cup L^1 \cup L^2 \cup \ldots$

$= \bigcup_{n \geq 0} L^n$.

**Example 1.8.** $a \in A$, $L = \{a^2\}$ then we have $L^* = \{\varepsilon, a^2, a^4, a^6, \ldots \} = \{a^{2n} \mid n \geq 0\}$

**Example 1.9.** $a,b \in A$, $L = \{ab, ba\}$ then we have $L^* = \{\varepsilon, ab, ba, abab, abba, baba, baab, \ldots \}$

**Example 1.10.** $\{\varepsilon\}^* = \{\varepsilon\} = \emptyset^*$
If \( L = \{ w \} \) sometimes write \( w^* \) for \( \{ w \}^* \) but be careful:

\[
ab^* = \{ a \} \{ b \}^* = \{ a \} \{ b^n : n \geq 0 \} = \{ ab^n : n \geq 0 \}
\]

the star is only attributed to the \( b \). So, \( \{ ab \}^* \) is written as

\[
(ab)^* = \{ (ab)^n : n \geq 0 \} = \{ \varepsilon, ab, abab, ababab, \ldots \}.
\]

Thus we have \( A^*aab^*aa \) means \( A^*\{ aa \} \{ b \}^*\{ aa \} = \{ waab^n aa : w \in A^*, n \geq 0 \} \).

## 2. Automata

A point of grammar – the singular form of automata is automaton.

### 2.1. Various kinds

We concentrate on two kinds of finite state automata.

- **DFA:** complete, deterministic, finite state automata
- **NDA:** non-deterministic finite state automata (usually not complete either).

Formally a DFA is a 5-tuple

\[
A = (A, Q, \delta, q_0, F)
\]

where we have

- \( A \) is an alphabet (so \( |A| < \infty \)),
- \( Q \) is a finite set of “states”,
- \( q_0 \in Q \) is the initial state,
- \( F \subseteq Q \) is the set of final (or accepting, or terminal) states,
- \( \delta: Q \times A \to Q \) is the state transition function or next state function.

### 2.2. State Transition Diagrams

States are represented by \( \bigcirc \). There are various different kinds of objects in a State Transition Diagram.

- State \( q \) is \( \bigcirc \),
- Final state is \( \bigcirc \) or \( \bigcirc \)
- Initial state by \( \bigcirc \)
- Indicate \( \delta(q_1, a) = q_2 \) by \( \bigcirc \xrightarrow{a} \bigcirc \)

**Example 2.1.** Let \( A = \{ a, b \} \) then the following

\[
\begin{align*}
\text{Example 2.1.} & \quad \text{Let } A = \{ a, b \} \text{ then the following} \\
& \quad \begin{tikzpicture}
\node (q0) at (0,0) {$q_0$};
\node (q1) at (1,0) {$q_1$};
\draw [->] (q0) edge [loop above] node {$a, b$} (q0);
\draw [->] (q0) edge [bend right] node {$a, b$} (q1);
\end{tikzpicture}
\end{align*}
\]
is the state transition diagram of the DFA

\[ A = \left( \{a, b\}, \{q_0, q_1\}, \delta, q_0, \{q_1\} \right). \]

Now we describe \( \delta \) as

\[ \delta(q_0, a) = q_1 = \delta(q_0, b), \]
\[ \delta(q_1, a) = q_0 = \delta(q_1, b). \]

We can describe \( \delta \) by a table

\[
\begin{array}{c|cc}
  & a & b \\
  q_0 & q_1 & q_1 \\
  q_1 & q_0 & q_0 \\
\end{array}
\]

For a DFA \( A = (A, Q, \delta, q_0, F) \) we extend \( \delta \) to give a function \( \delta : Q \times A^* \rightarrow Q \) as follows

\[ \delta(q, \varepsilon) = q \quad \forall q \in Q, \]
\[ \delta(q, wa) = \delta(\delta(q, w), a) \quad \forall w \in A^*, \forall a \in A, \forall q \in Q. \]

Returning to the example above we have

\[
\begin{align*}
\delta(q_0, aba) &= \delta(\delta(q_0, ab), a) \\
&= \delta(\delta(q_0, a), b), a) \\
&= \delta(\delta(q_1, b), a) \\
&= \delta(q_0, a) \\
&= q_1
\end{align*}
\]

A DFA \( A = (Q, A, \delta, q_0, F) \) has \( \delta : Q \times A \rightarrow Q \) a function. Thus because \( \delta \) is a function we have for all \((q, a) \in Q \times A\), \( \delta(q, a) \) is defined, thus \( A \) is complete. Also for all \((q, a) \in Q \times A\), \( \exists ! \delta(q, a) \) means \( A \) is deterministic.

RECALL: \( \delta : Q \times A^* \rightarrow Q \) is given by \( \delta(q, \varepsilon) = q \) and \( \delta(q, wa) = \delta(\delta(q, w), a) \) where \( w \in A^*, a \in A \).

FACT: For all \( u, v \in A^* \) we have

\[ \delta(q, uv) = \delta((q, u), v). \]

The proof of this is done by induction on \(|v|\), i.e. the number of letters in \( v \).

Definition: A word \( w \in A^* \) is accepted by \( A \) if \( \delta(q_0, w) \in F \) and \( w \in A^* \) is rejected by \( A \) if \( \delta(q_0, w) \notin F \). The language recognised by \( A \) is
\[ L(A) = \{ w \in A^* | \delta(q_0, w) \in F \}, \]
i.e. the set of words that \( A \) accepts. A language \( L \subseteq A^* \) is recognisable if there exists a DFA \( A \) with \( L = L(A) \).

**Example 2.2.** Find a DFA of \( A = \{ a, b \} \) which recognises

\[ L = \{ w \in A^* | w \text{ begins with } ab \} = abA^* \]

![DFA Diagram](image)

Thus we have that \( L(A) = L \).

**Example 2.3.** Find a DFA \( A \) which recognises

\[ L = \{ w \in A^* | |w|_b \leq 2 \} \]

![DFA Diagram](image)

*Note.* Using different notation we can express \( L \) as

\[ L = \{ a \}^* \cup \{ a \}^* \{ b \} \{ a \}^* \cup \{ a \}^* \{ b \} \{ a \}^* \{ b \} \{ a \}^* = a^* \cup a^* ba^* \cup a^* ba^* ba^* \]

**Example 2.4.** Given a DFA of \( A \)

![DFA Diagram](image)

find the language that is recognised by \( A \). This is

\[ L(A) = a^*b = \{ a \}^* \{ b \} = \{ a^n b | n \in \mathbb{N}^0 \} \]

**Example 2.5.** Given a DFA \( A \)
find the language that is recognised by $\mathcal{A}$. We can see that $\mathcal{A}$ accepts words of the form 
(for $n, m, h, k \in \mathbb{N}^0$) $a^{n+1}b, b^m a^{n+1}b, b^m a^{n+1}b^{h+2} a^{k+1}b$. We now guess that 

$$L(\mathcal{A}) = A^*ab = \{wab \mid w \in A^*\}.$$ 

Suppose that $v \in L(\mathcal{A})$ then 

$$\delta(q_0, v) = q_2.$$ 

For this to happen we must have $v = v'b$ where $\delta(q_0, v') = q_1$. For this to happen we must have $v' = v''a$ and hence $v = v'b = v''ab \Rightarrow v \in A^*ab$ and $L(\mathcal{A}) \subseteq A^*ab$.

Conversely let $w \in A^*ab$ so $w = vab$ for some $v \in A^*$. Notice that $\delta(q_i, ab) = q_2$ for any $i = 0, 1, 2$. Hence

$$\delta(q_0, w) = \delta(q_0, vab) = \delta(\delta(q_0, v), ab) = q_2 \in F.$$ 

Hence $A^*ab \subseteq L(\mathcal{A})$ and so $A^*ab = L(\mathcal{A})$.

**Example 2.6 (A Basic Automaton).** The following automaton represents a vending machine. The cost of goods is 20p and it has states $\{0, 5, 10, 15, 20, X\}$. The DFA $\mathcal{A}$ consists of

$$A = \{5, 10, 20\},$$ 

$$q_0 = \{0\},$$ 

$$F = \{20\},$$ 

$$\delta(X, a) = X,$$ 

$$\Rightarrow \delta(u, v) = u + v.$$
We have the language recognised by $A$ is

$$L(A) = \{555, 5510, 20, 1055, \ldots \}.$$ 

**Notation:** for an alphabet $A$ write $\text{Rec}_{A^*}$ for the class of recognisable languages over $A$. So, $L \in \text{Rec}_{A^*}$ means “$L$ is recognisable”, i.e. there exists a DFA $A$ with $L = L(A)$

To show $L \in \text{Rec}_{A^*}$ we must find a DFA $A$ with $L = L(A)$. How do we show that $L \notin \text{Rec}_{A^*}$?

**Lemma 2.1** (Pumping Lemma - PL). Let $L \in \text{Rec}_{A^*}$. Then there exists $N \in \mathbb{N}$ such that for all $w \in L$ with $|w| \geq N$ there exists a factorisation $w = uvx$ $(u,v,x \in A^*)$ with $|v| \neq \varepsilon$ and $|uv| \leq N$ and $uv^kx \in L$ for all $k \geq 0$ (i.e. $ux, uvx, uv^2x, \ldots$ all lie in $L$).

**Note.**

1. $u, v, x \in A^*$; usually not in $L$; $u, x$ can be empty; we must have $v \neq \varepsilon$.
2. $N$ is a pumping length for $L$; if $M \geq N$, then $M$ is also a pumping length.
3. The conditions of the pumping lemma are necessary for $L \in \text{Rec}_{A^*}$ but not sufficient.

**Examples of the use of the Pumping Lemma**

1. $A = \{a, b\}; L = \{a^n b^n \mid n \geq 0\}$ is not recognisable.

   **Proof.** Suppose $L \in \text{Rec}_{A^*}$. Let $N$ be a pumping length for $L$. Choose $w = a^n b^n$, so $w \in L$ and $|w| = 2N \geq N$. So, there exists a factorisation $w = uvx$ where $|uv| \leq N$ and $v \neq \varepsilon$. So, $u = a^r$, $v = a^s$ and $x = a^t b^N$ where $r + s + t = N$ ($u > w = uvx = a^N b^N$) and $s \neq 0$. By the pumping lemma, $uv^2x \in L$, i.e. $a^r a^s a^t a^N b^N = a^{N+s} b^N \in L$ but this is a contradiction as $N + s \neq N$. Hence $L \notin \text{Rec}_{A^*}$. \hfill \Box

2. $A = \{a, b\}$, $L = \{w \in A^* \mid |w|_a = |w|_b\}$. We claim that $L \notin \text{Rec}_{A^*}$.
Given $L \subseteq A^*$, suppose we want to show $L \not\in \text{Rec } A^*$. Assume $L \in \text{Rec } A^*$ and aim for a contradiction. Let $N$ be a pumping length for $L$. Choose $w \in L$ with $|w| \geq N$. By the pumping lemma, $w$ has a fact satisfying the conditions of PL. Use this to get a contradiction. Therefore $L \not\in \text{Rec } A^*$ (Note: need only choose one $w$ - choose an easy one!).

(3) $A = \{a\}$, $L = \{a^p \mid p \text{ is prime}\}$. Claim $L \not\in \text{Rec } A^*$.

Proof. Suppose $L \in \text{Rec } A^*$. Let $N$ be a pumping length for $L$. Let $p$ be prime, $p \geq N$. Then $w = a^p \in L$ and $|w| \geq N$. By PL there exists a factorisation $w = uvx$ where $|vx| \leq N$ and $v \neq \varepsilon$. Thus $uv^kx \in L$ for all $k \geq 0$. Therefore $L \not\in \text{Rec } A^*$. □

Proof of PL. Let $L \in \text{Rec } A^*$. Then $L = L(A)$ for some DFA $A$, where $A = (A, Q, \delta, q_0, F)$. Let $N = |Q|$, the number of states of $A$. If $w \in L$ and $|w| \geq N$, then $\delta(q_i, w) \in F$. Let $w = a_1a_2\ldots a_N\ldots a_m$ where $a_i \in A$ and $m = |w| \geq N$. As $w \in L$ we have

![Diagram](https://example.com/diagram.png)

where $q_i \in Q$, $q_0$ is the initial state and $q_m \in F$ and $\delta(q_i, a_i) = q_{i+1}$ where $0 \leq i \leq m - 1$. Since $N + 1 > N = |Q|$, the list $q_0, q_1, \ldots, q_N$ must contain repeats; say $q_i = q_j$ where $0 \leq i < j \leq N \leq m$. Then we have

![Diagram](https://example.com/diagram.png)

Put $u = a_1 \ldots a_i$, $v = a_{i+1} \ldots a_j$, $x = a_{j+1} \ldots a_m$ ($u = \varepsilon$ if $i = 0$, $v \neq \varepsilon$ as $i < j$, $x = \varepsilon$ if $j = N = m$). We have $|uv| = j \leq N$, $v \neq \varepsilon$, $w = uvx$. For any $k \geq 0$,

$$\delta(q_0, uv^kx) = \delta(\delta(q_0, u), v^kx) = \delta(q_i, v^kx) = \delta(\delta(q_i, v^k), x) = \delta(q_i, x) = \delta(q_N, x) = q_m \in F.$$ Therefore $uv^k \in L$ for all $k \geq 0$. □
2.3. NDAs: Non-Deterministic finite state Automata

Example 2.7. In Exercises 2, you are asked to find a DFA which accepts \( L = \{ abwab \mid w \in A^* \} \) where \( A = \{ a, b \} \). Want to write

\[
\begin{array}{c}
q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_2 \xrightarrow{a} q_3 \xrightarrow{b} q_4 \\
ap, b
\end{array}
\]

but this is not a DFA (neither complete nor deterministic). It is an example of an NDA.

Definition: An NDA \( \mathcal{A} \) is a 5-tuple \((A, Q, E, I, F)\) where
- \( A \) is a finite alphabet,
- \( Q \) is a finite set of states,
- \( E \) is a subset of \( Q \times A \times Q \),
- \( I \subseteq Q \) is a set of initial states,
- \( F \subseteq Q \) is a set of final states.

Elements of \( E \) have the form \((p, a, q)\) where \( p, q \in Q \) and \( a \in A \). These are called edges.

In the above example we can see that our edges are \((q_0, a, q_1), (q_1, b, q_2), (q_2, a, q_2), (q_2, b, q_2), (q_2, a, q_3), (q_3, b, q_4)\). A path in \( \mathcal{A} \) (of length \( n \geq 1 \)) is a finite sequence of edges. So, \((q_1, a_1, q_1), (q_1, a_2, q_2), \ldots, (q_n-1, a_n, q_n)\) is a path. The label of the path is \( a_1a_2\ldots a_n \); in the state transition diagram we have

\[
\begin{array}{c}
p_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \xrightarrow{a_3} a_{n-1} q_{n-1} \xrightarrow{a_n} q_n \\
op \xrightarrow{w} q \ (w \in A^*) \text{ means that there exists a path from } p \text{ to } q \text{ in } \mathcal{A}, \text{ with label } w. \text{ Note that there exists } p \xrightarrow{w} p \text{ for any } p \in Q. \\

Definition: \( w \in A^* \) is accepted by the NDA \( \mathcal{A} \) if there exists a path \( q_0 \xrightarrow{w} q \) for some \( q_0 \in I \) and \( q \in F \).

Definition: The language recognised by the NDA \( \mathcal{A} \) is

\[
L(\mathcal{A}) = \{ w \in A^* \mid w \text{ is accepted by } \mathcal{A} \}.
\]

Note that in the example the language recognised by the NDA is
\[
\{\text{abwab} \mid w \in A^*\} \quad A = \{a,b\}.
\]

We claim that for a language \( L \subseteq A^* \) we have that

\( L \) is recognised by a DFA \( \iff \) \( L \) is recognised by an NDA.

**Proposition.** We start by showing \( L \in \text{Rec} A^* \Rightarrow \) \( L \) is recognised by an NDA.

**Proof.** Let \( L = L(A) \) where \( A = (A, Q, \delta, q_0, F) \) is a DFA. Put

\[
E = \{(q,a,\delta(q,a)) \mid q \in Q, a \in A\} \subseteq Q \times A \times Q
\]

and \( I = \{q_0\} \). Now we have an NDA

\[
A' = (A, Q, E, I, F)
\]

and \( L(A) = L(A') \). \( \square \)

We can think of a DFA as a special kind of NDA, one in which there exists one initial state and for all \( q \in Q, a \in A \), there exists exactly one triple \((q,a,p)\).

Now, we need to prove the converse. First we define some notation. Let

\[
A = (A, Q, E, I, F)
\]

be an NDA. For \( S \subseteq Q, w \in A^* \), we define \( Sw = \{q \in Q \mid p \xrightarrow{w} q \text{ for some } p \in S\} \). Note that \( Sw \subseteq Q \) (so there exists only finitely many sets of the form \( Sw \)).

**Example 2.8.** Given an NDA \( A \)

\[
\begin{array}{c}
1 \\
\begin{array}{ccc}
\text{a} & \text{b} & \text{3} \\
\text{1} & \text{2} & \text{a} & \text{4} & \text{a} & \text{5}
\end{array}
\end{array}
\]

Now we have that

\[
\begin{align*}
\{1,2\}ab &= \{3\} = \{1\}ab, \\
\{2\}ab &= \emptyset, \\
\{1\}aa &= \{5\}, \\
\{1\}a &= \{2,4\}, \\
\emptyset a &= \emptyset = \emptyset w \quad \forall w.
\end{align*}
\]
In general, for $a \in A$ we have that

$$S\varepsilon = S,$$

$$Sa = \{p \in Q \mid \exists (q, a, p), q \in S\},$$

$$Sa_1a_2\ldots a_n = (\ldots ((Sa_1)a_2)\ldots )a_n),$$

$$\emptyset w = \emptyset \quad w \in A^*.$$

We now construct a DFA from our NDA $A = (a, Q, E, I, F)$ as follows. Put $Q' = \{Iw \mid w \in A^*\}$.

**Note.** We have $Q' \subseteq \mathcal{P}(Q)$ (set of all subsets of $Q$).

As $Q$ and hence $\mathcal{P}(Q)$ are finite, then $Q'$ is finite. How do we find $Q''$? Say $A = \{a_1, a_2, \ldots, a_n\}$. Now write down $I = I\varepsilon$ and calculate $Ia_i$ for each $a_i$. Then for each $Ia_i$ we calculate $Ia_ia_j$ for all $i$ and for all $j$. We continue this process until we have a list

$$Iw_1, Iw_2, \ldots, Iw_k$$

such that $Iw_ka_i$ is already in the list for all $h$ and for all $i$.

Now given an NDA $A = (A, Q, E, I, F)$ we define a DFA $B = (A, Q', \delta, I, F')$ where $\delta(S, a) = Sa$ and $F' = \{s \in Q' \mid S \cap F \neq \emptyset\}$.

**Note.** $\delta(S, a_1a_2\ldots a_n) = \delta(\delta(S, a_1), a_2)\ldots ), a_n) = (\ldots (Sa_1)a_2)\ldots a_n) = Sa_1\ldots a_n$

**EXAMPLE 2.9 (Construction of a DFA from and NDA).** Let our NDA $A$ be

![Diagram of a DFA]

Then the language accepted by $A$ is

$$L(A) = \{\varepsilon, ab, aa\}.$$

We now calculate our set $Q'$. We note that the set of initial states is $I = \{1, 3\}$. Then
We have a DFA $B$ where

$$B = (A, Q', \delta, q_0, F').$$

For this we have

- $Q' = \{ I, \{2, 4\}, \emptyset, \{3\}, \{5\}\}$
- $q_0 = I = \{1, 3\}$
- $F' = \{ S \in Q' | S \cap F \neq \emptyset \} = \{ S \in Q' | S \cap \{3, 5\} \neq \emptyset \} = \{ I, \{3\}, \{5\}\}$

and $\delta$ is given as in the following state transition diagram.

Then we have $L(B) = \{ \epsilon, ab, aa \}$

**Proposition.** $L \subseteq A^* \text{ recognised by an NDA } \Rightarrow L \in \text{Rec } A^*$.

**Proof.** Let $L = L(A)$ where $A = (A, Q, E, I, F)$. Define a DFA $B = (A, Q', \delta, q_0, F')$ as above. Now recall that

- $Q' = \{ Iw | w \in A^* \}$,
- $\delta(S, a) = Sa$,
- $q_0 = I$,
- $F' = \{ \delta \in Q' | S \cap F \neq \emptyset \}$.

**Claim.** $L(A) = L(B)$

We have that
\[ w \in L(B) \iff \delta(q_0, w) \in F' \]
\[ \iff \delta(I, w) \in F' \]
\[ \iff Iw \in F' \]
\[ \iff Iw \cap F \neq \emptyset \]
\[ \iff \text{there exists a path } p \xrightarrow{w} q \]
\[ \text{for some } p \in I, q \in F \]
\[ \iff w \in L(A). \]

Hence this gives us our theorem.

**Theorem 2.1.** \( L \in \text{Rec} \ A^* \iff L = L(A) \) for some NDA \( A \).

**Example 2.10.** Any \( A \) such that \( A^* \in \text{Rec} \ A^* \) as the DFA

\[
\begin{array}{c}
\text{\includegraphics{figure1}}
\end{array}
\]

for all \( a \in A \) recognises \( A^* \).

**Example 2.11.** The \( \emptyset \) \( \in \text{Rec} \ A^* \) as \( \emptyset \) recognised by the NDA

\[
\begin{array}{c}
\text{\includegraphics{figure2}}
\end{array}
\]

**Example 2.12.** \( \{\varepsilon\} \) \( \in \text{Rec} \ A^* \) as \( \{\varepsilon\} \) is recognisable by the NDA

\[
\begin{array}{c}
\text{\includegraphics{figure3}}
\end{array}
\]

**Example 2.13.** For \( w = a_1a_2 \ldots a_n \in A^+ \) (\( a_i \in A \)) then \( \{w\} \) is recognisable by the NDA

\[
\begin{array}{c}
\text{\includegraphics{figure4}}
\end{array}
\]

So all singleton languages lie in \( \text{Rec} \ A^* \).

**3. Rational Languages and Kleene’s Theorem**

3.1. **Closure Properties of Rec \( A^* \)**

**Proposition (1).** \( L \in \text{Rec} \ A^* \Rightarrow L^c \in \text{Rec} \ A^* \)
Proof. If \( L \in \text{Rec} \) then \( L = L(A) \) where \( A = (A, Q, \delta, q_0, F) \). Let \( A^c = (A, Q, \delta, q_0, F^c) \). Then

\[
w \in L(A^c) \iff \delta(q_0, w) \in F^c \iff \delta(q_0, w) \notin F \iff w \notin L(A) = L \iff w \in L^c.
\]

Therefore \( L(A^c) = L^c \) and \( L^c \in \text{Rec} \). \( \square \)

Proposition (2). \( L, K \in \text{Rec} \) \( \Rightarrow \) \( L \cup K \in \text{Rec} \)

Proof. Let \( L = L(A) \) and \( K = L(B) \) where \( A = (A, Q, E, I, F) \) and \( B = (A, P, E', I', F') \) are NDAs. Assume \( Q \cap P = \emptyset \). Put \( C = (A, Q \cup P, E \cup E', I \cup I', F \cup F') \). Then

\[
w \in L \cup K \iff w \in L \text{ or } w \in K
\]

\[
\iff \exists \text{ path } q_0 \xrightarrow{w} q \text{ in } A \text{ with } q_0 \in I \text{ and } q \in F
\]

or \( \exists \text{ path } p_0 \xrightarrow{w} p \text{ in } B \text{ with } p_0 \in I' \text{ and } p \in F' \).

\[
\iff \exists \text{ path } r_0 \xrightarrow{w} r \text{ in } C \text{ with } r_0 \in I \cup I' \text{ and } r \in F \cup F' \text{ (since } P \cap Q = \emptyset)
\]

\( \iff w \in L(C) \).

Therefore \( L \cup K \in \text{Rec} \). \( \square \)

Corollary 3.1. \( L_1, L_2, \ldots, L_m \in \text{Rec} \) \( \Rightarrow \) \( L_1 \cup L_2 \cup \cdots \cup L_m \in \text{Rec} \).

Proof. Proposition 2 and Induction. \( \square \)

Corollary 3.2. \( L, K \in \text{Rec} \) \( \Rightarrow \) \( L \cap K \in \text{Rec} \).

Proof. \( L \cap K = (L^c \cup K^c)^c \); hence result by propositions 1 and 2. \( \square \)

Corollary 3.3. \( L_1, L_2, \ldots, L_m \in \text{Rec} \) \( \Rightarrow \) \( L_1 \cap L_2 \cap \cdots \cap L_m \in \text{Rec} \).

Proof. Corollary 3.2 and Induction. \( \square \)

Corollary 3.4. \( L, K \in \text{Rec} \) \( \Rightarrow \) \( L \setminus K \in \text{Rec} \).

Proof. Exercise Sheet 4. \( \square \)

Note. \( \text{Rec} \) is NOT closed under infinite \( \cup \) and \( \cap \) (Exercise Sheet 4).

Proposition (3). Let \( L, K \in \text{Rec} \). Then \( LK \in \text{Rec} \) (Recall \( LK = \{wv \mid w \in L, v \in K\} \)).

Proof. First assume \( \varepsilon \notin K \). Let \( L = L(A) \) and \( K = L(B) \) where

\[
A = (A, Q, E, I, F) \quad \text{and} \quad B = (A, P, E', I', F')
\]

are NDAs and \( P \cap Q = \emptyset \).

[We would like
but this would not ‘separate’ $\mathcal{A}$ and $\mathcal{B}$ adequately].

Put $\mathcal{C} = (A, Q \cup P, \tilde{E}, I, F')$ where

$$\tilde{E} = \tilde{E} = E \cup E' \cup \{(q, ar) \mid q \in F \text{ and } (p_0, a, r) \in E' \text{ for some } p_0 \in I\}.$$  

$(p_0, a, r) \in E' \iff (q, a, r) \in \tilde{E}$. Now we have

$$w \in LK \iff w = uv, \text{ some } u \in L, v \in K$$

$$\iff w = uav', \text{ some } u \in L, v = av' \in K, a \in A \text{ (as } \varepsilon \notin K)$$

$$\iff \exists q_0 \in I, q \in F, q_0 \xrightarrow{w} q \text{ in } \mathcal{A}$$

and $\exists p_0 \in I, p \in F', p_0 \xrightarrow{a} p \text{ in } \mathcal{B}$

$$\iff \exists q_0 \in I, q \in F, q_0 \xrightarrow{\tilde{w}} q \text{ in } \mathcal{A} \text{ and}$$

$$\exists p_0 \in I', r \in P, p \in F' \text{ with } p_0 \xrightarrow{a} r \xrightarrow{v'} p \text{ in } \mathcal{B}$$

$$\iff \exists q_0 \in I, p \in F, q_0 \xrightarrow{uav'} p \text{ in } \mathcal{C}$$

$$\iff uav' = uv \in L(C).$$

Hence $L(\mathcal{C}) = LK$ and so $LK \in \text{Rec } A^*$. Hence, if $\varepsilon \notin K$, then $LK \in \text{Rec } A^*$. Finally, if $\varepsilon \in K$, then $K' = K \setminus \{\varepsilon\}$ is recognisable by Corollary 3.4. We have

$$LK = L(K' \cup \{\varepsilon\})$$

$$= LK' \cup L\{\varepsilon\} \quad \text{(Exercise 1)}$$

$$= LK' \cup L$$

and $LK' \in \text{Rec } A^*$ by the first part of the proof, so $LK \in \text{Rec } A^*$ by Proposition 2. \qed

**Proposition.** $L \in \text{Rec } A^* \Rightarrow L^* \in \text{Rec } A^*$
Proof. Recall that

\[ L^* = \bigcup_{n \geq 0} L^n = L^0 \cup L^1 \cup L^2 \cup \ldots = \{\varepsilon\} \cup L \cup L^2 \cup L^3 \cup \ldots \]

Since \( L \) is recognisable, \( L = L(A) \) for some DFA \( A = (A, Q, \delta, q_0, F) \).

Claim. We claim, \( L = L(B) \) where \( B = (A, P, \sigma, p_0, G) \) for a DFA \( B \) with \( \sigma(p, a) \neq p_0 \) for any \( p \in P, a \in A \).

Proof. Put \( P = Q \cup \{p_0\} \) where \( p_0 \not\in Q \) and

\[ \sigma(q, a) = \delta(q, a) \quad \text{for all } q \in Q, a \in A, \]
\[ \sigma(p_0, a) = \delta(q_0, a) \]

Now put

\[ G = \begin{cases} F & \text{if } \varepsilon \not\in L(A) \text{ (i.e. } q_0 \not\in F), \\ F \cup \{p_0\} & \text{if } \varepsilon \in L(A) \text{ (i.e. } q_0 \in F). \end{cases} \]

Now check that \( L(A) = L(B) \)

Note. \( \sigma(p, a) \neq p_0 \) for all \( p \in P, a \in A \).

Let \( L = L(B) \) where \( B = (A, P, \sigma, p_0, G) \) is a DFA with \( \sigma(p, a) \neq p_0 \) for all \( p \in P, a \in A \). Put \( C = (A, P, E, \{p_0\}, \{p_0\}) \) where

\[ E = \{ (p, a, \sigma(p, a)) \mid p \in P, a \in A \} \cup \{ (p, a, p_0) \mid p \in P, \sigma(p, a) \in G \} \]

Note. \( \varepsilon \in L^* \) and \( \varepsilon \in L(C) \)
Suppose \( w \neq \varepsilon \). Then

\[
w \in L^* \iff w = w_1 w_2 \ldots w_t \text{ with } t \geq 1, w_i \in L \setminus \{\varepsilon\} \text{ for all } i, \\
\Rightarrow w = w_1 w_2 \ldots w_t, t \geq 1, \sigma(p_0,w_i) \in G \forall i, \\
\Rightarrow w = w_1 w_2 \ldots w_t, t \geq 1, p_0 \xrightarrow{w_i} p \text{ in } B \forall i, p \in G, \\
\Rightarrow w = w_1 \ldots w_t, t \geq 1, p_0 \xrightarrow{w_i} p_0 \text{ in } C \forall i, \\
\Rightarrow p_0 \xrightarrow{w_i} p_0 \text{ in } C, \\
\Rightarrow w \in L(C).
\]

Hence we have \( L^* \subseteq L(C) \). Conversely let \( w \in L(C) \Rightarrow p_0 \xrightarrow{w_i} p_0 \in C \). Let \( w = a_1 a_2 \ldots a_n \) (\( a_i \in A \)) and

\[
p_0 \xrightarrow{a_1} p_1 \xrightarrow{a_2} p_2 \ldots \xrightarrow{a_n} p_n = p_0
\]

amongst \( 1, \ldots, n \). Let \( i_1, i_2, \ldots, i_t = n \) be such that

\[
0 < i_1 < i_2 < \ldots < i_t \quad \text{and } p_{ij} = p_0.
\]

Put

\[
w_1 = a_1 a_2 \ldots a_{i_1}, \\
w_2 = a_{i_1+1} \ldots a_{i_2}, \\
\vdots \\
w_t = a_{i_{t-1}+1} \ldots a_{i_t}.
\]

Then \( w = w_1 w_2 \ldots w_t \) and \( p_0 \xrightarrow{w_i} p_0 \in C \) for all \( j \) (\( p_0 \xrightarrow{w_i} p \xrightarrow{a_{i_j}} p_0 \) in \( C \), so in \( B \), \( p_0 \xrightarrow{w_i} p \xrightarrow{a_{i_j}} p' \in G \) in \( B \)). So, \( w = w_1 w_2 \ldots w_t \) and \( p_0 \xrightarrow{w_i} p' \in G \) in \( B \), i.e. \( w = w_1 w_2 \ldots w_t \) where \( w_j \in L(B) = L \) for all \( j \Rightarrow w \in L^* \). Therefore \( L(C) \subseteq L^* \) and so \( L(C) = L^* \). \( \square \)

**Examples of using Closure Properties**

**Example 3.1.** \( L \) finite \( \Rightarrow L \in \text{Rec } A^* \).

**Proof.** \( L \) finite \( \Rightarrow L = \emptyset \) or \( L = \{w_1, w_2, \ldots, w_n\} \) for some \( w_i \in A^* \). We know \( \emptyset \in \text{Rec } A^* \) and \( \{w_i\} \in \text{Rec } A^* \) for all \( i \). Therefore \( L = \{w_1\} \cup \{w_2\} \cup \ldots \cup \{w_n\} \) is recognisable by Corollary 3.5. \( \square \)

**Example 3.2.** \( L \) cofinite \( \Rightarrow L \in \text{Rec } A^* \).

**Proof.** \( L \) cofinite \( \Rightarrow L^c \) is finite \( \Rightarrow L^c \in \text{Rec } A^* \) by above example. Hence \( L = (L^c)^c \in \text{Rec } A^* \) by proposition 1. \( \square \)
Example 3.3. \( A = \{a, b\} \). Then \( L = A^*aaA^* \cup A^*bbA^* \in \text{Rec} A^* \).

Proof. \( A^*, \{aa\}, \{bb\} \in \text{Rec} A^* \) so \( A^*aaA^*, A^*bbA^* \in \text{Rec} A^* \) by proposition 7 (twice). Hence \( L = A^*aaA^* \cup A^*bbA^* \in \text{Rec} A^* \). \( \square \)

Example 3.4. \( L = \{a^n \mid n \text{ is not prime} \} \notin \text{Rec} A^* \).

Proof. \( L \in \text{Rec} A^* \Rightarrow L^c \in \text{Rec} A^* \) (by Proposition 1). But \( L^c = \{a^p \mid p \text{ is prime} \} \) is not in \( \text{Rec} A^* \). Contradiction. Hence \( L \notin \text{Rec} A^* \). \( \square \)

Example 3.5. \( L = \{w \in \{a, b\}^* \mid |w|_a = |w|_b\} \) an alternate argument for \( L \notin \text{Rec} A^* \).

Let \( L = \{a^mb^n \mid m \geq 0, n \geq 0\} \in \text{Rec} A^* \) (See Exercises 4). Suppose \( L \in \text{Rec} A^* \), then \( L \cap K \in \text{Rec} A^* \) by Corollary 6. But \( L \cap K = \{a^mb^n \mid n \geq 0\} \) – we know this is not recognisable by the Pumping Lemma. This is a contradiction and hence \( L \) is not recognisable.

Note. \( B \subseteq A \) then for \( L \subseteq B^* \) we have \( L \in \text{Rec} B^* \Leftrightarrow L \in \text{Rec} A^* \) (check).

Example 3.6.

(a) \( L' = \{a^n b^p \mid n \geq 0, p \text{ prime} \} \notin \text{Rec} A^* \), \( A = \{a, b\} \). Now,

\[ L' \in \text{Rec} A^* \Rightarrow L' \cap B^* \in \text{Rec} A^* \Rightarrow \{b^p \mid p \text{ is prime}\} \in \text{Rec} A^* \]

a contradiction and hence \( L' \) is not recognisable. In fact,

\[ L = \{a^n b^p \mid n \geq 1, p \text{ prime}\} \]

is not recognisable (see later for why).

(b) \( L \cup b^* \notin \text{Rec} A^* \)

Proof. \( L \cup b^* \in \text{Rec} A^* \Rightarrow (L \cup b^*) \cap a^+b^* \in \text{Rec} A^* \). Recall tat for an alphabet \( A, A^+ = A^* \setminus \{\varepsilon\} \), so \( a^+ = \{a^n \mid n \geq 1\} \) – note \( a^+b^* = (a^* \setminus \{\varepsilon\})b^* \in \text{Rec} A^* \).

But \( (L \cup b^*) \cap a^+b^* = L \) – and \( L \) is not recognisable, a contradiction. Hence \( L \cup b^* \notin \text{Rec} A^* \). \( \square \)

(c) \( L \cup b^* \) satisfies the conditions of the Pumping Lemma (exercise).

3.2. Rational Operations

Let \( A \) be an alphabet. The rational operations (on languages over \( A \)) are union, product and star, i.e. \( L, K \Rightarrow L \cup K, L, K \Rightarrow LK \) and \( L \Rightarrow L^* \). The Boolean operations are union, intersection and complement, i.e. \( L, K \Rightarrow L \cup K, L, K \Rightarrow L \cap K \) and \( L \Rightarrow L^c \).

We have seen that \( \text{Rec} A^* \) is closed under the rational operations and the Boolean operations.

Definition: \( L \subseteq A^* \) is rational if

(i) \( L \) is finite or
(ii) $L$ can be obtained from finite languages by applying rational operations a finite number of times.

$\text{Rat } A^*$ is the set of all rational languages over $A$.

**Observation**: We have already proved that any finite language lies in $\text{Rec } A^*$ and if $L, K \in \text{Rec } A^*$ then $L \cup K, LK, L^* \in \text{Rec } A^*$ – consequently

$$\text{Rat } A^* \subseteq \text{Rec } A^*.$$ 

**Example 3.7.**

(a) $\emptyset, \{w\}, \{ab, ba, a^6bc\}$ are finite and so rational.

(b) $\{ab, ba, a^6bc\}^*, ab^*a = \{a\}\{b\}^*\{a\} \in \text{Rat } A^*$.

(c) $L = \{abwab \mid w \in A^*\} = \{ab\}\{a, b\}^*\{ab\} \in \text{Rat } A^*$

(d) $L = \{x \in \{a, b\}^* \mid |x|_a \leq 1\} = b^* \cup b^*ab^* \in \text{Rat } A^*$.

**Theorem 3.1** (Kleene’s Theorem). $\text{Rat } A^* = \text{Rec } A^*$.

**Proof.** We have already observed that $\text{Rat } A^* \subseteq \text{Rec } A^*$.

Let $L \in \text{Rec } A^*$. Then $L = L(A)$ for some NDA $A = (A, Q, E, I, F)$. We prove by induction on $|E|$ that $L \in \text{Rat } A^*$. If $|E| = 0$ then $L = \{\varepsilon\}$ if $I \cap F \neq \emptyset$ and $L = \emptyset$ if $I \cap F = \emptyset$. So $L$ is finite, hence $L \in \text{Rat } A^*$.

Now let $|E| = n > 0$ and suppose $L(B) \in \text{Rat } A^*$ for all NDAs $B$ with the number of edges of $B < n$. Let $e \in E$, so $e = (p, a, q)$ and define 4 new NDAs as follows:

$$A_0 = (A, Q, E \setminus \{e\}, I, F),$$

$$A_1 = (A, Q, E \setminus \{e\}, I, \{p\}),$$

$$A_2 = (A, Q, E \setminus \{e\}, \{q\}, \{p\}),$$

$$A_3 = (A, Q, E \setminus \{e\}, \{q\}, F).$$

Let $L_i = L(A_i)$. By our induction hypothesis each $L_i \in \text{Rat } A^*$ (as each $A_i$ has $n - 1$ edges). Hence

$$L_4 = L_0 \cup L_1\{a\}(L_2\{a\})^*L_3 \in \text{Rat } A^*.$$ 

We claim that $L = L_4$. First we note that

$$L_0 = L(A_0) = \{w \in L \mid \exists q_o \xrightarrow{w} r, q_o \in I, r \in F \text{ not involving the edge } e\},$$

$$\subseteq L = L(A).$$ 

Let $w \in L_1\{a\}(L_2\{a\})^*L_3$. Then $w = ua(v_1av_2a\ldots v_ma)x$, where $u \in L_1$, $v_i \in L_2$, $x \in L_3$ with $1 \leq i \leq m$ and there exists a path in $A$

$$q_0 \overset{u}{\rightarrow} p \xrightarrow{a} q \xrightarrow{x} r$$
Therefore \( w \in L(A) = L \). We have shown that \( L_4 \subseteq L \). Conversely suppose \( w \in L(A) \). Then there exists a path \( q_0 \xrightarrow{w} r \in F \) in \( A \).

If the edge \( e \) is not used in this path, we have \( q_0 \xrightarrow{w} r \in F \) in \( A_{\emptyset} \) so \( w \in L(A_{\emptyset}) = L_0 \subseteq L_4 \).

Suppose now that \( w = a_1a_2 \ldots a_n \) and

\[
q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \xrightarrow{} \ldots \xrightarrow{} q_n = r
\]

where the edge \( e \) occurs. Suppose that

\[
(q_{i_1-1}, a_{i_1}, q_{i_1}), \ldots, (q_{i_t-1}, a_{i_t}, q_{i_t})
\]

are all the occurrences of \( e = (p, a, q) \) (each \( a_{i_j} = a \)). Then \( w = w_0a_1w_1 \ldots aw_t \) where

\[
q_0 \xrightarrow{w_0} p \xrightarrow{a} q \xrightarrow{w_1} p \xrightarrow{a} q \xrightarrow{} p \xrightarrow{a} q \xrightarrow{w_t} r
\]

Hence \( w_0 \in L(A_1) = L_1 \), \( w_i \in L(A_2) = L_2 \) (\( 1 \leq i < t \)), \( w_t \in L(A_3) = L_3 \). Hence \( w = w_0a_1w_1 \ldots a_{i_{t-1}}w_t \in L_1a(L_2a)^*L_3 \subseteq L_4 \).

Therefore \( L \subseteq L_4 \). Hence \( L = L_4 \) and \( L \in \text{Rec } A^* \). \( \square \)

Hence for \( L \subseteq A^* \) we know

(i) \( L = L(A) \) for some DFA \( A \) (\( L \in \text{Rec } A^* \)),

(ii) \( L = L(A) \) for some NDA \( A \),

(iii) \( L \) is rational (\( L \in \text{Rec } A^* \)).

### 3.3. Specialisation to \( A = \{a\} \)

Let \( A = (Q, \delta, q_0, F) \) be a DFA. Then we have that \( q \in Q \) is accessible if \( \delta(q_0, w) = q \) for some \( w \in A^* \). \( A \) is accessible if every state of \( A \) is accessible.

Clearly if \( A \) has inaccessible states, these can be removed to give a DFA \( A' \) with \( L(A') = L(A) \) – so we lose nothing by assuming our DFAs are accessible. We assume from now on our DFAs are accessible.

**Proposition.** Let \( L \subseteq a^* \{a\}^* \). Then \( L \in \text{Rec } A^* \iff L = K \cup J(a^p)^* \) for some finite \( K, J \subseteq A^* \).

**Proof.** (\( \Rightarrow \)) Kleene’s theorem.

(\( \Leftarrow \)) Let \( L = L(A) \) where \( A = (\{a\}, Q, \delta, q_0, F) \) is an accessible DFA. Put \( q_k = \delta(q_0, a^k) \) as \( A \) is accessible \( Q = \{q_0, q_1, \ldots\} \). We have \( Q \) is a finite set, so let \( m \geq 0 \) be the least number such that \( q_m = q_{m+r} \) for some \( r \geq 1 \) and let \( p \geq 1 \) be least such that \( q_m = q_m + p \).
Let $F' = \{q_0, q_1, \ldots, q_{m-1}\} \cap F$ and $F'' = \{q_m, q_{m+1}, \ldots, q_{m+p-1}\} \cap F$, $F = F' \cup F''$. Put

\[
K = \{a^i \mid q_i \in F\} = \{a^i \mid \delta(q_0, a^i) \in F\} \quad (|K| < \infty)
\]

\[
J = \{a^i \mid m \leq i < m + p, q_i \in F''\} = \{a^i \mid m \leq i < m + p, \delta(q_0, a^i) \in F''\} \quad (|J| < \infty)
\]

Then $K, J \subseteq L(A) = L$ and $K \cup J = L \cap \{a^0, a^1, \ldots, a^{m+p-1}\}$. For $n \geq m + p$ we have

\[
a^n \in L(A) \iff \delta(q_0, a^n) \in F
\]

\[
\iff \delta(q_0, a^n) = q_i \text{ some } q_i \in F''
\]

\[
\iff q_n = q_i, \text{ some } q_i \in F''
\]

\[
\iff n = i + tp, \text{ for some } t \geq 1
\]

\[
\iff a^n = a^{i+tp} = a^i (a^p)^t, \text{ some } t \geq 1, a^i \in J
\]

\[
\iff a^n \in J(a^p)^+.
\]

We also have for $n \leq m + p - 1$

\[
a^n \in L(A) \iff a^n \in K \cup J.
\]

Hence $L(A) = K \cup J \cup J(a^p)^+ = K \cup J(a^p)^\ast$. \hfill \Box

### 3.4. Revision of Equivalence Relations

A relation $\sim$ on a set $A$ is an *equivalence relation* if

1. $a \sim a$ for all $a \in A$ (Reflexive),
2. $a \sim b \Rightarrow b \sim a$ for all $a, b \in A$ (Symmetric),
3. $a \sim b, b \sim c \Rightarrow a \sim c$ for all $a, b, c \in A$ (Transitive).

Then $\sim$-equivalence class (or just $\sim$-class) of $a \in A$ is the set $\{b \in A \mid a \sim b\}$. Often write $[a]$ for this set.

**Note.** $[a] = \{b \in A \mid a \sim b\} = \{b \in A \mid b \sim a\}$ as $\sim$ is symmetric $a \in [a]$ as $a \sim a$ (reflexive).
FACTS:
(1) \([a] = [b] \iff [a] \cap [b] \neq \emptyset\), so the equivalence classes partition \(A\), i.e. cut up \(A\) into disjoint non-empty subsets.
(2) \([a] = [b] \iff b \in [a] \iff a \sim b (\iff [a] \cap [b] \neq \emptyset)\) or \([a] \neq [b] \iff b \notin [a] \iff a \neq b (\iff [a] \cap [b] = \emptyset)\).

4. Reduced DFAs

Given a DFA \(A = (A, Q, \delta, q_0, F)\) with \(L(A) = L\) we find a DFA \(\bar{A} = (\bar{A}, \bar{Q}, \bar{\delta}, \bar{q}_0, \bar{F})\) with \(L(\bar{A}) = L\) such that \(\bar{A}\) has the smallest number of states of any DFA accepting \(L\).

Two DFA’s, \(A\) and \(B\) (with the same alphabet), are equivalent if \(L(A) = L(B)\). We have remarked that any DFA is equivalent to an accessible DFA. We assume that all DFA’s are accesible.

Let \(A = (A, Q, \delta, q_0, F)\). Define \(\sim\) on \(Q\) by

\[q \sim q' \iff \forall w \in A^* (\delta(q, w) \in F \iff \delta(q', w) \in F)\).

Note. \(\sim\) is an equivalence relation on \(Q\).

Definition: An (accessable) DFA \(A\) is reduced if \(q \sim q' \Rightarrow q = q'\).

Theorem 4.1. Any DFA \(A\) is equivalent to a reduced DFA.

Proof. Let \(A = (A, Q, \delta, q_0, F)\) be an (accessible) DFA. \([q]\) is the \(\sim\)-class of \(q\) and \(\bar{Q} = \{[q] \mid q \in Q\}\). Define \(\bar{\delta} : \bar{Q} \times A \rightarrow \bar{Q}\) by \(\bar{\delta}([q], a) = [(q, a)]\).

(1) \(\bar{\delta}\) is well-defined.

Proof. We have that
\[
[q] = [q'] \Rightarrow q \sim q' \\
\Rightarrow \forall w \in A^*, \delta(q, w) \in F \iff \delta(q', w) \in F \\
\Rightarrow \forall a \in A, \forall w \in A^*, \delta(q, aw) \in F \iff \delta(q', aw) \in F. \\
\Rightarrow \forall a \in A, \forall w \in A^*, \delta(\delta(q, a), w) \in F \iff \delta(\delta(q', a), w) \in F \\
\iff \forall a \in A, \delta(q, a) \sim \delta(q', a) \\
\iff \forall a \in A, [\delta(q, a)] = [\delta(q', a)]
\]

Hence \(\bar{\delta}([q], a) = \bar{\delta}([q'], a)\), so \(\bar{\delta}\) is well-defined. \(\square\)

(2) For \(q \sim q', q \in F \iff \delta(q, \varepsilon) \in F \iff \delta(q', \varepsilon) \in F \iff q' \in F\). So, in \([q]\) either all states are final or none are final. We put \(\bar{F} = \{[q] \mid q \in F\}, \bar{q}_0 = [q_0]\). So, \(\bar{A} = (A, \bar{Q}, \bar{\delta}, \bar{q}_0, \bar{F})\) is a DFA.
(3) For any $w \in A^*$ we have $\bar{\delta}([q], w) = [\delta(q, w)]$. Then

$$\bar{\delta}([q], \varepsilon) = [q] = [\delta(q, \varepsilon)].$$

For $w \in A$, result is true by definition of $\bar{\delta}$. Suppose the result is true for all $w \in A^*$ with $|w| = n$. Then

$$\bar{\delta}([q], wa) = \bar{\delta}(\bar{\delta}([q], w), a) \quad \text{by definition of extended } \bar{\delta},$$

$$= \bar{\delta}(\delta(q, w), a) \quad \text{inductive assumption},$$

$$= [\delta(\delta(q, w), a)] \quad \text{definition of } \bar{\delta},$$

$$= [\delta(q, wa)] \quad \text{definition of extended } \delta.$$

(4) $\bar{A}$ is reduced.

Proof. We have that

$$[q] \sim [q'] \iff \forall w \in A^*, \bar{\delta}([q], w) \in \bar{F} \iff \bar{\delta}([q'], w) \in \bar{F}$$

$$\iff \forall w \in A^*, [\delta(q, w)] \in \bar{F} \iff [\delta(q', w)] \in \bar{F}$$

$$\iff \forall w \in A^*, \delta(q, w) \in F \iff \delta(q', w) \in F$$

by the definition of $\bar{F}$

$$\iff q \sim q'$$

$$\iff [q] = [q']$$

and so $\bar{A}$ is reduced. \qed

(5) $\bar{A}$ is equivalent to $A$

$$w \in L(\bar{A}) \iff \delta(q_0, w) \in F,$$

$$\iff [(q_0, w)] \in \bar{F},$$

$$\iff \bar{\delta}([q_0], w) \in \bar{\delta},$$

by the definition of the extended $\bar{\delta}$

$$\iff w \in L(\bar{A}).$$

Hence we have $L(\bar{A}) = L(A)$. \qed

Definition: Let $A = (A, Q, \delta, q_0, F)$, $B = (A, P, \sigma, p_0, T)$ be DFAs. Then $A$ is isomorphic to $B$ if there exists a bijection $\theta : Q \rightarrow P$ such that $q_0 \theta = p_0$, $F \theta = T$ and

$$\delta(q, a) \theta = \sigma(q \theta, a) \quad \forall q \in Q, a \in A.$$
We write maps on the right of the their arguments, with the exception of the next state function. So, we write \( af \) instead of \( f(a) \).

**Claim.** If \( \mathcal{A} \) and \( \mathcal{B} \) are reduced and equivalent, then \( \mathcal{A} \) is isomorphic to \( \mathcal{B} \). (So, in theorem above \( \overline{\mathcal{A}} \) is the unique (up to isomorphism) reduced DFA equivalent to \( \mathcal{A} \).)

**Proof.** \( \mathcal{A} \) and \( \mathcal{B} \) are accessible. Define \( \theta : Q \to P \) by \( \delta(q_0, w)\theta = \sigma(p_0, w) \). Certainly \( \theta \) is everywhere defined and onto. Is \( \theta \) well-defined?

\begin{align*}
\delta(q_0, w) = \delta(q_0, w') & \iff \delta(q_0, w) \sim \delta(q_0, w') \quad \mathcal{A} \text{ is reduced}, \\
& \iff \forall v \in A^* \quad \delta(\delta(q_0, w), v) \in F \iff \delta(\delta(q_0, w'), v) \in F, \\
& \iff \forall v \in A^* \quad \delta(q_0, wv) \in F \iff \delta(q_0, w'v) \in F, \\
& \iff \forall v \in A^* \quad wv \in L(\mathcal{A}) \iff w'v \in L(\mathcal{A}), \\
& \iff \forall v \in A^* \quad wv \in L(\mathcal{B}) \iff w'v \in L(\mathcal{B}), \\
& \iff \forall v \in A^* \quad \sigma(p_0, wv) \in T \iff \sigma(p_0, w'v) \in T, \\
& \iff \forall v \in A^* \quad \sigma(\sigma(p_0, w), v) \in T \iff \sigma(\sigma(p_0, w'), v) \in T, \\
& \iff \sigma(p_0, w) \sim \sigma(p_0, w'), \\
& \iff \sigma(p_0, w) = \sigma(p_0, w'), \\
& \iff \delta(q_0, w)\theta = \delta(q_0, w')\theta.
\end{align*}

Now \( \Rightarrow \) gives us that \( \theta \) is well-defined and \( \Leftarrow \) gives \( \theta \) is 1:1. \( \square \)

**Check:** \( q_0\theta = p_0, \ F\theta = T \) and \( \delta(q, a)\theta = \sigma(q\theta, a) \) for all \( q \in Q, a \in A \).

**Proposition.** If \( L = L(\mathcal{A}) \) where \( \mathcal{A} \) is a DFA, then \( \overline{\mathcal{A}} \) has the smallest number of states of any DFA accepting \( L \).

**Proof.** If \( L = L(\mathcal{B}) \) for some DFA \( \mathcal{B} \), then there exists a reduced DFA \( \overline{\mathcal{B}} \) with \( L = L(\mathcal{A}) = L(\overline{\mathcal{A}}) = L(\mathcal{B}) = L(\overline{\mathcal{B}}) \). Since \( \overline{\mathcal{A}} \) and \( \overline{\mathcal{B}} \) are reduced then there exists a bijection \( \theta : Q_{\overline{\mathcal{A}}} \to Q_{\overline{\mathcal{B}}} \). Therefore we have

\[ |Q_{\overline{\mathcal{A}}}| = |Q_{\overline{\mathcal{B}}}| \leq |Q_B| \.
\]

Given \( \mathcal{A} \) how do we fine \( \overline{\mathcal{A}} \)? We must calculate \( \sim \). We find a sequence \( \sim_0, \sim_1, \sim_2, \ldots \) of equivalence relations on \( Q \) such that there exists \( k \) with \( \sim_k = \sim \).

Let \( \mathcal{A} = (A, Q, \delta, q_0, F) \) and \( k \geq 0 \).

**Definition:** \( q \sim_k \iff \forall w \in A^*, \delta(q, w) \in F \iff \delta(q', w) \in F \) with \( |w| \leq k \). So \( q \sim_k q' \Rightarrow q \sim_{k-1} q' \Rightarrow \cdots \Rightarrow q \sim_0 q' \) and

\[ q \sim q' \iff q \sim_k q' \text{ for all } k \geq 0 \]
FACTS:
(1) We have that,
\[ q \sim_0 q' \iff \text{for all } w \in A^*, \delta(q, w) \in F \iff \delta(q', w) \in F \text{ where } |w| \leq 0 \]
i.e. \( q \sim_0 q' \Leftrightarrow q, q' \in F \) or \( q, q' \notin F \). So the \( \sim_0 \) classes are \( F \) and \( Q \setminus F \).
(2) \( q \sim_{k+1} q' \iff q \sim_k q' \) and for all \( a \in A \), \( \delta(q, a) \sim_k \delta(q', a) \).
So we can find \( \sim_0, \sim_1, \sim_2, \ldots \), in turn.

EXAMPLE 4.1.

We have that the \( \sim \) classes are

\[
\begin{array}{c|cc}
\sim & a & b \\
0 & 0 & 1 & 2 \\
1 & 4 & 5 \\
2 & 3 & 5 \\
3 & 5 & 5 \\
4 & 5 & 5 \\
5 & 5 & 5 \\
\end{array}
\]

\( \sim_0 \) classes: \( \{0, 1, 2, 5\} \quad \{3, 4\} \)
\( \sim_1 \) classes: \( \{0, 5\} \quad \{1, 2\} \quad \{3, 4\} \)
\( \sim_2 \) classes: \( \{0\} \quad \{5\} \quad \{1, 2\} \quad \{3, 4\} \)
\( \sim_3 \) classes: \( \{0\} \quad \{5\} \quad \{1, 2\} \quad \{3, 4\} \)

MORE FACTS:
(1) \( \sim_k = \sim_{k+1} \Rightarrow \sim_k = \sim_{k+1} = \sim_{k+2} \ldots \)
(2) there exists \( k \) such that \( \sim_k = \sim_{k+1} \)
(3) \( \sim_k = \sim_{k+1} \Rightarrow \sim_k = \sim \)
We note that (4) & (5) ⇒ there exists \( k \) such that \( \sim_k = \sim \). We calculate \( \sim_0, \sim_1, \ldots \) by finding a \( k \) such that \( \sim_k = \sim_{k+1} \) and then \( \sim = \sim_k \).

In our example we have

\[ \sim_2 = \sim_3 \Rightarrow \sim = \sim_2. \]

The reduced DFA equivalent to our example has four states

\[ [0] = \{0\}, \quad [5] = \{5\}, \quad [1] = \{1, 2\}, \quad [4] = \{3, 4\} \]

with initial state [0]. Unique final state [4]. Then we have \( \mathcal{A} \)

5. **Monoids and Transition Monoids**

5.1. **Monoids**

**Definition:** A monoid \( M \) is a set together with a binary operation (so \( M \) is closed under the operation) such that

(i) \((ab)c = a(bc)\) for all \( a, b, c \in M \),

(ii) there exists \( 1 \in M \) such that \( 1a = a = a1 \) for all \( a \in M \).

**Example 5.1.**

(1) Groups are monoids. However \( \mathbb{N} \) under \( \times \) is a monoid which is not a group.

(2) Let \( X \) be a set \( X \neq \emptyset \). \( T_X \) is the set of all functions \( X \to X \) and \( T_X \) is a monoid under \( \circ \) (usually omitted) with identity \( I_X \), called the full transformation monoid on \( X \).

**New Convention:** This applies to all functions except next state functions. If \( \alpha : U \to V \) is a function we write \( u\alpha \) for the image of \( u \in U \) under \( \alpha \) (instead of \( \alpha(u) \)). So, \( I_X : X \to X \) is defined by \( xI_X = x \) for all \( x \in X \). If \( \alpha : U \to V \) and \( \beta : V \to W \) then \( (u\alpha)\beta \) is the
image of \( u \in U \) under first \( \alpha \) and then \( \beta \). Naturally, we write \((u\alpha)\beta = u(\alpha\beta)\), so \( \alpha\beta \) now means “do \( \alpha \), then do \( \beta \)“.

If \( X = \{1, 2, \ldots, n\} \) we write \( T_X \) for \( T \) and \( I_n \) for \( I \). We may use “two-row“ notation for elements of \( T \). If \( \alpha \in T_4 \) is given by

\[
1\alpha = 1 \quad 2\alpha = 1 \quad 3\alpha = 2 \quad 4\alpha = 4.
\]

We can write \( \alpha = \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{array} \right) \) and for example

\[
\left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 3 \end{array} \right) \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 4 \end{array} \right) = \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 2 \end{array} \right).
\]

Note that \( |T_n| = n^n \) because for each element in \( \{1, 2, \ldots, n\} \) there are \( n \) choices for it’s image under a map in \( T_n \). There are \( n \) elements and hence \( |T_n| = n^n \).

### 5.2. Constant Functions in \( T_X \)

\( x \in X \), \( c_x : X \rightarrow X \) is given by \( yc_x = x \) for all \( y \in X \) and is called the constant function on \( x \). For example

\[
c_1 = \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{array} \right) \in T_4.
\]

Note that \( \alpha c_x = c_x \) for all \( \alpha \in T_X \). Since for all \( y \in X \) we have

\[
y(\alpha c_x) = (y\alpha)c_x = x = yc_x
\]

Also, \( c_x\alpha = c_{x\alpha} \) since for all \( y \in X \)

\[
y(c_x\alpha) = (yc_x)\alpha = x\alpha = yc_{x\alpha}
\]

**Definition:** Let \( M \) be a monoid and \( T \subseteq M \). Then \( T \) is a **submonoid** if

1. \( 1 \in T \) and
2. \( a, b \in T \Rightarrow ab \in T \)
**Definition:** Let $M$ be a monoid and $X \subseteq M$. \( \langle X \rangle = \{x_1x_2\ldots x_n \mid n \geq 0 \text{ and } x_i \in X\} \).

Notice that 1 (empty product) lies in \( \langle X \rangle \) and if \( x_1x_2\ldots x_n y_1y_2\ldots y_m \in \langle X \rangle \) (so \( x_i, y_i \in X \)) then

\[
(x_1x_2\ldots x_n)(y_1y_2\ldots y_m) = x_1x_2\ldots x_n y_1y_2\ldots y_m \in \langle X \rangle.
\]

So, \( \langle X \rangle \) is a submonoid of \( M \), the submonoid of \( M \) generated by \( X \). If \( M = \langle X \rangle \), we say \( M \) is generated by \( X \).

For example \( N = \langle P \rangle \), where \( P \) is the set of primes; \( A^* = \langle A \rangle \) under \( X \).

### 5.3. The Transition Monoid of a DFA

Let \( A = (A, Q, \delta, q_0, F) \) be a DFA. For each \( w \in A^* \) let \( \sigma_w \in T_Q \) be defined by

\[
q \sigma_w = \delta(q, w).
\]

**Claim.** \( \sigma_w \sigma_v = \sigma_{wv} \) for all \( w, v \in A^* \).

**Proof.** We have that

\[
q(\sigma_w \sigma_v) = (q \sigma_w) \sigma_v
= \delta(q, w) \sigma_v
= \delta(\delta(q, w), v)
= \delta(q, w) v
= q \sigma_{wv}.
\]

Therefore \( \sigma_w \sigma_v = \sigma_{wv} \). \( \square \)

Now we note that \( q \sigma_\varepsilon = \delta(q, \varepsilon) = q = qI_Q \) and therefore \( \sigma_\varepsilon = I_Q \). Therefore \( M(A) = \{\sigma_w \mid w \in A^*\} \) is a submonoid of \( T_Q \). Now \( M(A) \) is the transition monoid of the DFA \( A \). Note that the initial and final states do not matter for \( M(A) \).

Let \( w = a_1a_2\ldots a_n \in A^* \) where \( a_i \in A \). Then

\[
\sigma_w = \sigma_{a_1a_2\ldots a_n} = \sigma_{a_1} \sigma_{a_2} \ldots \sigma_{a_n}.
\]

Therefore \( M(A) = \langle \sigma_a \mid a \in A \rangle \). Now we note that

\[
|M(A)| \leq |T_Q| = |Q|^{|Q|} < \infty.
\]

**Examples of Finding Transition Monoids**

1. \( A = \{a, b\} \) and \( Q = \{1, 2\} \)
Calculate $\sigma_a, \sigma_b$ – then calculate all products until we don’t obtain any new elements

\[
\begin{array}{c|ccc}
\sigma_a & 1 & 2 \\
\hline 
1 & 2 & 2 \\
2 & 2 & 1 \\
\sigma_b & 2 & 1 \\
\end{array}
\]

Now we have

\[
\begin{align*}
\sigma_a &= c_2, \\
\sigma_a^2 &= \sigma_a \sigma_a = c_2 = \sigma_b = \sigma_b \sigma_a, \\
\sigma_b^2 &= \sigma_b \sigma_b = I_Q, \\
\sigma_a \sigma_b &= \sigma_{ab} = c_1.
\end{align*}
\]

Hence we have $M(\mathcal{A}) = \{I_Q, \sigma_b, c_2, c_1\}$, which will have multiplication table

\[
\begin{array}{c|cccc}
  & I & \sigma_b & c_2 & c_1 \\
\hline
I & I & \sigma_b & c_2 & c_1 \\
\sigma_b & \sigma_b & I & c_2 & c_1 \\
c_2 & c_2 & c_1 & c_2 & c_1 \\
c_1 & c_1 & c_2 & c_2 & c_1 \\
\end{array}
\]

(2) $A = \{a\}$ and $Q = \{1, 2, 3, 4, 5\}$. Now the STD of our DFA is

We have that $M(\mathcal{A}) = \langle \sigma_a \rangle = \{\sigma_a^n \mid n \geq 0\}$. Calculate $\sigma_a, \sigma_a^2 = \sigma_a^2, \sigma_a^3, \ldots$ So we have that $M(\mathcal{A}) = \{i, \sigma_a, \sigma_a^2, \sigma_a^3, \sigma_a^4\}$.

Note. We have that $T = \{\sigma_a^2, \sigma_a^3, \sigma_a^4\}$ is a 3 element subgroup of $M(\mathcal{A})$.

(3) $A = \{a, b\}$ and $Q = \{1, 2, 3\}$. The STD of our DFA is
We now have our table of transitions to be

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_a$</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>$\sigma_a^2$</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>$\sigma_a^3$</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>$\sigma_a^4$</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>$\sigma_a^5$</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

We now have our table of transitions to be

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_a$</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$\sigma_a^2$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$\sigma_a^3$</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$\sigma_a\sigma_a^2$</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$\sigma_a\sigma_a^3$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Thus we have $M(A) = \{I, \sigma_a, \sigma_a^2, c_1, c_2, c_3\}$. This has multiplication table
5.4. Some Notation for Functions

Let \( \theta : A \to B \) be a function and \( R \subseteq A, S \subseteq B \). Then we define

\[
R \theta = \{ a \theta \mid a \in R \}
\]
\[
S \theta^{-1} = \{ a \in A \mid a \theta \in S \}
\]

where \( S \theta^{-1} \) is the inverse image of \( S \) under \( \theta \). The notation \( S \theta^{-1} \) does NOT imply the function \( \theta^{-1} \) exists.

**Example 5.2.** \( A = \{1, 2, 3\} \), \( B = \{a, b, c\} \) and \( \theta : A \to B \) given by

\[
1 \theta = b \quad 2 \theta = b \quad 3 \theta = a.
\]

It is clear to see that \( \theta \) is not a bijection and hence \( \theta^{-1} \) does not exist. Now we have

\[
\begin{align*}
(1, 2) \theta &= \{1 \theta, 2 \theta\} = \{b\} \\
\{1\} \theta &= \{b\} \\
\emptyset \theta &= \emptyset
\end{align*}
\]
\[
\begin{align*}
\{b\} \theta^{-1} &= \{1, 2\} = \{b, c\} \theta^{-1} \\
\{a\} \theta^{-1} &= \{3\} \\
\{c\} \theta^{-1} &= \emptyset \\
\emptyset \theta^{-1} &= \emptyset
\end{align*}
\]

**Note.** \( (1, 2) \theta^{-1} = \{b\} \theta^{-1} = \{1, 2\} \) so we have \( \{1\} \theta \theta^{-1} \neq \{1\} \).

Let \( \theta : A \to B \), \( S_1, S_2 \subseteq A \) and \( R_1, R_2 \subseteq B \). Some facts:

1. \( (S_1 \cup S_2) \theta^{-1} = S_1 \theta^{-1} \cup S_2 \theta^{-1} \),
2. \( (R_1 \cap R_2) \theta = R_1 \theta \cap R_2 \theta \),
3. \( (R_1 \cap R_2) \theta \subseteq R_1 \theta \cap R_2 \theta \), (induction may be strict)
4. \( (S_1 \cap S_2) \theta^{-1} = S_1 \theta^{-1} \cap S_2 \theta^{-1} \).

**Proof.**

1. We have that
\[ x \in (S_1 \cup S_2)\theta^{-1} \iff x\theta \in S_1 \cup S_2 \]
\[ \iff x\theta \in S_1 \text{ or } x\theta \in S_2 \]
\[ \iff x \in S_1\theta^{-1} \text{ or } x \in S_2\theta^{-1} \]
\[ \iff x \in S_1\theta^{-1} \cup S_2\theta^{-1} \]

5.5. The Syntactic Monoid of a Language

Let \( L \) be a language over \( A \). For \( u \in A^* \) we have

\[ c_L(u) = \{(w, z) \in A^* \times A^* \mid wuz \in L\} \]

the context of \( u \). Now define \( \sim_L \) on \( A^* \) by

\[ u \sim_L v \text{ iff } c_L(u) = c_L(v). \]

It is clear that \( \sim_L \) is an equivalence relation on \( A^* \).

**Lemma 5.1.** \( u \sim_L v \) and \( u' \sim_L v' \) \( \Rightarrow \) \( uu' \sim_L vv' \).

**Proof.** Suppose \( u \sim_L v \) and \( u' \sim_L v' \). Then

\[(w, z) \in c_L(uu') \iff wuu'z \in L \]
\[ \iff w(u'z) \in L \]
\[ \iff (w, u'z) \in c_L(u) \]
\[ \iff (w, u'z) \in c_L(v) \]
\[ \iff wvu'z \in L \]
\[ \iff (wu)v'u'z \in L \]
\[ \iff (wu, z) \in c_L(u') \]
\[ \iff (wu, z) \in c_L(v') \]
\[ \iff wvu'z \in L \]
\[ \iff (w, z) \in c_L(vv'). \]

Hence we have \( uu' \sim_L vv' \). \( \square \)

Now set \( M(L) = \{[w] \mid w \in A^*\} \) and define a ‘product’ on \( M(L) \) by \([u][v] = [uv]\). If \([u] = [u']\) and \([v] = [v']\) then \( u \sim_L u' \) and \( v \sim_L v' \), so by the Lemma above

\[ uv \sim_L u'v' \]

and so \([uv] = [u'v']\). Hence our ‘product’ above is a well-defined binary operation on \( M(L) \).

**Lemma 5.2.** \( M(L) \) is a monoid under this binary operation.
Proof. For all $[u], [v], [w] \in M(L)$ then

$$[u][v][w] = [u][v][w] = [u][w][v] = [(uv)(vw) = (uv)[w] = ([u][v])[w].$$

Also we have that $[\varepsilon][u] = [\varepsilon][u] = [u] = [u][\varepsilon] = [u][\varepsilon]$ and hence $[\varepsilon]$ is the identity of $M(L)$. Thus $M(L)$ is a monoid. $\square$

Some terminology:

- $\sim_L$ is the syntactic congruence of $L$
- $M(L)$ is the syntactic monoid of $L$.

Note. Suppose $u \in L$ and $u \sim_L v$. We have $(\varepsilon, \varepsilon) \in c_L(u) = c_L(v)$. We have that $v = \varepsilon v \varepsilon \Rightarrow v \in L$. Therefore $L$ is a union of $\sim_L$-classes.

Calculation of $M(L)$

Example 5.3. Take $A = \{a, b\}$ and $L = A$. For $w \in A^*$ with $|w| > 1$, we have

$$c_L(w) = \emptyset,$$

$$c_L(\varepsilon) = \{(\varepsilon, a), (a, \varepsilon), (\varepsilon, b), (b, \varepsilon)\},$$

$$c_L(a) = \{(\varepsilon, \varepsilon)\} = c_L(b).$$

So, there exists three $\sim_L$-classes;

$$\{\varepsilon\} = [\varepsilon] = 1 \quad \{a, b\} = [a] = L \quad \{w \in A^* \mid |w| \geq 2\} = T.$$

So the multiplication table of our monoid is

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>L</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>L</td>
<td>T</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

because we have

$$LL = [a][a] = [a^2] = T,$$

$$LT = [a][a^2] = [a^3] = T.$$

Note $T$ is zero for $M(L)$ – had we known we could have used 0 for $T$.

Example 5.4. $A = \{a, b\}$ and $L = \{ba, ab\}$. Now the contexts are
\[ c_L(\varepsilon) = \{ (\varepsilon, ba), (b, a), (ba, \varepsilon), (\varepsilon, ab), (a, b), (ab, \varepsilon) \} \]
\[ c_L(a) = \{ (b, \varepsilon), (\varepsilon, b) \} \]
\[ c_L(b) = \{ (\varepsilon, a), (a, \varepsilon) \} \]
\[ c_L(ba) = \{ (\varepsilon, \varepsilon) \} = c_L(ab) \]
\[ c_L(a^2) = \emptyset = c_L(b^2) = c_L(w) \]

for all \( w \) with \( |w| \geq 3 \). So, there exists 5 \( \sim_L \)-classes:

\[ [\varepsilon] = \{ \varepsilon \} = 1 \quad [a] = [a] = P \quad [b] = [b] = Q \quad [ab] = [ab, ba] = L \quad [a^2] = \{ a^2, b^2, w \mid |w| \geq 3 \} = 0. \]

So, \( M(L) = \{ 1, P, Q, L, 0 \} \) and has multiplication table

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>P</th>
<th>Q</th>
<th>L</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>P</td>
<td>Q</td>
<td>L</td>
<td>0</td>
</tr>
<tr>
<td>P</td>
<td>P</td>
<td>0</td>
<td>L</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q</td>
<td>Q</td>
<td>L</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

We know the above because

\[ P^2 = [a][a] = [a^2] = 0, \]
\[ PQ = [a][b] = [ab] = L, \]
\[ PL = [a^2b] = 0. \]

6. Recognition of a Monoid

**Definition:** Let \( M, N \) be monoids. Then \( \theta : M \to N \) is a \((monoid)\) morphism if

(i) \( (ab)\theta = a\theta b\theta \),
(ii) \( 1_M \theta = 1_N \).

**Why is the free monoid called free?**

Let \( A \) be an alphabet, \( M \) a monoid and \( \varphi : A \to M \) a function. Then there exists a unique morphism \( \theta : A^* \to M \) such that \( a\theta = a\varphi \) for all \( a \in A \).

**Proof.** Define \( \theta : A^* \to M \) by

\[ \varepsilon \theta = 1 \]
\[ (a_1 \ldots a_n)\theta = a_1 \varphi \ldots a_n \varphi \]
(a_i \in A). Clearly \( \theta \) is well-defined; it is easy to check that \( \theta \) is a morphism. For any \( a \in A \) we have \( a\theta = a\varphi \).

If \( \psi : A^* \to M \) is a morphism such that \( a\psi = a\varphi \) for all \( a \in A \), then \( \varepsilon\psi = 1 = \varepsilon\theta \). Now for all \( w = a_1a_2 \ldots a_n, a_i \in A, n \geq 1 \) we have

\[
\begin{align*}
  w\psi &= (a_1 \ldots a_n)\psi = a_1\psi \ldots a_n\psi \\
  &= a_1\varphi \ldots a_n\varphi \\
  &= (a_1 \ldots a_n)\theta \\
  &= w\theta.
\end{align*}
\]

Therefore \( \psi = \theta \) and \( \theta : A^* \to M \) is the unique morphism such that \( a\theta = a\varphi \) for all \( a \in A \). \( \square \)

**Definition:** Let \( L \subseteq A^* \) and let \( M \) be a monoid. Then \( L \) is **recognised** by \( M \) if there exists a morphism \( \theta : A^* \to M \) such that \( L = (L\theta)\theta^{-1} \).

**Remark.** We know \( L \subseteq (L\theta)\theta^{-1} \). For \( L = (L\theta)\theta^{-1} \), we need that \( w \in (L\theta)\theta^{-1} \Rightarrow w \in L \).

\[
\begin{align*}
  w\theta &\in L\theta \Rightarrow w \in L \\
  w\theta = v\theta, \text{ some } v \in L \Rightarrow w \in L.
\end{align*}
\]

**Theorem 6.1.** Let \( L \) be a language. Then \( L \) is recognised by \( M(L) \).

**Proof.** Define \( \nu_L : A^* \to M(L) \) by \( w\nu_L = [w] \), then \( \varepsilon\nu_L = [\varepsilon] \), which is the identity of \( M(L) \) and

\[
(wv)\nu_L = [wv] = [w][v] = w\nuLv\nu_L.
\]

Hence \( \nu_L \) is a morphism. Suppose \( w \in (L\nu_L)\nu_L^{-1} \). Then \( w\nu_L \in L\nu_L \), so \( w\nu_L = v\nu_L \) for some \( v \in L \). We have \( [w] = [v] \) by definition of \( \nu_L \), hence \( w \sim_L v \). As \( (\varepsilon, \varepsilon) \in c_L(v) \) we must have \( (\varepsilon, \varepsilon) \in c_L(w) \) so that \( w \in L \). Hence \( (L\nu_L)\nu_L^{-1} \subseteq L \) so that \( (L\nu_L)\nu_L^{-1} = L \) and hence \( L \) is recognised by \( M(L) \). \( \square \)

**Theorem 6.2.** The following are equivalent for a language \( L \subseteq A^* \):

(i) \( M(L) \) is finite;
(ii) \( L \) is recognised by a finite monoid;
(iii) \( L \in \text{Rec} A^* \).

**Proof.** (i) \( \Rightarrow \) (ii) from the above.

(ii) \( \Rightarrow \) (iii): Let \( M \) be a finite monoid and \( \theta : A^* \to M \) a morphism such that \( L = (L\theta)\theta^{-1} \). Let \( \mathcal{A} = (A, M, \delta, 1_M, L\theta) \) where \( \delta(m, a) = m(a\theta) \). Check \( \delta(m, w) = m(w\theta) \) for all \( w \in A^* \). Then
\[ w \in L(A) \iff \delta(1, w) \in L\theta, \]
\[ \iff 1(w\theta) \in L\theta, \]
\[ \iff w\theta \in L\theta, \]
\[ \iff w \in (L\theta)\theta^{-1}, \]
\[ \iff w \in L \text{ as } (L\theta)\theta^{-1}L. \]

Hence \( L(A) = L \) so \( L \) is recognisable by \( A \).

(iii) \( \Rightarrow \) (i): If \( L \in \text{Rec } A^* \) then \( L = L(A) \) for some reduced (accessible) DFA \( A = (A, Q, \delta, q_0, F) \).

**Claim.** We claim that for \( u, v \in A^* \), \( u \sim_L v \iff \sigma_u = \sigma_v \). So, the number of \( \sim_L \)-classes \( = |M(A)| \leq |T_Q| \leq |Q|^{[Q]} < \infty \).

**Proof.** We have that

\[ u \sim_L v \iff c_L(u) = c_L(v), \]

\[ \iff ((w, z) \in c_L(u) \iff (w, z) \in c_L(v)), \]

\[ \iff (wuz \in L \iff wvz \in L \forall w, z \in A^*), \]

\[ \iff \forall w, z \in A^*, \]

\[ \delta(q_0, wuz) \in F \iff \delta(q_0, wvz) \in F \]

\[ \iff \forall q \in Q \forall z \in A^*, \]

\[ \delta(\delta(q_0, w), uz) \in F \iff \delta(\delta(q_0, w), vz) \in F \]

\[ \iff \forall q \in Q \forall z \in A^*, \]

\[ \delta(q, uz) \in F \iff \delta(q, vz) \in F \]

\[ \iff \forall q \in Q \forall z \in A^*, \]

\[ \delta(\delta(q, u), z) \in F \iff \delta(\delta(q, v), z) \in F \]

\[ \iff \forall q \in Q, \delta(q, u) \sim \delta(q, v) \]

\[ \iff \forall q \in Q, \delta(q, u) = \delta(q, v) \]

\[ \iff \forall q \in Q, q\sigma_u = q\sigma_v \]

\[ \iff \sigma_u = \sigma_v \] \( \Box \)

Hence all statements are equivalent. \( \Box \)

We have now proved the following

**Theorem 6.3.** Let \( L \) be a language over \( A^* \). The following are equivalent;

(i) \( L \) is recognisable \( (L \in \text{Rec } A^*; \ L = L(A) \text{ for some DFA } A) \);

(ii) \( L = L(A) \) for some NDA \( A \);
(iii) $L$ is rational ($L \in \text{Rat} A^*$);
(iv) $L$ is recognised by a finite monoid $M$ (i.e. there exists a morphism $\theta : A^* \to M$ such that $L = (L\theta)\theta^{-1}$);
(v) $M(L)$ is finite.

Common terminology for a language satisfying any of these equivalent conditions is regular.

Let $L \in \text{Rec} A^*$; we know that $M(L)$ is finite. How do we calculate it? Either directly by finding contexts; or we find a DFA $\mathcal{A}$ with $L = L(\mathcal{A})$, reduce $\mathcal{A}$ to $\mathcal{A}'$ with $L = L(\mathcal{A}')$ and find $M(\mathcal{A}')$, then use the following.

**Proposition.** If $L = L(\mathcal{A})$ for a reduced DFA $\mathcal{A}$, then $M(L) = M(\mathcal{A})$, i.e. there exists a bijective morphism (an isomorphism) $\theta : M(L) \to M(\mathcal{A})$.

**Proof.** We have

$$M(L) = \{[u] \mid u \in A^*\} \text{ where } u \sim_L v \iff c_L(u) = c_L(v),$$

$$M(\mathcal{A}) = \{\sigma_u \mid u \in A^*\} \text{ where } q\sigma_u = \delta(q, u).$$

From an earlier result, $\theta : M(L) \to M(\mathcal{A})$ given by $[u]\theta = \sigma_u$ is a bijection. Let $[u], [v] \in M(L)$. Then

$$([u][v])\theta = [uv]\theta = \sigma_{uv} = \sigma_u\sigma_v = [u]\theta[v]\theta.$$

The identity of $M(L)$ is $[\varepsilon]$ and

$$[\varepsilon]\theta = \sigma_\varepsilon = I_Q \quad \text{(identity of } M(\mathcal{A})).$$

Therefore $\theta$ is a morphism and hence an isomorphism as required. $\square$

### 7. How do Monoids help us?

Let $L \subseteq A^*$, $w \in A^*$.

**Definition:** $w^{-1}L = \{v \in A^* \mid vw \in L\}$.

**Lemma 7.1.** $L \in \text{Rec} A^* \Rightarrow w^{-1}L \in \text{Rec} A^*$ for any $w \in A^*$.

**Proof.** $L \in \text{Rec} A^* \Rightarrow L$ is recognised by a finite monoid $M$. Hence there exists a morphism $\theta : A^* \to M$ such that

$$L = (L\theta)\theta^{-1}$$

We show $(w^{-1}L)\theta^{-1} = w^{-1}L$. We know

$$w^{-1}L \subseteq ((w^{-1}L)\theta)\theta^{-1}.$$ 

Now
Recall that a language $L$.

Note we can replace (ii) above with $A$.

Then $(wv)\theta = w\theta v\theta = w\theta x\theta = (wx)\theta \in L\theta \Rightarrow wv \in (L\theta)\theta^{-1} = L$. Hence $v \in w^{-1}L$ and so $(w^{-1}L)\theta^{-1} \subseteq w^{-1}L$ as required. \hfill \Box

RECALL: We needed that

$$L = \{ a^n b^p \mid n \geq 1, p \text{ prime} \} \not\subseteq \text{Rec } A^*.$$  

We argued that $K = \{ a^n b^p \mid n \geq 0, p \text{ prime} \} \not\subseteq \text{Rec } A^*$. We have that $u \in a^{-1}L \iff au \in L \iff u \in K$. Hence $a^{-1}L = K$. If $L \in \text{Rec } A^*$, then we would have $a^{-1}L \in \text{Rec } A^*$, i.e. $K \in \text{Rec } A^*$ – a contradiction. Hence $L \not\subseteq \text{Rec } A^*$ as required.

**Lemma 7.2.** $L, K \in \text{Rec } A^* \Rightarrow L \cap K \in \text{Rec } A^*$.

**Proof.** There exists finite monoids $M, N$ and morphisms $\theta : A^* \rightarrow M$ and $\psi : A^* \rightarrow N$ such that $L = (L\theta)\theta^{-1}$, $K = (K\psi)\psi^{-1}$. Now we have that $M \times N$ is a finite monoid under

$$(m, n)(m', n') = (mm', nn')$$  

with identity $(1_M, 1_N)$. Define $\varphi : A^* \rightarrow M \times N$ by $w\varphi = (w\theta, w\psi)$. Check $\varphi$ is a morphism.

We know $L \cap K \subseteq ((L \cap K)\varphi)\varphi^{-1}$. Let $w \in ((L \cap K)\varphi)\varphi^{-1}$. Then $w\varphi \in (L \cap K)\varphi$, so there exists $u \in L \cap K$ with $w\varphi = u\varphi$. Hence $(w\theta, w\psi) = (u\theta, u\psi)$, so

$$w\theta = u\theta \quad \text{and} \quad w\psi = u\psi.$$  

As $u \in K$, $w \in (L\theta)\theta^{-1} = L$ and as $u \in K$, $w \in (K\psi)\psi^{-1} = K$. Hence $w \in L \cap K$ so that $((L \cap K)\varphi)\varphi^{-1} \subseteq L \cap K$. Hence $L \cap K = ((L \cap K)\varphi)\varphi^{-1}$ and $L \cap K$ is recognisable by $M \times N$, hence $L \cap K \in \text{Rec } A^*$. \hfill \Box

**8. Schützenberger's Theorem**

Recall that a language $L \subseteq A^*$ is rational if

(i) $L$ is finite or
(ii) $L$ can be obtained from finite subsets of $A^*$ by applying rational operations ($\cup$, product, star) a finite number of times.

Note we can replace (ii) above with

(ii)' $L$ can be obtained from subsets of $A^*$ by applying $\cup$, $\cap$, $\cdot$, product and star a finite number of times (as Rat $A^* = \text{Rec } A^*$ it is closed under $\cap$ and $\cdot$).

**Definition:** $L \subseteq A^*$ is star-free if

(1) $L$ is finite or
(2) $L$ can be obtained from finite languages by applying product and the boolean operations of $\cup$, $\cap$, $^c$ a finite number of times.

We have that if $L$ is star-free then $L \in \text{Rec} A^*$ (as $\text{Rec} A^*$ contains the finite languages and is closed under Boolean operations and product). $L$ star-free $\Rightarrow L \in \text{Rat} A^*$ (by Kleene’s Theorem).

**Example 8.1.**

(a) $\{ab, a, bab\}, \emptyset, \{\varepsilon\}$ are finite, hence star-free.

(b) $\{ab, a\}^c\{ba, aba\} \cup (\{aa\}^c \cap \{bb\}^c)$ is star-free.

(c) $A^* = \emptyset^c$ so $A^*$ is star-free.

(d) Let $A = \{a, b, c\}$ then

$$\{a\}^* = (A^*bA^* \cup A^*cA^*)^c = (\emptyset^c b \emptyset^c \cup \emptyset^c c \emptyset^c)^c$$

is star-free.

(e) $L = \{x \in A^* \mid |x|_a \geq 1\} = A^*aA^* = \emptyset^c a \emptyset^c$ is star-free.

(f) $(ab)^* = (bA^* \cup A^*a \cup A^*aaA^* \cup A^*bbA^*)^c$ is star-free.

(g) $(aa)^*$ is not star-free.

**Definition:** Let $M$ be a monoid and let $G \subseteq M$ then $G$ is a subgroup of $M$ if

1. $G$ is closed $a, b \in G \Rightarrow ab \in G$;
2. there exists $e \in G$ such that $ea = a = ae$ for all $a \in G$;
3. for all $a \in G$ there exists $b \in G$ such that $ab = e = ba$.

i.e. $G$ is a group under the restriction of the binary operation on $M$ to the subset $G$.

**Definition:** $e \in M$ is idempotent if $e = e^2$ then we have $E(M)$ is the set of idempotents of $M$.

**Example 8.2.**

(i) $e \in E(M) \Rightarrow \{e\}$ is a subgroup, a trivial subgroup with identity $e$.

(ii) $S_X$ is a subgroup of $T_X$.

(iii) $\text{GL}_n(\mathbb{R})$ is a subgroup of $M_n(\mathbb{R})$.

(iv) We have multiplication table

\[
\begin{array}{ccc|c}
I & \alpha & 0 \\
\hline
I & I & \alpha \\
\alpha & \alpha & I \\
0 & 0 & 0 & 0 \\
\end{array}
\]

\{0\}, \{I\} are subgroups and \{I, \alpha\} is a subgroup.

(v) From the example of finding $M(\mathcal{A})$ number 2
Let $T = \{\sigma_a^2, \sigma_a^3, \sigma_a^4\}$. By inspection $T$ is closed, $\sigma_a^3$ is the identity and $(\sigma_a^3)^2 = \sigma_a^3$, $\sigma_a^2$ and $\sigma_a^4$ are mutually inverse. Now

$$\sigma_a^2 \sigma_a^4 = \sigma_a^3 = \sigma_a^4 \sigma_a^2.$$ 

So $T$ is a subgroup of $M(A)$.

**Definition:** A finite monoid $M$ is *aperiodic* if all of its subgroups are trivial.

**Theorem 8.1** (Schützenbergers Theorem). A language $L$ is star-free $\iff M(L)$ is finite and aperiodic.

**Proof.** No proof in this course. □

**Example 8.3.** $L = (aa)^* \subseteq \{a, b\}^*$ with DFA

![DFA Diagram](attachment:dfa.png)

Now we have that $L(A) = L$. The $\sim$-classes are

$\sim_0$ -classes: $\{0\}, \{1, 2\}$,

$\sim_1$ -classes: $\{0\}, \{1\}, \{2\}$.

Hence $\sim = \sim_1$ and the $\sim$-classes are $\{0\}, \{1\}, \{2\}$ and so $A$ is reduced. We have that $M(L) \cong M(A)$, clearly $M(L)$ is finite. The transition table for this is

$$
\begin{array}{c|ccc}
\sigma_a & 0 & 1 & 2 \\
\sigma_a^2 & 1 & 0 & 2 \\
\sigma_b & 2 & 2 & 2 \\
\sigma_a^3 & 0 & 1 & 2 \\
\end{array}
$$
Hence $M(\mathcal{A}) = \{I, \sigma_a, c_2\}$. Now $M(\mathcal{A})$ has table

\[
\begin{array}{ccc}
  I & \sigma_a & c_2 \\
  I & \sigma_b & c_2 \\
  \sigma_a & I & c_2 \\
  c_2 & c_2 & c_2 \\
\end{array}
\]

Now $\{I, \sigma_a\}$ is a subgroup. So $M(L)$ is not aperiodic hence $L$ is not star-free by Schützenbergers' theorem.