FORMAL LANGUAGES & AUTOMATA 2021/22

VICTORIA GOULD

The module investigates the relationship between a special kind of machine (automata), special languages (regular languages) and a special kind of algebra (monoids).

Machines	$\longleftrightarrow$	Languages	$\longleftrightarrow$	Algebra
Automata	$\longleftrightarrow$	Regular Languages	$\longleftrightarrow$	Monoids

1. Fundamental concepts

1.1. Alphabets, Words and Languages

We will study (sets of) finite sequences of symbols.

Definition 1.1.
- 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.
- The *empty word* is denoted by ε (in some books 1 or λ).
- If $a_1, a_2, \ldots, a_n, a'_1, a'_2, \ldots, a'_m \in A$, then

$$a_1a_2\ldots a_n = a'_1a'_2\ldots a'_m \Leftrightarrow n = m \text{ and } a_i = a'_i, 1 \leqslant i \leqslant n.$$

- $A^+ = \{a_1a_2\ldots a_n \mid n \in \mathbb{N}, a_i \in A, 1 \leqslant i \leqslant n\}$ is the set of all *non-empty* words over A.
- $A^* = A^+ \cup \{\varepsilon\}$ is the set of *all* words over A.

Example 1.2. (i) $A = \{0, 1\}$; 0, 10, 01011 are words over A.
(ii) $A = \{a, b\}$: $a, b, ab, ba, aaa, aab, \ldots$ are words over A.
(iii) If A is the English alphabet $\{a, b, \ldots, z\}$ then *cat* and *atz* are words over A.

Definition 1.3. A *language* (over A) is a subset of A^*.
A language L is *finite* if $|L| < \infty$ and *cofinite* if $|L^c| = |A^* \setminus L| < \infty$.

Example 1.4. $\emptyset, \{\varepsilon\}, \{a, b, ba\}$ are finite languages.
A^+ is cofinite as $A^* \setminus A^+ = \{\varepsilon\}$.

LENGTH OF WORDS For $w \in A^*$ define the length $|w|$ of w to be the no. of letters in w. Hence $|\varepsilon| = 0$ and $|a_1 a_2 \dots a_n| = n$ where $a_i \in A$.

EXAMPLE 1.5. $|abab| = 4$, $|a| = 1$ and $|aa| = |ab| = 2$.
$L = \{w : |w| \geq 2\}$ is cofinite as

$$L^c = \{w : |w| = 0\} \cup \{w : |w| = 1\} = \{\varepsilon\} \cup A.$$

1.2. **Monoids**

DEFINITION 1.6. A *monoid* is a set M together with an associative binary operation and having an identity. i.e.

- for all $a, b \in M$ there exists a unique $ab \in M$;
- for all $a, b, c \in M$ we have $(ab)c = a(bc)$;
- there exists $1 \in M$ such that $1a = a = a1$ for all $a \in M$.

Note. The identity of M is unique.

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 1.7. Let $x = ab$ and $y = bca$ then

$$xy = abbca, \; yx = bcaab.$$

Notice that $xy \neq yx$.

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

For $a \in A$, a^n $(n \geqslant 0)$ is the word consisting of n a's, i.e. $a^0 = \varepsilon$, $a^1 = a$, $a^2 = aa$, $a^3 = aaa$, etc.
We have $\{a\}^* = \{\varepsilon, a, aa, aaa, \dots\} = \{\varepsilon, a, a^2, a^3, \dots\} = \{a^n \mid n \geqslant 0\}$.

We often write a^* for $\{a\}^*$.
More generally, for any $x \in A^*$ (or, in any monoid), $x^0 = \varepsilon$ and for $n \in \mathbb{N}$ we have

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

e.g. If $x = ab$ then $x^3 = ababab$.

THE INDEX LAWS For any monoid M and $x \in M, n, m \geqslant 0$ we have

$$x^n x^m = x^{n+m} \text{ and } (x^n)^m = x^{nm}.$$

You have seen this for groups/rings - the proof depends only on associativity.

1.3. More on Words

Letter Count

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

Example 1.8. 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 ε is a prefix of x for any $x \in A^*$ as $x = \varepsilon x$.
Any word $x \in A^*$ is a prefix of itself because $x = x\varepsilon$.
e.g. If $x = a^2b$, then the prefixes of x are

$$\varepsilon, a, a^2, a^2b.$$

Suffix: dual to prefix

If $x = a^2b$, then the suffices of x are

$$\varepsilon, b, ab, a^2b.$$

1.4. 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 1.9. If we have $\{a, ab\}$ and $\{b, bc\}$ are languages then

$$\{a, ab\}\{b, bc\} = \{ab, abc, abb, abbc\}.$$

FACT $(KL)M = K(LM)$ for any languages K, L, M (See Exercises).
Further

$$\{\varepsilon\}L = L = L\{\varepsilon\}$$

for any language L. So,

$$\mathscr{L}(A) = \{L : L \text{ is a language over } A\}$$

forms a monoid.

SHORTHAND: for $w \in A^*$ and $L \subseteq A^*$, usually write wL for $\{w\}L$ and Lw for $L\{w\}$, etc. e.g.

$$wL = \{wv \mid v \in L\}$$

and

$$KwL = K\{w\}L = \{uwv \mid u \in K, v \in L\}.$$

We define:

$$L^0 = \{\varepsilon\} \text{ and for } n \geq 1, L^n = \underbrace{L \dots L}_{n \text{ times}}.$$

So $L^1 = L, L^2 = LL = \{uv : u, v \in L\}, L^3 = LLL, \dots, L^{n+1} = L^n L$.

The (Kleene) Star: of $L \subseteq A^*$ is

$$\begin{aligned} L^* &= \{x_1 x_2 \dots x_n \mid n \geqslant 0 \text{ and } x_i \in L, 1 \leqslant i \leqslant n\} \\ &= L^0 \cup L^1 \cup L^2 \cup \dots \\ &= \bigcup_{n \geqslant 0} L^n. \end{aligned}$$

For any $w \in A^*$ we have

$$\{w\}^* = \{w\}^0 \cup \{w\}^1 \cup \{w\}^2 \cup \dots = \{w^n : n \geq 0\}$$

and in particular, if $a \in A$ then

$$\{a\}^* = \{a^n : n \geq 0\}.$$

Example 1.10. (i) $a \in A$, $L = \{a^2\}$ then we have

$$L^* = \{\varepsilon, a^2, a^4, a^6, \dots\} = \{a^{2n} \mid n \geqslant 0\}$$

(ii) $a, b \in A$, $L = \{ab, ba\}$ then we have

$$L^* = \{\varepsilon, ab, ba, abab, abba, baba, baab, \dots\};$$

(iii) $\{\varepsilon\}^0 = \{\varepsilon\}$ (by definition); and for $n \geq 1$,

$$\{\varepsilon\}^n = \{\varepsilon^n : n \in \mathbb{N}\} = \{\varepsilon\},$$

so that $\{\varepsilon\}^* = \{\varepsilon\}$;
(iv) $\emptyset^0 = \{\varepsilon\}$ (by definition); and for $n \geq 1$,

$$\emptyset^n = \{x_1 \dots x_n : x_i \in \emptyset\} = \emptyset,$$

so that

$$\emptyset^* = \{\varepsilon\} \cup \emptyset = \{\varepsilon\};$$

(v) $\{a, a^2\}^* = \{a\}^*$.

Notational hazard If $L = \{w\}$ sometimes write w^* for $\{w\}^*$ but be careful:

$$ab^* \text{ means } \{a\}\{b\}^* = \{a\}\{b^n : n \geqslant 0\} = \{ab^n \mid n \geqslant 0\};$$

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

$$(ab)^* = \big\{(ab)^n \mid n \geqslant 0\big\} = \{\varepsilon, ab, abab, ababab, \dots\}.$$

Thus we have A^*aab^*aa means

$$A^*\{aa\}\{b\}^*\{aa\} = \{waab^naa \mid w \in A^*, n \geqslant 0\}.$$

2. Automata: DFAs

A point of grammar – the singular form of automata is automaton.
We concentrate on two kinds of finite state automata.

DFA: deterministic finite state automata (which are also complete)
NDA: non-deterministic finite state automata (which do not have to be complete).

Definition 2.1. A *DFA* is a 5-tuple

$$\mathscr{A} = (A, Q, \delta, q_0, F)$$

where we have

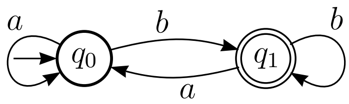
- A is an alphabet (so $0 < |A| < \infty$),
- Q is a finite set of "states",
- $q_0 \in Q$ is the *initial state*,
- $F \subseteq Q$ is the set of *final* (or *accepting*, or *terminal*) states,
- $\delta : Q \times A \to Q$ is the *state transition function* or *next state function*.

2.1. (State) Transition Diagrams (t.d.s)

States are represented by $\bigcirc$

- State q is $\textcircled{q}$
- Final state is $\circledcirc$
- Initial state by $\to\bigcirc$
- Indicate $\delta(q,a) = p$ by $\textcircled{q} \xrightarrow{a} \textcircled{p}$

EXAMPLE 2.2. Let $A = \{a, b\}$ then the following



is the state transition diagram of the DFA

$$\mathscr{A} = \big(\{a,b\}, \{q_0, q_1\}, \delta, q_0, \{q_1\}\big).$$

Now we describe δ as

$$\begin{aligned} \delta(q_0, a) = q_0, \delta(q_0, b) = q_1, \\ \delta(q_1, a) = q_0, \delta(q_1, b) = q_1. \end{aligned}$$

We can describe δ by a table

	a	b
q_0	q_0	q_1
q_1	q_0	q_1

Extended next state function

For a DFA $\mathscr{A} = (A, Q, \delta, q_0, F)$ we extend δ to give a function $\delta : Q \times A^* \to Q$, defined inductively as follows

$$\begin{array}{lcll} \delta(q, \varepsilon) & = & q & \forall q \in Q, \\ \delta(q, wa) & = & \delta\big(\delta(q, w), a\big) & \forall w \in A^*, \forall a \in A, \forall q \in Q. \end{array}$$

Returning to the example above we have

$$\begin{aligned}\delta(q_0, aba) &= \delta\big(\delta(q_0, ab), a\big)\\ &= \delta\big(\delta\big(\delta(q_0, a), b\big), a\big)\\ &= \delta\big(\delta(q_0, b), a\big)\\ &= \delta(q_1, a)\\ &= q_0\end{aligned}$$

Lemma 2.3. *THE δ-LEMMA For all $u, v \in A^*$ we have*

$$\delta(q, uv) = \delta\big(\delta(q, u), v\big).$$

Proof. By induction on $|v|$ - see Exercises. $\square$

Complete and deterministic

For a DFA $\mathscr{A} = (A, Q, \delta, q_0, F)$ we have $\delta : Q \times A \to Q$ is *a function.*

Because δ is a function we have for all $(q, a) \in Q \times A$, $\delta(q, a)$ is DEFINED - we thus say $\mathscr{A}$ is *complete.*

Also for all $(q, a) \in Q \times A$, $\exists$ a UNIQUE $\delta(q, a)$ - we say $\mathscr{A}$ is *deterministic.*

Definition 2.4. (i) A word $w \in A^*$ is *accepted* by $\mathscr{A}$ if $\delta(q_0, w) \in F$ and $w \in A^*$ is *rejected* by $\mathscr{A}$ if $\delta(q_0, w) \notin F$.
(ii) The language *recognised* by $\mathscr{A}$ is

$$L(\mathscr{A}) = \{w \in A^* \mid \delta(q_0, w) \in F\},$$

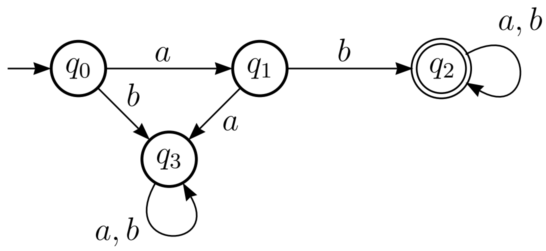
i.e. the set of words that $\mathscr{A}$ accepts.
(iii) A language $L \subseteq A^*$ is *recognisable* if there exists a DFA $\mathscr{A}$ with $L = L(\mathscr{A})$.

The DFA in (iii) will not be unique!

Example 2.5. Let $A = \{a, b\}$. Find a DFA which recognises

$$L = \{w \in A^* \mid w \text{ has prefix } ab\} = abA^*.$$

Draw

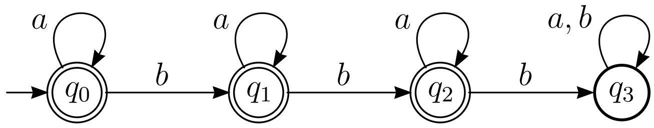


We see that $L(\mathscr{A}) = L$.

Example 2.6. Let $A = \{a, b\}$. Find a DFA $\mathscr{A}$ which recognises

$$L = \{w \in A^* \mid |w|_b \leqslant 2\}.$$

Draw

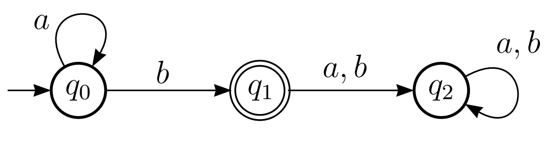


We see that $L = L(\mathscr{A})$.

Note. Using different notation we can express L as

$$\begin{aligned} L &= \{a\}^* \cup \{a\}^*\{b\}\{a\}^* \cup \{a\}^*\{b\}\{a\}^*\{b\}\{a\}^* \\ &= a^* \cup a^*ba^* \cup a^*ba^*ba^* \end{aligned}$$

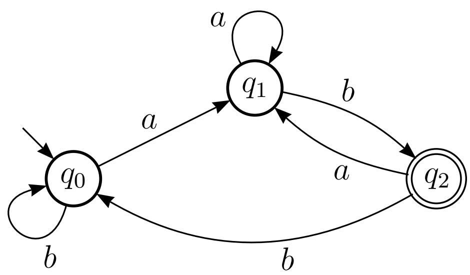
Example 2.7. Let $A = \{a, b\}$. Given the DFA



find the language that is recognised by $\mathscr{A}$. This is

$$L(\mathscr{A}) = a^*b = \{a\}^*\{b\} = \{a^n b \mid n \in \mathbb{N}^0\}$$

Example 2.8. Let $A = \{a, b\}$. Given the DFA



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

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

Suppose that $v \in L(\mathscr{A})$ 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 $L(\mathscr{A}) \subseteq A^*ab$.

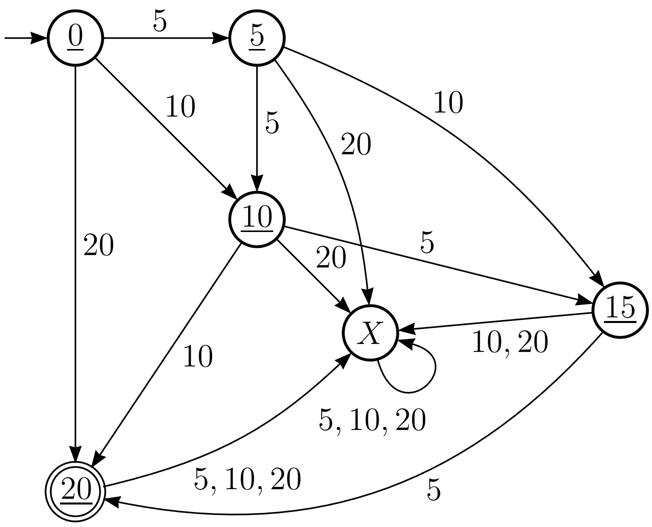
Conversely let $w \in A^*ab$ so $w = vab$ for some $v \in A^*$. Notice that $\delta(q_i, ab) = q_2$ for any $i = 0, 1, 2$. Hence

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

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

Example 2.9 (A Basic Automaton). The following automaton represents a vending machine. The cost of goods is 20p and it has states $\{\underline{0}, \underline{5}, \underline{10}, \underline{15}, \underline{20}, X\}$. The DFA $\mathscr{A}$ consists of

$$\begin{aligned} A &= \{5, 10, 20\}, \\ q_0 &= \{\underline{0}\}, \\ F &= \{\underline{20}\}, \\ \delta(X, a) &= X, \\ \delta(\underline{u}, v) &= \begin{cases} \underline{u+v} & \text{if } u + v \leq 20 \\ X & \text{else} \end{cases}. \end{aligned}$$



We have the language recognised by $\mathscr{A}$ is

$$L(\mathscr{A}) = \{5555,\ 55\,10,\ 510\,5,\ 10\,55,\ 10\,10,\ 20\}.$$

DEFINITION 2.10. For an alphabet A write $\operatorname{Rec} A^*$ for the class of recognisable languages over A.

So, $L \in \operatorname{Rec} A^*$ means "L is recognisable", i.e. there exists a DFA $\mathscr{A}$ with $L = L(\mathscr{A})$.

To show $L \in \operatorname{Rec} A^*$ we must *find* a DFA $\mathscr{A}$ with $L = L(\mathscr{A})$.

QUESTION How do we show that $L \notin \operatorname{Rec} A^*$?

2.2. **Pumping Lemma - PL**

Let $x \in A^*$. We say that $v \in A^*$ is a *factor* of x if $x = uvy$ for some $u, y \in A^*$. *So, prefixes and suffixes are special types of factors*; uvy is a *factorisation* of x.

DEFINITION 2.11. Let $L \subseteq A^*$. A natural number N is a *pumping length* for L if for all $w \in L$ with $|w| \geqslant N$ there exists a factorisation $w = uvx$ $(u, v, x \in A^*)$ with:

1. $v \neq \varepsilon$;
2. $|uv| \leqslant N$;
3. $uv^kx \in L$ for all $k \geqslant 0$.

Note.

1. The last condition says $ux, uvx, uv^2x, \ldots$ all lie in L.
2. $u, v, x \in A^*$; usually *not* in L; u, x can be empty; we must have $v \neq \varepsilon$.
3. If $M \geqslant N$, then M is also a pumping length for L.
4. Any finite language has pumping length N where $N > \max\{|w| : w \in L\}$.

Lemma 2.12. THE PUMPING LEMMA *Let $L \in \operatorname{Rec} A^*$. Then L has a pumping length.*

Having a pumping length is necessary *for $L \in \operatorname{Rec} A^*$ but* not *sufficient.*

Examples of the use of the Pumping Lemma

1. $L = \{a\}^*$ has pumping length of 1.

   Proof. If $w \in L$ with $|w| \geq 1$, then $w = a^h = \varepsilon a a^{h-1}$. Put $u = \varepsilon, v = a, x = a^{h-1}$. Then $v \neq \varepsilon$, $|uv| = 1 \leq 1$ and $uv^k x = a^{h+k-1} \in L$ for all $k \in \mathbb{N}^0$. □

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

   Proof. Suppose $L \in \operatorname{Rec} A^*$. By PL, L has a pumping length, say N. Choose $w = a^N b^N$, so $w \in L$ and $|w| = 2N \geqslant N$. So, there exists a factorisation $w = uvx$ where $|uv| \leqslant N$ and $v \neq \varepsilon$.

   We have $u = a^r$, $v = a^s$ and $x = a^t b^N$ where $r + s + t = N$ and $s \neq 0$. As N is a pumping length, $uv^2 x \in L$, i.e. $a^r a^s a^s a^t b^N = a^{N+s} b^N \in L$ but this is a contradiction as $N + s \neq N$ as $s \neq 0$. Hence $L \notin \operatorname{Rec} A^*$. □

3. $A = \{a, b\}$, $L = \{w \in A^* \mid |w|_a = |w|_b\}$. We claim that $L \notin \operatorname{Rec} A^*$.

   Proof. If $L \in \operatorname{Rec} A^*$, we pick a pumping length N. Choose $w = a^N b^N$ then $w \in L$, $|w| \geqslant N$ and proceed as in (2). □

General strategy for use of PL

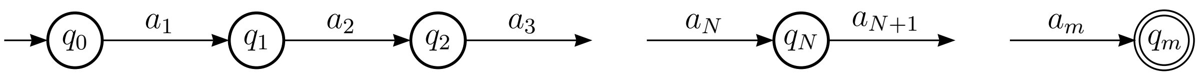
Given $L \subseteq A^*$, suppose we want to show $L \notin \operatorname{Rec} A^*$. Assume $L \in \operatorname{Rec} A^*$ and aim for a contradiction. Let N be a pumping length for L. Choose $w \in L$ with $|w| \geqslant N$. By the pumping lemma w has a factorisation satisfying the conditions of PL.
Use this to get a contradiction *by showing that it implies words lie in L when you know that they do not.* (Note: need only choose one w - choose an easy one! *comes with practice*).
Conclude that $L \notin \operatorname{Rec} A^*$.

(4) $A = \{a\}$, $L = \{a^p \mid p \text{ is prime}\}$. Claim $L \notin \operatorname{Rec} A^*$.

   Proof. Suppose $L \in \operatorname{Rec} A^*$. By PL, L has a pumping length, say N. Let p be prime, $p \geqslant N$. Then $w = a^p \in L$ and $|w| \geqslant N$. By PL there exists a factorisation $w = uvx$ where $|uv| \leqslant N$ and $v \neq \varepsilon$. Then $u = a^r$, $v = a^s$, $x = a^t$ where $r + s \leqslant N$, $s \neq 0$ and $r + s + t = p$ (as $w = a^p = uvx$). By PL, the words $uv^k x \in L$ for all $k \geqslant 0$. We have $uv^k x = a^r a^{sk} a^t = a^{r+sk+t} = a^{p+(k-1)s}$.

   Choose $k = p + 1$, then $uv^k x \in L$; but $uv^k x = a^{p+ps} = a^{p(1+s)}$ and $p(1 + s)$ is not prime as $s \neq 0$. Contradiction and hence $L \notin \operatorname{Rec} A^*$. □

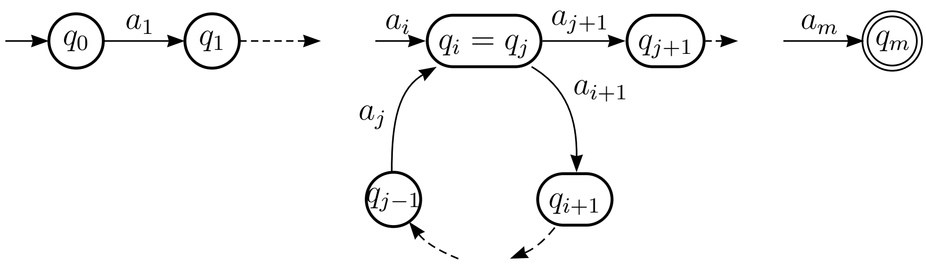
Proof of PL. Let $L \in \operatorname{Rec} A^*$. Then $L = L(\mathscr{A})$ for some DFA $\mathscr{A}$, where $\mathscr{A} = (A, Q, \delta, q_0, F)$. Let $N = |Q|$, the number of states of $\mathscr{A}$. If $w \in L$ and $|w| \geqslant N$, then $\delta(q_0, w) \in F$. Let $w = a_1 a_2 \dots a_N \dots a_m$ where $a_i \in A$ and $m = |w| \geqslant N$. As $w \in L$ we have



where $q_i \in Q$, $q_m \in F$ and $\delta(q_{i-1}, a_i) = q_i$ where $0 \leqslant i \leqslant m$. Since $N + 1 > N = |Q|$, at least two of

$$q_0, q_1, \dots, q_N$$

are equal; say $q_i = q_j$ where $0 \leqslant i < j \leqslant N \leqslant m$. Then we have



Put
$u = a_1 \dots a_i$ ($u = \varepsilon$ if $i = 0$),
$v = a_{i+1} \dots a_j$ ($v \neq \varepsilon$ as $i < j$),
$x = a_{j+1} \dots a_m$ ($x = \varepsilon$ if $j = N = m$).

We have $|uv| = j \leqslant N$, $v \neq \varepsilon$, $w = uvx$. For any $k \geqslant 0$,

$$\begin{aligned} \delta(q_0, uv^k x) &= \delta\big(\delta(q_0, u), v^k x\big) = \delta(q_i, v^k x) = \delta\big(\delta(q_i, v^k), x\big) \\ &= \delta(q_i, x) = \delta(q_j, x) = q_m \in F. \end{aligned}$$

Therefore $uv^k x \in L$ for all $k \geqslant 0$. □

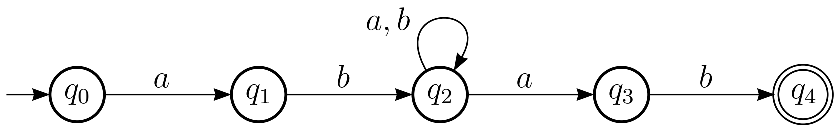
3. Automata: NDAs

Non-Deterministic (incomplete) finite state automata.

Example 3.1. To find a DFA which accepts

$$L = \{abwab \mid w \in A^*\}$$

where $A = \{a, b\}$. Want to write



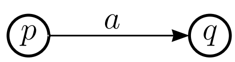
but this is not a DFA (neither complete nor deterministic). It is an example of the t.d. of an NDA.

Definition 3.2. An *NDA* $\mathscr{A}$ is a 5-tuple (A, Q, E, I, F) where

- A is an alphabet (so, a finite non-empty set),
- 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 t.d. of an NDA



denotes $(p, a, q) \in E$ (other notation being the same).

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 an NDA $\mathscr{A}$ (of length $n \geqslant 1$) is a finite sequence of edges

$$(p_1, a_1, q_1), (q_1, a_2, q_2), \ldots, (q_{n-1}, a_n, q_n)$$

often abbreviated as

$$p_1 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \rightarrow \ldots\ldots \xrightarrow{a_n} q_n.$$

Note: this is an excerpt from the t.d., with circles dropped around labels of states.

The *label* of the above path is $a_1 a_2 \ldots a_n$.
A path of length 1 is an edge.

Empty paths For each $q \in Q$ there exists a path ε_q of length 0 at q, with label ε. *We do not (usually) draw ε_q at q.*

$p \overset{w}{\Rightarrow} q (w \in A^*)$ means that there exists a path from p to q in $\mathscr{A}$, with label w.

Note that there exists $p \overset{\varepsilon}{\Rightarrow} p$ for *any* $p \in Q$.

In Example 3.1, we have
(i)

$$q_0 \xrightarrow{a} q_1$$

represents the edge (q_0, a, q_1), and is a path of length 1.
(ii)

$$q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_2$$

represents a path of length 2 and
(iii)

$$q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_2 \xrightarrow{a} q_2$$

represents a path of length 3.
We can write

$$q_0 \overset{a}{\Rightarrow} q_1,\ q_0 \overset{ab}{\Rightarrow} q_2 \text{ and } q_0 \overset{aba}{\Rightarrow} q_2.$$

DEFINITION 3.3. $w \in A^*$ is *accepted* by the NDA $\mathscr{A}$ if there exists a path $q_0 \overset{w}{\Rightarrow} q$ for some $q_0 \in I$ and $q \in F$.
Such a path is called *successful*.

DEFINITION 3.4. The *language recognised* by the NDA $\mathscr{A}$ is

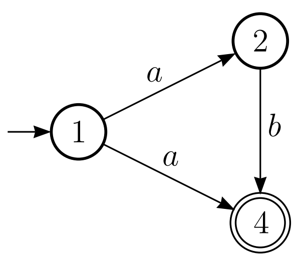
$$L(\mathscr{A}) = \{w \in A^* \mid w \text{ is accepted by } \mathscr{A}\}.$$

Note that in Example 3.1 the language recognised by the NDA is

$$\{abwab \mid w \in A^*\}$$

as required.

EXAMPLE 3.5. In the following NDA $\mathscr{A}$ we have $L(\mathscr{A}) = \{ab, a\}$.



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

$$L \in \operatorname{Rec} A^* \Leftrightarrow L \text{ is recognised by an NDA.}$$

Proposition 3.6. *L is recognised by a DFA $\Rightarrow$ L is recognised by an NDA.*

Proof. Let $L = L(\mathscr{A})$ where $\mathscr{A} = (A, Q, \delta, q_0, F)$ is a DFA. Put

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

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

$$\mathcal{A}' = (A, Q, E, I, F).$$

Notice that for any $w \in A^*$, there is only one path in $\mathscr{A}'$ from q_0 with label w, ending at $\delta(q_0, w)$. Hence

$$\begin{aligned} w \in L(\mathscr{A}) \quad &\Leftrightarrow \quad \delta(q_0, w) \in F \\ &\Leftrightarrow \quad \exists \text{ a path } q_0 \overset{w}{\Rightarrow} q \text{ in } \mathscr{A}' \text{ where } q \in F \\ &\Leftrightarrow \quad w \in L(\mathscr{A}') \end{aligned}$$

so that $L(\mathscr{A}) = L(\mathcal{A}')$. $\square$

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 edge (q, a, p).

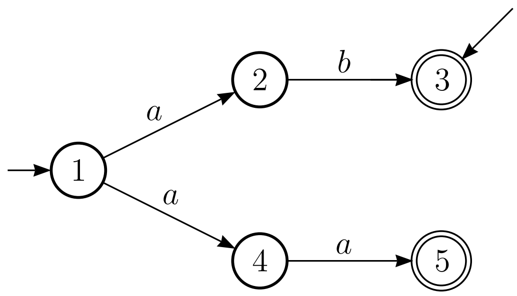
For the converse, we aim to show: if $L = L(\mathscr{A})$ for an NDA $\mathscr{A}$, then $L = L(\mathscr{A}')$ for a DFA $\mathscr{A}'$.

Notation. Let $\mathscr{A} = (A, Q, E, I, F)$ be an NDA. For $S \subseteq Q$, $w \in A^*$, we define

$$Sw = \{q \in Q \mid p \overset{w}{\Rightarrow} q \text{ for some } p \in S\}.$$

Note that $Sw \subseteq Q$ *so there exists only finitely many sets of the form Sw.*

Example 3.7. Given an NDA $\mathscr{A}$



we have that $L(\mathscr{A}) = \{\varepsilon, ab, a^2\}$ and
$\{1,3\}a = \{2,4\} = \{1\}a$, $\{1,3\}b = \emptyset$
$\{1,3\}a^2 = \{5\} = \{2,4\}a, \{1,3\}a^3 = \emptyset$
$\emptyset a = \emptyset b = \emptyset$
$\{2,4\}b = \{3\}$
$\{5\}a = \{5\}b = \{3\}a = \{3\}b = \emptyset$

Comments For $S \subseteq Q, a, a_1, \ldots, a_n \in A$, $w, v \in A^*$ we have that

$$\begin{aligned}
Sw &= \{q \in Q \mid p \overset{w}{\Rightarrow} q \text{ for some } p \in S\} = \bigcup_{p \in S} \{p\}w \\
S\varepsilon &= S \ (\varepsilon \text{ is only the label of paths } \varepsilon_p : p \overset{\varepsilon}{\Rightarrow} p) \\
Sa &= \{p \in Q \mid \exists (q, a, p) \in E, q \in S\}, \\
Sa_1a_2 \ldots a_n &= \big(\ldots\big((Sa_1)a_2\big)\ldots\big)a_n, \\
(Sw)v &= Swv \\
\emptyset w &= \emptyset.
\end{aligned}$$

Proposition 3.8. *If $L = L(\mathscr{A})$ for an NDA $\mathscr{A}$, then $L = L(\mathscr{A}')$ for a DFA $\mathscr{A}'$.*

Proof. Let $L = L(\mathscr{A})$ where

$$\mathscr{A} = (A, Q, E, I, F)$$

is an NDA. Construct a DFA

$$\mathscr{A}' = (A, Q', \delta, q_0, F')$$

where

$$\begin{aligned}
Q' &= \{Iw : w \in A^*\} \\
\delta(S, a) &= Sa \ \forall S \in Q', a \in A \\
q_0 &= I \\
F' &= \{S \in Q' : S \cap F \neq \emptyset\}.
\end{aligned}$$

Note. We have $Q' \subseteq \mathcal{P}(Q)$ (set of all subsets of Q), so $|Q'| < \infty$.

For $S \in Q', a \in A$ we have $S = Iw$ for some $w \in A^*$, so

$$\delta(S, a) = \delta(Iw, a) = (Iw)a = Iwa \in Q'.$$

Also, $q_0 = I = I\varepsilon \in Q'$.

Note

$$\begin{aligned}
\delta(S, a_1 \ldots a_n) &= \delta((\ldots\delta(\delta(S, a_1), a_2)\ldots), a_n) \\
&= (\ldots(Sa_1)a_2)\ldots)a_n \\
&= Sa_1 \ldots a_n.
\end{aligned}$$

Claim. $L(\mathscr{A}) = L(\mathscr{A}')$

We have that

$$\begin{aligned} w \in L(\mathscr{A}') &\Leftrightarrow \delta(q_0, w) \in F' \\ &\Leftrightarrow \delta(I, w) \in F' \\ &\Leftrightarrow Iw \in F' \\ &\Leftrightarrow Iw \cap F \neq \emptyset \\ &\Leftrightarrow \text{there exists a path } p \overset{w}{\Rightarrow} q \\ &\qquad \text{for some } p \in I, q \in F \\ &\Leftrightarrow w \in L(\mathscr{A}). \end{aligned}$$

□

Hence

Theorem 3.9. *$L \in \operatorname{Rec} A^*$ iff L is recognised by an NDA.*

Note *We know that Q' above must be finite, but how do we find it in general? How do we know we can stop our calculations at a certain point?*

Let

$$\mathcal{A} = (A, Q, E, I, F)$$

be an NDA. As above, we form a DFA

$$\mathcal{A}' = (A, Q', \delta, q_0, F')$$

where

$$Q' = \{Iw : w \in A^*\},$$
$$q_0 = I$$

and

$$F' = \{S \in Q' : S \cap F \neq \emptyset\}.$$

We know that Q' is finite, but how do we find it in general?
Let $A = \{a_1, \dots, a_n\}$.
Write down $I (= I\varepsilon)$
Caclulate Ia_i and add it to a set containing I, for all $1 \leq i \leq n$ (we could have $Ia_i = I$)
Then calculate Ia_ia_j for all $1 \leq i, j \leq n$ and add it to our set $\{I, Ia_1, \dots, Ia_n\}$ (unless it is already there)
Continue with this process until we have a set

$$T = \{I, Iw_1, \dots, Iw_k\}$$

such that for any $1 \leq i \leq n$, and any w_h with $0 \leq h \leq k$, where $w_0 = \varepsilon$, we have that

$$Iw_h a_i \in T.$$

Claim

$$T = Q'.$$

Proof Certainly

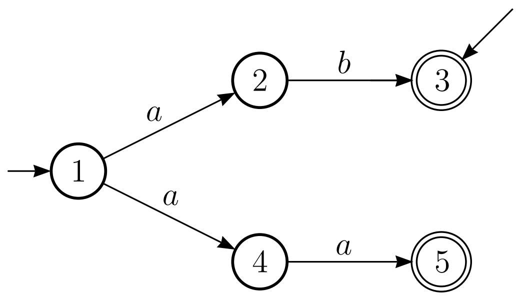
$$T \subseteq Q'.$$

For any word w of length 0, $Iw \in T$ (this is trivial - the only such w is ε).
Suppose for induction that $w \in A^*$ has length $n \geq 1$ and for every $v \in A^*$ with $|v| < n$, we have $Iv \in T$.
Then $w = w_h a_i$ for some $0 \leq h \leq k$, $1 \leq i \leq n$ and by the inductive hypothesis,

$$Iw = (Iw_h)a_i = Iw_h a_i$$

By assumption, $Iw_h a_i \in T$, as required.
By induction, $Iw \in T$ for any $w \in A^*$, that is, $Q' \subseteq T$, so that $Q' = T$ as required.

Example 3.10 (Construction of a DFA from an NDA). Let our NDA $\mathscr{A}$ be as in Example 3.7



Clearly $L(\mathscr{A}) = \{\varepsilon, ab, aa\}$.
From Example 3.7 we have Q':

$$\begin{array}{rclrcl} I &=& \{1,3\} & Ia &=& \{2,4\} \\ Ib &=& \emptyset & \emptyset a &=& \emptyset b = \emptyset \\ \{2,4\}a &=& \{5\} & \{2,4\}b &=& \{3\} \end{array}$$

and

$$\{5\}a = \{5\}b = \{3\}a = \{3\}b = \emptyset.$$

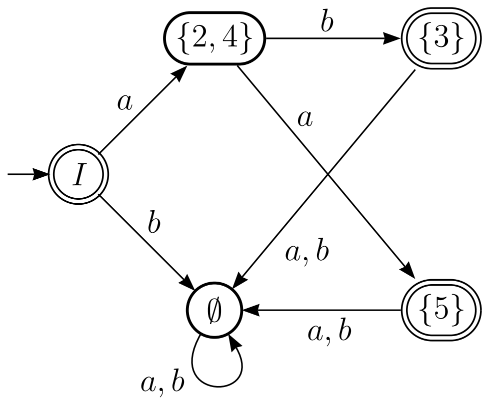
We have a DFA $\mathscr{A}'$ where

$$\mathscr{A}' = (A, Q', \delta, q_0, F').$$

and

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

and δ is given as in the following transition diagram.



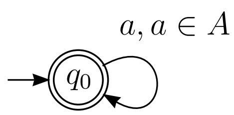
Then we can easily check $L(\mathscr{A}') = \{\varepsilon, ab, aa\} = L(\mathscr{A})$.

4. Closure Properties of $\operatorname{Rec} A^*$

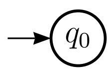
We begin by showing that empty and singleton languages are in $\operatorname{Rec} A^*$*. We then use NDAs and DFAs to prove that* $\operatorname{Rec} A^*$ *is closed under Boolean operations, product and star*

Example 4.1. A any alphabet.

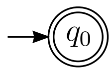
1. $A^* \in \operatorname{Rec} A^*$ as the DFA



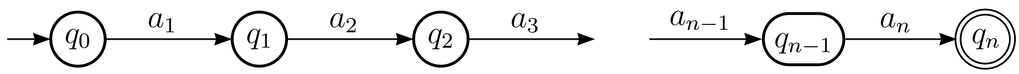
   recognises A^*.
2. $\emptyset \in \operatorname{Rec} A^*$ as $\emptyset$ recognised by the NDA



3. $\{\varepsilon\} \in \operatorname{Rec} A^*$ as $\{\varepsilon\}$ is recognisable by the NDA



4. For $w = a_1 a_2 \dots a_n \in A^+$ $(a_i \in A)$ then $\{w\}$ is recognisable by the NDA



So, **all singleton languages lie in** $\operatorname{Rec} A^*$**.**

Proposition 4.2. $L \in \operatorname{Rec} A^* \Rightarrow L^c \in \operatorname{Rec} A^*$

Proof. If $L \in \operatorname{Rec} A^*$ then $L = L(\mathscr{A})$ where $\mathscr{A} = (A, Q, \delta, q_0, F)$ is a DFA. Let $\mathscr{A}^c = (A, Q, \delta, q_0, F^c)$. Then

$$w \in L(\mathscr{A}^c) \Leftrightarrow \delta(q_0, w) \in F^c \Leftrightarrow \delta(q_0, w) \notin F \Leftrightarrow w \notin L(\mathscr{A}) = L \Leftrightarrow w \in L^c.$$

Therefore $L(\mathscr{A}^c) = L^c$ and $L^c \in \operatorname{Rec} A^*$. □

Proposition 4.3. $L, K \in \operatorname{Rec} A^* \Rightarrow L \cup K \in \operatorname{Rec} A^*$

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

$$\begin{aligned} w \in L \cup K \Leftrightarrow{}& w \in L \text{ or } w \in K \\ &\Leftrightarrow \exists \text{ path } q_0 \overset{w}{\Rightarrow} q \text{ in } \mathscr{A} \text{ with } q_0 \in I \text{ and } q \in F \\ &\quad \text{or } \exists \text{ path } p_0 \overset{w}{\Rightarrow} p \text{ in } \mathscr{B} \text{ with } p_0 \in I' \text{ and } p \in F' \\ &\Leftrightarrow \exists \text{ path } r_0 \overset{w}{\Rightarrow} r \text{ in } \mathscr{C} \text{ with } r_0 \in I \cup I' \text{ and } r \in F \cup F' \\ &\quad (\text{since } Q \cap Q' = \emptyset) \\ &\Leftrightarrow w \in L(\mathscr{C}). \end{aligned}$$

Therefore $L \cup K = L(\mathscr{C})$ so that $L \cup K \in \operatorname{Rec} A^*$. □

Corollary 4.4. $L_1, L_2, \ldots, L_m \in \operatorname{Rec} A^* \Rightarrow L_1 \cup L_2 \cup \cdots \cup L_m \in \operatorname{Rec} A^*$.

Proof. Proposition 4.3 and Induction. □

Corollary 4.5. $L, K \in \operatorname{Rec} A^* \Rightarrow L \cap K \in \operatorname{Rec} A^*$.

Proof. $L \cap K = \big(L^c \cup K^c\big)^c$; hence result by Propositions 4.2 and 4.3. □

Corollary 4.6. $L_1, L_2, \ldots, L_m \in \operatorname{Rec} A^* \Rightarrow L_1 \cap L_2 \cap \cdots \cap L_m \in \operatorname{Rec} A^*$

Proof. Corollary 4.5 and Induction. □

Corollary 4.7. $L, K \in \operatorname{Rec} A^* \Rightarrow L \setminus K \in \operatorname{Rec} A^*$

Proof. $L \setminus K = L \cap K^c$ - Proposition 4.2 and Corollary 4.5. □

Note. $\operatorname{Rec} A^*$ is NOT closed under infinite $\cup$ and $\cap$.

Recall $LK = \{wv \mid w \in L, v \in K\}$.

Proposition 4.8. *Let $L, K \in \operatorname{Rec} A^*$. Then $LK \in \operatorname{Rec} A^*$*

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

$$\mathscr{A} = (A, Q, E, I, F) \qquad \text{and} \qquad \mathscr{B} = (A, Q', E', I', F')$$

are NDAs and $Q \cap Q' = \emptyset$.

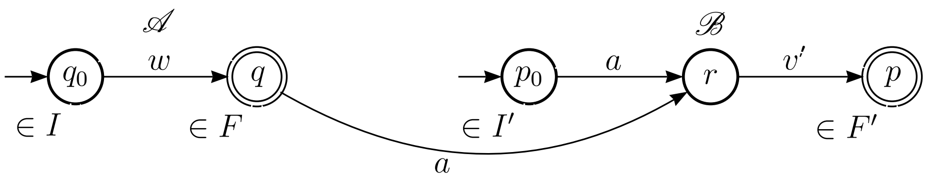
[We would like to do the following 'glueing':

$$\begin{array}{ccc} q_0 \overset{w}{\Longrightarrow} q & \equiv & p_0 \overset{v}{\Longrightarrow} p \\ \in I \quad \in F & & \in I' \quad \in F' \end{array}$$

but this would not 'separate' $\mathscr{A}$ and $\mathscr{B}$ adequately].

Put $\mathscr{C} = (A, Q \cup Q', \widetilde{E}, I, F')$ where

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



The proof below proceeds via 'iff' statements. Make sure you understand why both implications work in each instance. In some cases it is obvious, but in others you need to pay attention

We have

$$\begin{aligned}
w \in LK &\Leftrightarrow w = uv, \text{ some } u \in L, v \in K \\
&\Leftrightarrow w = uav', \text{ some } u \in L, v = av' \in K, a \in A \text{ (as } \varepsilon \notin K) \\
&\Leftrightarrow w = uav',\ \exists\, q_0 \in I, q \in F, q_0 \overset{u}{\Rightarrow} q \text{ in } \mathscr{A} \\
&\qquad \text{and } \exists\, p_0 \in I', p \in F', p_0 \overset{av'}{\Rightarrow} p \text{ in } \mathscr{B} \\
&\Leftrightarrow w = uav',\ \exists\, q_0 \in I, q \in F, q_0 \overset{u}{\Rightarrow} q \text{ in } \mathscr{A} \text{ and} \\
&\qquad \exists\, p_0 \in I', r \in Q', p \in F' \text{ with } p_0 \overset{a}{\to} r \overset{v'}{\Rightarrow} p \text{ in } \mathscr{B} \\
&\Leftrightarrow w = uav',\ \exists\, q_0 \in I, q \in F, q_0 \overset{u}{\Rightarrow} q \text{ in } \mathscr{A} \text{ and} \\
&\qquad \exists r \in Q', p \in F' \text{ with } (q, a, r) \in \widetilde{E}, r \overset{v'}{\Rightarrow} p \text{ in } \mathscr{B} \\
&\Leftrightarrow w = uav',\ \exists\, q_0 \in I, p \in F', q_0 \overset{uav'}{\Rightarrow} p \text{ in } \mathscr{C} \\
&\Leftrightarrow w = uav' = uv \in L(\mathscr{C}).
\end{aligned}$$

Hence $L(\mathscr{C}) = LK$ and so $LK \in \operatorname{Rec} A^*$.
We have shown if $\varepsilon \notin K$, then $LK \in \operatorname{Rec} A^*$. Finally, if $\varepsilon \in K$, then $K' = K \setminus \{\varepsilon\}$ is recognisable by Corollary 4.7. We have

$$\begin{aligned}
LK &= L\big(K' \cup \{\varepsilon\}\big) \\
&= LK' \cup L\{\varepsilon\} \\
&= LK' \cup L
\end{aligned}$$

and $LK' \in \operatorname{Rec} A^*$ by the first part of the proof, so $LK \in \operatorname{Rec} A^*$ by Proposition 4.3. $\square$

Proposition 4.9. $L \in \operatorname{Rec} A^* \Rightarrow L^* \in \operatorname{Rec} A^*$

Proof. Recall that

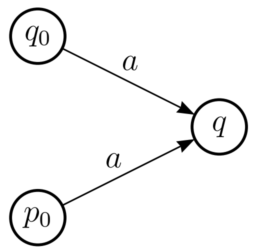
$$\begin{aligned}
L^* = \bigcup_{n \geqslant 0} L^n &= L^0 \cup L^1 \cup L^2 \cup \dots \\
&= \{\varepsilon\} \cup L \cup L^2 \cup L^3 \cup \dots
\end{aligned}$$

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

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

Proof. Put $P = Q \cup \{p_0\}$ where $p_0 \notin Q$ and

$$\begin{aligned} \sigma(q,a) &= \delta(q,a) \qquad \text{for all } q \in Q,\ a \in A, \\ \sigma(p_0,a) &= \delta(q_0,a) \end{aligned}$$



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

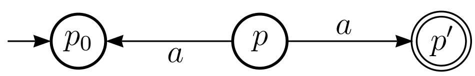
Now put

$$G = \begin{cases} F & \text{if } \varepsilon \notin L(\mathscr{A}) \text{ (i.e. } q_0 \notin F), \\ F \cup \{p_0\} & \text{if } \varepsilon \in L(\mathscr{A}) \text{ (i.e. } q_0 \in F). \end{cases}$$

Now check that $L(\mathscr{A}) = L(\mathscr{B})$ □

Back to main proof: let $L = L(\mathscr{B})$ where $\mathscr{B} = (A, P, \sigma, p_0, G)$ is a DFA with $\sigma(p,a) \neq p_0$ for all $p \in P$, $a \in A$.
Put $\mathscr{C} = (A, P, E, \{p_0\}, \{p_0\})$ where

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



Note. $\varepsilon \in L^*$ and $\varepsilon \in L(\mathscr{C})$

Suppose $w \neq \varepsilon$. Then

$$
\begin{aligned}
w \in L^* &\Leftrightarrow w = w_1 w_2 \dots w_t \text{ with } t \geqslant 1,\ w_i \in L \setminus \{\varepsilon\} \text{ for all } i,\\
&\Rightarrow w = w_1 w_2 \dots w_t, t \geqslant 1, \sigma(p_0, w_i) \in G\, \forall\, i,\\
&\Rightarrow w = w_1 w_2 \dots w_t, t \geqslant 1, \forall\, i\ \ p_0 \overset{w_i}{\Rightarrow} p_i \text{ in } \mathscr{B},\ p_i \in G\\
&\Rightarrow w = w_1 \dots w_t, t \geqslant 1, p_0 \overset{w_i}{\Rightarrow} p_0 \text{ in } \mathscr{C}\, \forall\, i,\\
&\qquad\quad \textit{think of the last step for each } p_i!\\
&\Rightarrow p_0 \overset{w}{\Rightarrow} p_0 \text{ in } \mathscr{C},\\
&\Rightarrow w \in L(\mathscr{C}).
\end{aligned}
$$

Hence we have $L^* \subseteq L(\mathscr{C})$.
Conversely let $w \in L(\mathscr{C})$, so that $p_0 \overset{w}{\Rightarrow} p_0$ in $\mathscr{C}$. Let $w = a_1 a_2 \dots a_n$ $(a_i \in A)$ and

$$
p_0 \xrightarrow{a_1} p_1 \xrightarrow{a_2} p_2 \dashrightarrow \quad \xrightarrow{a_n} p_n = p_0
$$

Let $i_1, i_2, \dots, i_t = n$ be such that

$$
0 < i_1 < i_2 < \dots < i_t \qquad \text{and } p_{i_j} = p_0.
$$

Put

$$
\begin{aligned}
w_1 &= a_1 a_2 \dots a_{i_1},\\
w_2 &= a_{i_1+1} \dots a_{i_2},\\
&\ \vdots\\
w_t &= a_{i_{t-1}+1} \dots a_{i_t=n}.
\end{aligned}
$$

Then $w = w_1 w_2 \dots w_t$ and $p_0 \overset{w_j}{\Rightarrow} p_0$ in $\mathscr{C}$ for all j.
Considering the last letter of $w_j = v_j a_{i_j}$ we see that $p_0 \overset{v_j}{\Rightarrow} p \overset{a_{i_j}}{\to} p_0$ in $\mathscr{C}$, so in $\mathscr{B}$ we have $p_0 \overset{v_j}{\Rightarrow} p \overset{a_{i_j}}{\to} p' \in G$. So, $w = w_1 w_2 \dots w_t$ and $p_0 \overset{w_j}{\Rightarrow} p' \in G$ in $\mathscr{B}$, i.e. $w = w_1 w_2 \dots w_t$ where $w_j \in L(\mathscr{B}) = L$ for all j. Hence $w \in L^*$. Therefore, $L(\mathscr{C}) \subseteq L^*$ and so $L(\mathscr{C}) = L^*$. □

Examples of using Closure Properties

EXAMPLE 4.10. L finite $\Rightarrow L \in \operatorname{Rec} A^*$.

Proof. L finite $\Rightarrow L = \emptyset$ or $L = \{w_1, w_2, \dots, w_n\}$ for some $w_i \in A^*$. We know $\emptyset \in \operatorname{Rec} A^*$ and $\{w_i\} \in \operatorname{Rec} A^*$ for all i. Therefore $L = \{w_1\} \cup \{w_2\} \cup \dots \cup \{w_n\}$ is recognisable by Corollary 4.4. □

EXAMPLE 4.11. L cofinite $\Rightarrow L \in \operatorname{Rec} A^*$.

Proof. L cofinite $\Rightarrow L^c$ is finite $\Rightarrow L^c \in \operatorname{Rec} A^*$ by above example. Hence $L = (L^c)^c \in \operatorname{Rec} A^*$ by Proposition 4.2. $\square$

EXAMPLE 4.12. $A = \{a, b\}$. Then $L = A^*aaA^* \cup A^*bbA^* \in \operatorname{Rec} A^*$.

Proof. A^*, $\{aa\}$, $\{bb\} \in \operatorname{Rec} A^*$ so A^*aaA^*, $A^*bbA^* \in \operatorname{Rec} A^*$ by Proposition 4.8 (twice). Hence $L = A^*aaA^* \cup A^*bbA^* \in \operatorname{Rec} A^*$ by Proposition 4.3. $\square$

EXAMPLE 4.13. $L = \{a^n \mid n \text{ is } \textit{not} \text{ prime}\} \notin \operatorname{Rec} A^*$.

Proof. $L \in \operatorname{Rec} A^* \Rightarrow L^c \in \operatorname{Rec} A^*$ (by Proposition 4.2). But $L^c = \{a^p \mid p \text{ is prime}\}$ is *not* in $\operatorname{Rec} A^*$. Contradiction. Hence $L \notin \operatorname{Rec} A^*$. $\square$

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

We now give (with one gap, to be filled later) an example of a language with a pumping length that is not recognisable.

EXAMPLE 4.14.

(a) $L' = \{a^n b^p \mid n \geqslant 0, p \text{ prime }\} \notin \operatorname{Rec} A^*$. We have

$$L' \in \operatorname{Rec} A^* \Rightarrow L' \cap b^* \in \operatorname{Rec} A^* \Rightarrow \{b^p \mid p \text{ is prime}\} \in \operatorname{Rec} A^*,$$

contradiction. Hence L' is *not* recognisable. In fact, WE ASSUME

$$L = \{a^n b^p \mid n \geqslant 1, p \text{ prime}\}$$

is not recognisable (see later for proof).

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

Proof.

$$L \cup b^* \in \operatorname{Rec} A^* \Rightarrow L = (L \cup b^*) \cap (a^* \setminus \{\varepsilon\})b^* \in \operatorname{Rec} A^*,$$

contradiction. Hence $L \cup b^* \notin \operatorname{Rec} A^*$. $\square$

(c) $L \cup b^*$ has pumping length.

Proof. Let $N = 1$ and let $w \in L \cup b^*$, with $|w| \geq 1$.

If $w \in b^*$, then $w = uvx, u = \varepsilon, v = b, x \in b^*$ and $|uv| = 1 \leq 1, v \neq \varepsilon$ and $uv^k b \in L \cup b^*$ for all $k \geq 0$.

If $w \in L$, then $w = a^n b^p$ where $n \geq 1$, p is prime. Then $w = uvx$ where $u = \varepsilon, v = a, x = a^{n-1}b^p$, and $|uv| = 1 \leq 1, v \neq \varepsilon, ux = a^{n-1}b^p \in L \cup b^*$ and for $k \geq 1$ we have $uv^k x = a^k a^{n-1} b^p \in L \cup b^*$.

$\square$

5. Rational Operations and Kleene's Theorem

Let A be an alphabet.

Definition 5.1. The *rational operations* on languages over A are union, product and star, i.e.

$$L, K \mapsto L \cup K,\ L, K \mapsto LK \text{ and } L \mapsto L^*.$$

Definition 5.2. $L \subseteq A^*$ 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.

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

Example 5.3.

(a) $\emptyset$, $\{\varepsilon\}$, $\{w\}$, $\{ab, ba, a^6bc\}$ are finite and so rational.
(b) $\{ab, ba, a^6bc\}^*$, $ab^*a = \{a\}\{b\}^*\{a\} \in \operatorname{Rat} A^*$.
(c) $L = \{abwab \mid w \in A^*\} = \{ab\}\{a, b\}^*\{ab\} \in \operatorname{Rat} A^*$
(d) $L = \big\{x \in \{a, b\}^* \mid |x|_a \leqslant 1\big\} = b^* \cup b^*ab^* \in \operatorname{Rat} A^*$.

Observation: We have already proved that any finite language lies in $\operatorname{Rec} A^*$ and if $L, K \in \operatorname{Rec} A^*$ then $L \cup K$, LK, $L^* \in \operatorname{Rec} A^*$[1] – consequently

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

Theorem 5.4 (Kleene's Theorem)**.** $\operatorname{Rat} A^* = \operatorname{Rec} A^*$.

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

Let $L \in \operatorname{Rec} A^*$. Then $L = L(\mathscr{A})$ for some NDA $\mathscr{A} = (A, Q, E, I, F)$. We prove by induction on $|E|$ that $L \in \operatorname{Rat} A^*$.

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 $L \in \operatorname{Rat} A^*$.

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

[1] Recall the *Boolean operations* on languages over A are union, intersection, complement and set difference, i.e.

$$L, K \Rightarrow L \cup K,\ L, K \mapsto L \cap K,\ L \mapsto L^c, \text{ and } L, K \mapsto L \setminus K.$$

We have seen that $\operatorname{Rec} A^*$ is closed under the Boolean operations, product and star.

$$\begin{aligned}
\mathscr{A}_0 &= (A, Q, E \setminus \{e\}, I, F),\\
\mathscr{A}_1 &= (A, Q, E \setminus \{e\}, I, \{p\}),\\
\mathscr{A}_2 &= (A, Q, E \setminus \{e\}, \{q\}, \{p\}),\\
\mathscr{A}_3 &= (A, Q, E \setminus \{e\}, \{q\}, F).
\end{aligned}$$

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

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

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

$$\begin{aligned}
L_0 &= L(\mathscr{A}_0)\\
&= \{w \in L(\mathscr{A}) \mid \exists\, q_0 \overset{w}{\Rightarrow} p, q_0 \in I, p \in F\\
&\qquad \text{not involving the edge } e\},\\
&\subseteq L(\mathscr{A}) = L.
\end{aligned}$$

Let $w \in L_1\{a\}\big(L_2\{a\}\big)^* L_3$. Then $w = ua(v_1 a v_2 a \dots v_m a)x$, where $u \in L_1$, $m \geq 0$, $v_i \in L_2$, with $1 \leqslant i \leqslant m$ and $x \in L_3$.
There exists a path in $\mathscr{A}$

$$q_0 \overset{u}{\Longrightarrow} p \underset{v_i}{\overset{a}{\rightleftarrows}} q \overset{x}{\Longrightarrow} r$$

with $q_0 \in I, r \in F$.
Therefore $w \in L(\mathscr{A}) = L$. We have shown that $L_4 \subseteq L$.

Conversely suppose $w \in L(\mathscr{A})$. Then there exists a path

$$\underset{\in I}{q_0} \overset{w}{\Rightarrow} \underset{\in F}{r}$$

in $\mathscr{A}$.

If the edge e is not used in this path, we have $\underset{\in I}{q_0} \overset{w}{\Rightarrow} \underset{\in F}{r}$ in $\mathscr{A}_0$ so $w \in L(\mathscr{A}_0) = L_0 \subseteq L_4$.

Suppose now that $w = a_1 a_2 \dots a_n$ and we have a path

$$(q_0, a_1, q_1), (q_1, a_2, q_2), \dots, (q_{n-1}, a_n, q_n)$$

where $q_n = r$, i.e.

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \longrightarrow \cdots \xrightarrow{a_n} q_n$$

where the edge $e = (p, a, q)$ 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. Then $w = w_0 a w_1 a \ldots a w_t$ where

$$q_0 \overset{w_0}{\Longrightarrow} p \xrightarrow{a} q \overset{w_1}{\Longrightarrow} p \xrightarrow{a} q \dashrightarrow p \xrightarrow{a} q \overset{w_t}{\Longrightarrow} r$$

where $w_0 \in L(\mathscr{A}_1) = L_1$, $w_i \in L(\mathscr{A}_2) = L_2$ $(1 \leqslant i < t)$, $w_t \in L(\mathscr{A}_3) = L_3$. Hence

$$w = w_0 a w_1 a \ldots w_{t-1} a w_t \in L_1 a (L_2 a)^* L_3 \subseteq L_4.$$

Therefore $L \subseteq L_4$. Hence $L = L_4$ and $L \in \operatorname{Rat} A^*$. □

Rational Expressions

DEFINITION 5.5. A *rational expression* for a language L over A is one that expresses L using only finite languages and rational operations, used a finite number of times.[2]

EXAMPLE 5.6. Let $L = (A^*ab)^c$. As $A, \{ab\} \in \operatorname{Rec} A^*$, we have

$$A^*\{ab\} = A^*ab \in \operatorname{Rec} A^*.$$

By Proposition 4.2,

$$(A^*ab)^c \in \operatorname{Rec} A^*.$$

Hence $(A^*ab)^c \in \operatorname{Rat} A^*$.
We have

$$L = \{\varepsilon, a, b\} \cup A^*aa \cup A^*ba \cup A^*bb-$$

a *rational expression* for L.

EXAMPLE 5.7. Let $L \subseteq A^*$ where $A = \{a, b, c\}$ consist of all words that start with an a and end with a b and have no factor of b^2. Then

$$L = a\{a, c\}^*(b\{a, c\}\{a, c\}^*)^*b$$

is a rational expression for L *can you check this!?*, so that $L \in \operatorname{Rat} A^* = \operatorname{Rec} A^*$.

Notice also $L = L = a\{a, c\}^*(b\{a, c\}\{a, c\}^*)^*\{a, c\}^*b \cup \{ab\}$, so **rational expressions are not unique**.

Hence for $L \subseteq \mathscr{A}^*$ we know the following are equivalent:

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

[2] In fact, I am taking a rather informal approach to rational expressions for the purposes of this module. You will see in the literature that a rational expression is a formula constructed using variables and symbols for rational operations, into which languages can be substituted - we do not pursue this route here.

(ii) $L = L(\mathscr{A})$ for some NDA $\mathscr{A}$,
(iii) L is rational ($L \in \operatorname{Rat} A^*$).

6. Reduced DFAs

6.1. 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).

E.g. **Equality**: $a \sim b \Leftrightarrow a = b$.

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.

Example For the equivalence relation of equality, $[a] = \{a\}$.

Note. (i) $[a] = \{b \in A \mid a \sim b\} = \{b \in A \mid b \sim a\}$ ($\sim$ is symmetric);
(ii) $a \in [a]$ as $a \sim a$ ($\sim$ is reflexive).

Facts:

1. $[a] = [b] \Leftrightarrow [a] \cap [b] \neq \emptyset$, so the equivalence classes *partition* A, i.e. cut up A into disjoint non-empty subsets.
2. $[a] = [b] \Leftrightarrow b \in [a] \Leftrightarrow a \sim b \Leftrightarrow [a] \cap [b] \neq \emptyset$;
   the contrapositive of (2) is
   $[a] \neq [b] \Leftrightarrow b \notin [a] \Leftrightarrow a \not\sim b \Leftrightarrow [a] \cap [b] = \emptyset$.

Suppose A is finite. Let

$$\overline{A} = \{[a] : a \in A\}.$$

Then $|\overline{A}| \leq |A|$ and

$$\begin{aligned} |\overline{A}| = |A| &\Leftrightarrow |[a]| = 1 \forall a \in A \\ &\Leftrightarrow \{a\} = [a] \forall a \in A \\ &\Leftrightarrow \sim \text{ is equality .} \end{aligned}$$

6.2. **Reduced DFAs**

Our aim *Given a DFA* $\mathscr{A} = (A, Q, \delta, q_0, F)$ *with* $L(\mathscr{A}) = L$ *we find a DFA* $\bar{\mathscr{A}} = (A, \bar{Q}, \bar{\delta}, \bar{q_0}, \overline{F})$ *with* $L(\bar{\mathscr{A}}) = L$ *such that* $\bar{\mathscr{A}}$ *has the smallest number of states of any DFA accepting* L*. We will also show that* $\bar{\mathscr{A}}$ *is 'unique'.*

Definition 6.1. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA, $q \in Q$.
(i) $q \in Q$ is *accessible* if $\delta(q_0, w) = q$ for some $w \in A^*$;
(ii) $\mathscr{A}$ is *accessible* if every $q \in Q$ is is accessible.

Definition 6.2. DFAs $\mathscr{A}$ and $\mathscr{B}$ (over the same alphabet) are *equivalent* if $L(\mathscr{A}) = L(\mathscr{B})$.

Fact Any DFA is equivalent to an accessible DFA.

Proof. Sketch If a DFA $\mathscr{A}$ has inaccessible states, these can be removed to give a DFA $\mathscr{A}'$ with $L(\mathscr{A}') = L(\mathscr{A})$ (See Exercises). □

We assume from now on that our DFAs are accessible.

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

$$q \sim q' \Leftrightarrow \forall\, w \in A^* \big(\delta(q, w) \in F \Leftrightarrow \delta(q', w) \in F\big).$$

Note. $\sim$ is an equivalence relation on Q.

Definition 6.3. An (accessible) DFA $\mathscr{A}$ is *reduced* if

$$q \sim q' \Rightarrow q = q'.$$

Theorem 6.4. *Any DFA* $\mathscr{A}$ *is equivalent to a reduced DFA.*

Proof. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be an (accessible) DFA.
Let $[q]$ be the $\sim$-class of q.
Put

$$\overline{Q} = \big\{[q] \mid q \in Q\big\}.$$

Note that $|\overline{Q}| \leq |Q|$ and $|\overline{Q}| = |Q| \Leftrightarrow \mathscr{A}$ is reduced.
Define $\bar{\delta} : \overline{Q} \times A \to \overline{Q}$ by $\bar{\delta}\big([q], a\big) = \big[\delta(q, a)\big]$.

1. $\bar{\delta}$ is well-defined.

Aside: We want $\bar{\delta}(X, a)$ *to take only* **one** *value. If we have* $X = [q]$ *we have*

$$\bar{\delta}(X, a) = \bar{\delta}([q], a) = [\delta(q, a)]$$

but if we also have $X = [q']$ *(so,* $q \sim q'$*), then*

$$\bar{\delta}(X, a) = \bar{\delta}([q'], a) = [\delta(q', a)].$$

Thus we must show $[\delta(q, a)] = [\delta(q', a)]$.

Proof. Suppose $[q], [q'] \in \overline{Q}$ and $a \in A$:

$$\begin{aligned}
& [q] = [q'] \\
\Leftrightarrow\ & q \sim q' \\
\Leftrightarrow\ & \forall\, w \in A^*,\ \big(\delta(q,w) \in F \Leftrightarrow \delta(q',w) \in F\big) \\
\Rightarrow\ & \forall\, w \in A^*,\ \big(\delta(q,aw) \in F \Leftrightarrow \delta(q',aw) \in F\big) \\
\Leftrightarrow\ & \forall\, w \in A^*,\ \big(\delta\big(\delta(q,a),w\big) \in F \Leftrightarrow \delta\big(\delta(q',a),w\big) \in F\big) \\
\Leftrightarrow\ & \delta(q,a) \sim \delta(q',a) \\
\Leftrightarrow\ & \big[\delta(q,a)\big] = \big[\delta(q',a)\big] \\
\Leftrightarrow\ & \bar{\delta}\big([q],a\big) = \bar{\delta}\big([q'],a\big)
\end{aligned}$$

Hence $\bar{\delta}$ is well-defined. ☐

2. For $q \sim q'$,

$$q \in F \Leftrightarrow \delta(q,\varepsilon) \in F \Leftrightarrow \delta(q',\varepsilon) \in F \Leftrightarrow q' \in F.$$

So, in $[q]$ either all states are final or none are final.

We put $\overline{F} = \big\{[q] \mid q \in F\big\}$, $\bar{q_0} = [q_0]$, so

$$\overline{\mathscr{A}} = (A, \overline{Q}, \bar{\delta}, \bar{q_0}, \overline{F})$$

is a DFA.

3. For any $w \in A^*$ we have $\bar{\delta}\big([q],w\big) = \big[\delta(q,w)\big]$.

Proof.

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

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

$$\begin{aligned}
\bar{\delta}\big([q],wa\big) &= \bar{\delta}\big(\bar{\delta}([q],w),a\big) && \text{by definition of extended } \bar{\delta}, \\
&= \bar{\delta}\big([\delta(q,w)],a\big) && \text{inductive assumption,} \\
&= \big[\delta(\delta(q,w),a)\big] && \text{definition of } \bar{\delta}, \\
&= \big[\delta(q,wa)\big] && \text{definition of extended } \delta.
\end{aligned}$$

☐

4. $\bar{\mathscr{A}}$ is reduced.

Proof. We have that

$$\begin{array}{rcl}[q]\sim[q'] & \Leftrightarrow & \forall\, w\in A^*,\ \big(\bar\delta\big([q],w\big)\in\overline{F}\Leftrightarrow\bar\delta\big([q'],w\big)\in\overline{F}\big)\\ & \Leftrightarrow & \forall\, w\in A^*,\ \big(\big[\delta(q,w)\big]\in\overline{F}\Leftrightarrow\big[\delta(q',w)\big]\in\overline{F}\big)\\ & \Leftrightarrow & \forall\, w\in A^*,\ \big(\delta(q,w)\in F\Leftrightarrow\delta(q',w)\in F\big)\\ & & \text{ by the definition of } \overline{F}\\ & \Leftrightarrow & q\sim q'\\ & \Leftrightarrow & [q]=[q']\end{array}$$

and so $\bar{\mathscr{A}}$ is reduced. □

5. $\bar{\mathscr{A}}$ is equivalent to $\mathscr{A}$

$$\begin{aligned} w\in L(\mathscr{A}) &\Leftrightarrow \delta(q_0,w)\in F,\\ &\Leftrightarrow \big[\delta(q_0,w)\big]\in\overline{F},\\ &\Leftrightarrow \bar\delta\big([q_0],w\big)\in\overline{F}, \text{by (3)}\\ &\Leftrightarrow w\in L(\bar{\mathscr{A}}).\end{aligned}$$

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

NOTE $\overline{\mathscr{A}}$ is accessible: for $[q]\in\overline{Q}$, we have $q=\delta(q_0,w)$ for some w and then

$$[q]=\overline{\delta}([q_0],w).$$

6.3. Procedure to find $\overline{\mathscr{A}}$

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

Let $\mathscr{A}=(A,Q,\delta,q_o,F)$ and $k\geqslant 0$.

DEFINITION 6.5. $q\sim_k q'$ if and only if $\forall\, w\in A^*$ with $|w|\leqslant k$,

$$\delta(q,w)\in F\Leftrightarrow\delta(q',w)\in F.$$

Note that each q_k is an equivalence relation

$$q\ \sim_k\ q'\Rightarrow q\ \sim_{k-1}\ q'\Rightarrow\ldots\Rightarrow q\ \sim_0\ q'$$

and

$$\boxed{q\sim q'\Leftrightarrow q\sim_k q' \text{ for all } k\geqslant 0}$$

FACTS

(1) $q\ \sim_0\ q'\Leftrightarrow q,q'\in F$ or $q,q'\notin F$.

Proof.

$$\begin{aligned} q \sim_0 q' \quad &\Leftrightarrow \quad \text{for all } w \in A^*, |w| \leqslant 0, (\delta(q,w) \in F \Leftrightarrow \delta(q',w) \in F) \\ &\Leftrightarrow \quad (\delta(q,\varepsilon) \in F \Leftrightarrow \delta(q',\varepsilon) \in F) \\ &\Leftrightarrow \quad q, q' \in F \text{ or } q, q' \notin F. \end{aligned}$$

So the $\sim_0$ classes are F and $Q \setminus F$. ☐

(2) $q \sim_{k+1} q' \Leftrightarrow q \sim_k q'$ AND $\delta(q,a) \sim_k \delta(q',a)$ for all $a \in A$.

Proof. The following statements are equivalent by the definitions of the relations $\sim_k$ and the extended version of δ:

(a) $q \sim_{k+1} q'$,

(b) for all $w \in A^*$ with $|w| \leq k+1$,
$(\delta(q,w) \in F \Leftrightarrow \delta(q',w) \in F)$

(c) for all $v \in A^*$ with $|v| \leq k$,
$[(\delta(q,v) \in F \Leftrightarrow \delta(q',v) \in F)$ AND for all $a \in A$, $(\delta(q,av) \in F \Leftrightarrow \delta(q',av) \in F)]$,

(d) $q \sim_k q'$ AND for all $v \in A^*$ with $|v| \leq k$, for all $a \in A$,
$(\delta(\delta(q,a),v) \in F \Leftrightarrow \delta(\delta(q',a),v) \in F)$,

(e) $q \sim_k q'$ AND $\delta(q,a) \sim_k \delta(q',a)$ for all $a \in A$.

☐

(3) $\sim_k = \sim_{k+1} \;\Rightarrow\; \sim_k = \sim_{k+1} = \sim_{k+2} = \dots$.

Proof. Using (2) and the hypothesis we have

$$\begin{aligned} q \sim_{k+2} q' &\Leftrightarrow q \sim_{k+1} q' \text{ AND } \delta(q,a) \sim_{k+1} \delta(q',a) \text{ for all } a \in A \\ &\Leftrightarrow q \sim_k q' \text{ AND } \delta(q,a) \sim_k \delta(q',a) \text{ for all } a \in A \\ &\Leftrightarrow q \sim_{k+1} q'. \end{aligned}$$

Hence $\sim_{k+1} = \sim_{k+2}$ and so on. ☐

(4) There is a k such that $\sim_k = \sim_{k+1}$.

Proof. For $q \in Q$, denote the $\sim_i$-equivalence class of q by $[q]_i$. If $q \sim_{i+1} q'$, then certainly $q \sim_i q'$, so

$$[q]_0 \supseteq [q]_1 \supseteq [q]_2 \supseteq \dots$$

Since $[q]_0$ is finite, there is an integer $h(q)$ such that $[q]_{h(q)} = [q]_{h(q)+1}$ and so by (3),

$$[q]_{h(q)} = [q]_{h(q)+1} = \dots$$

Put $k = \max\{h(q) : q \in Q\}$; k exists because Q is finite. Then $[q]_k = [q]_{k+1}$ for all $q \in Q$ so that $\sim_k = \sim_{k+1}$. ☐

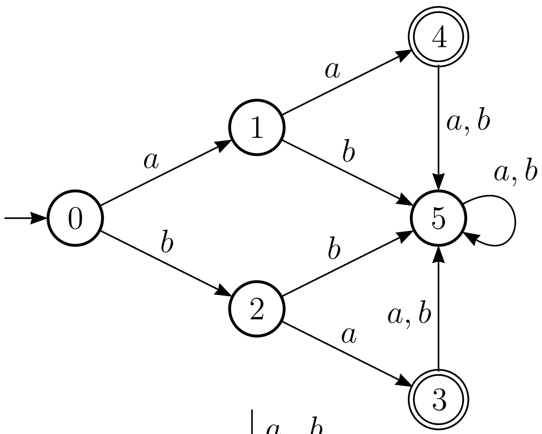
(5) $\sim_k = \sim_{k+1} \;\Rightarrow \sim_k = \sim$.

Proof. This follows from (3) and the fact that $q \sim q'$ if and only if $q \sim_i q'$ for all i. □

It now follows from (4) and (5) that $\sim_k = \sim$ for some k and that we can find such an integer k by looking for the smallest k such that $\sim_k = \sim_{k+1}$.

We now have that $q \sim_{k+1} q' \Leftrightarrow q \sim_k q'$ 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. Once this process stops with $\sim_k = \sim_{k+1}$, we know $\sim_k = \sim$.

Example 6.6.



	a	b
0	1	2
1	4	5
2	3	5
3	5	5
4	5	5
5	5	5

We have that the $\sim$ classes are

$\sim_0$ − classes :	$\{0,1,2,5\}$	$\{3,4\}$		
$\sim_1$ − classes :	$\{0,5\}$	$\{1,2\}$	$\{3,4\}$	
$\sim_2$ − classes :	$\{0\}$	$\{5\}$	$\{1,2\}$	$\{3,4\}$
$\sim_3$ − classes :	$\{0\}$	$\{5\}$	$\{1,2\}$	$\{3,4\}$

In our example we have

$$\sim_2 = \sim_3 \quad \Rightarrow \quad \sim = \sim_2 .$$

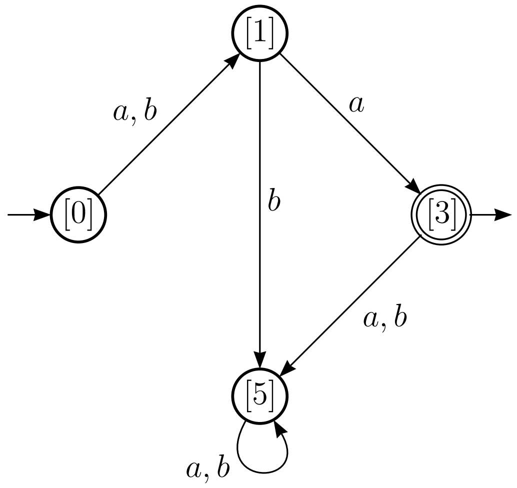
The reduced DFA equivalent to our example has four states

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

with initial state [0]. Unique final state [3]. Then we have

$$\overline{\mathscr{A}} = (A, \{[0], [5], [1], [3]\}, \overline{\delta}, [0], \{[3]\})$$

where $\overline{\delta}$ is given by the transition diagram:



6.4. When are two DFAs 'the same'?

New notation: Let $\theta : X \to Y$ be a function. We write $x\theta$ for $\theta(x)$ $(x \in X)$. Exception next state functions.

Definition 6.7. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$, $\mathscr{B} = (A, P, \sigma, p_0, T)$ be DFAs. Then $\mathscr{A}$ is *isomorphic* to $\mathscr{B}$ if there exists a bijection $\theta : Q \to P$ such that $q_0\theta = p_0$, $F\theta = T$ and

$$\delta(q, a)\theta = \sigma(q\theta, a) \qquad \forall\, q \in Q, a \in A.$$

The extended δ: If θ is as above, then for any $(q, w) \in Q \times A^*$ we have

$$\delta(q, w)\theta = \sigma(q\theta, w).$$

See Exercises for solution!

Proposition 6.8. *If $\mathscr{A} = (A, Q, \delta, q_0, F)$ and $\mathscr{B} = (A, P, \sigma, p_0, T)$ are reduced and equivalent, then $\mathscr{A}$ is isomorphic to $\mathscr{B}$.*

Proof. Define $\theta : Q \to P$ by

$$\delta(q_0, w)\theta = \sigma(p_0, w).$$

Certainly θ is everywhere defined and onto as $\mathscr{A}$ and $\mathscr{B}$ are accessible. The argument below shows that θ is well defined and one-one.

$$\begin{array}{lll}
 & \delta(q_0, w) = \delta(q_0, w') & \\
\Leftrightarrow & \delta(q_0, w) \sim \delta(q_0, w') & \text{as } \mathscr{A} \text{ is reduced} \\
\Leftrightarrow & \forall v \in A^*, \big(\delta(\delta(q_0, w), v) \in F \Leftrightarrow \delta(\delta(q_0, w'), v) \in F\big) & \text{defn of } \sim \\
\Leftrightarrow & \forall v \in A^*, \big(\delta(q_0, wv) \in F \Leftrightarrow \delta(q_0, w'v) \in F\big) & \text{extended } \delta \\
\Leftrightarrow & wv \in L(\mathscr{A}) \Leftrightarrow wv' \in L(\mathscr{A}) & \\
\Leftrightarrow & wv \in L(\mathscr{B}) \Leftrightarrow wv' \in L(\mathscr{B}) & \text{as } \mathscr{A}, \mathscr{B} \text{ equiv.} \\
\Leftrightarrow & \forall v \in A^*, \big(\sigma(p_0, wv) \in T \Leftrightarrow \sigma(p_0, w'v) \in T\big) & \\
\Leftrightarrow & \forall v \in A^*, \big(\sigma(\sigma(p_0, w), v) \in T \Leftrightarrow \sigma(\sigma(p_0, w'), v) \in T\big) \text{ extended } \sigma & \\
\Leftrightarrow & \sigma(p_0, w) \sim \sigma(p_0, w') & \text{defn of } \sim \\
\Leftrightarrow & \sigma(p_0, w) = \sigma(p_0, w') & \text{as } \mathscr{B} \text{ is reduced} \\
\Leftrightarrow & \delta(q_0, w)\theta = \delta(q_0, w')\theta. &
\end{array}$$

Now $\Rightarrow$ gives us that θ is well-defined and $\Leftarrow$ gives θ is 1:1. Thus θ is a bijection.

$\underline{q_0\theta = p_0}$
We have

$$q_0\theta = (\delta(q_0, \varepsilon))\theta = \sigma(p_0, \varepsilon) = p_0.$$

$\underline{F\theta = T}$
We have that for $\delta(q_0, w) \in Q$,

$$\begin{array}{rcl}
\delta(q_0, w) \in F & \Leftrightarrow & w \in L(\mathscr{A}) \\
 & \Leftrightarrow & \sigma(p_0, w) \in T \\
 & \Leftrightarrow & \delta(q_0, w)\theta \in T
\end{array}$$

so that as $\mathscr{A}$ is accessible and θ is onto, $F\theta = T$.

$\underline{\delta(q, a)\theta = \sigma(q\theta, a) \text{ for all } q \in Q,\ a \in A.}$
Let $q = \delta(q_0, w) \in Q$. Then

$$(\delta(q, a))\theta = (\delta(\delta(q_0, w), a))\theta = (\delta(q_0, wa))\theta =$$

$$\sigma(p_0, wa) = \sigma(\sigma(p_0, w), a)) = \sigma(\delta(q_0, w)\theta, a) = \sigma(q\theta, a)$$

as required.

Hence θ is an isomorphism. $\square$

Convention: we may write $Q_{\mathscr{C}}$ to denote that $Q_{\mathscr{C}}$ is the set of states of a DFA $\mathscr{C}$. We ALWAYS have

$$|Q_{\overline{\mathscr{A}}}| \leq |Q_{\mathscr{A}}|$$

as the states of $\overline{\mathscr{A}}$ are equivalence classes of states of $\mathscr{A}$.

Proposition 6.9. *Let $L \in \operatorname{Rec} A^*$. The following are equivalent for a DFA $\mathscr{A}$ with $L(\mathscr{A}) = L$:*
(i) $\mathscr{A}$ is reduced;
(ii) $\mathscr{A}$ has the smallest number of states of any DFA accepting L.

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

$$|Q_{\mathscr{A}}| = |Q_{\overline{\mathscr{B}}}| \leqslant |Q_{\mathscr{B}}|.$$ □

$(ii) \Rightarrow (i)$ We have $L(\mathscr{A}) = L(\overline{\mathscr{A}})$ and by (ii), $|Q_{\mathscr{A}}| = |Q_{\overline{\mathscr{A}}}|$, so that $\sim$ is equality and $\mathscr{A}$ is reduced.

Corollary 6.10. *For any DFA $\mathscr{A}$ we have $\overline{\mathscr{A}}$ is the unique (up to isomorphism) reduced DFA equivalent to $\mathscr{A}$.*

Proof. We know $L = L(\overline{\mathscr{A}})$ and $\overline{\mathcal{A}}$ is reduced. If also $L = L(\mathscr{B})$ and $\mathscr{B}$ is reduced, then as $L = L(\overline{\mathscr{A}}) = L(\mathscr{B})$ and both DFAs are reduced, we have $\overline{\mathscr{A}}$ is isomorphic to $\mathscr{B}$ by Proposition 6.9. So $\overline{\mathscr{A}}$ is unique as required. □

7. Monoids and Transition Monoids

7.1. Monoids

Definition 7.1. 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 7.2.

1. Groups are monoids. However $\mathbb{N}$ under $\times$ is a monoid which is *not* a group.
2. Let X be a set $X \neq \emptyset$.

$$\mathcal{T}_X = \{\alpha | \alpha : X \to X\}$$

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 α (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 α and then β. Naturally, we write $(u\alpha)\beta = u(\alpha\beta)$, so $\alpha\beta$ now means "do α, then do β".

If $X = \{1, 2, \ldots, n\}$ we write $\mathcal{T}_n$ for $\mathcal{T}_X$ and I_n for I_X.

We may use "two-row" notation for elements of $\mathcal{T}_n$. If $\alpha \in \mathcal{T}_4$ is given by

$$1\alpha = 1 \qquad 2\alpha = 1 \qquad 3\alpha = 2 \qquad 4\alpha = 4.$$

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 2 \end{pmatrix}.$$

Note that $|\mathcal{T}_n| = n^n$ because for each element in $\{1, 2, \ldots, n\}$ there are n choices for its image under a map in $\mathcal{T}_n$.

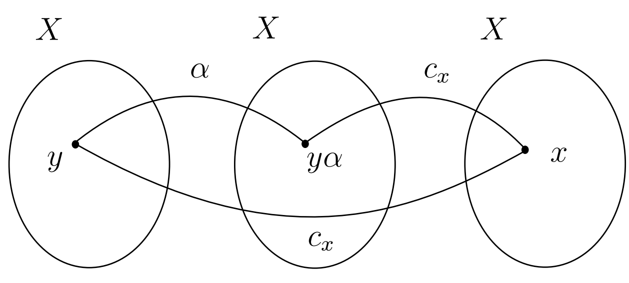
7.2. **Constant Functions in $\mathcal{T}_X$**

For any $x \in X$, $c_x : X \to X$ is given by $yc_x = x$ for all $y \in X$; c_x is called the *constant function* on x. For example

$$c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{T}_4.$$

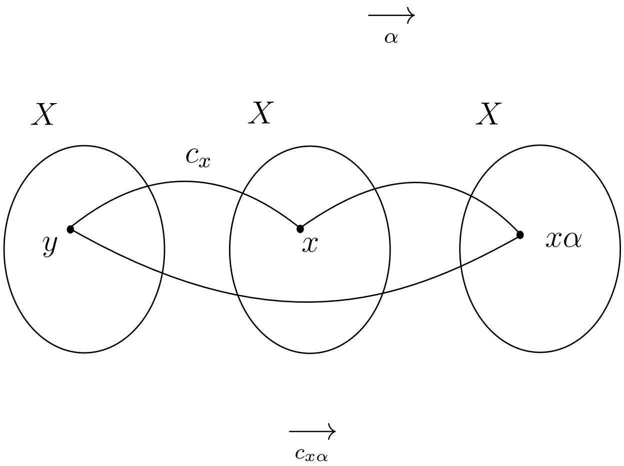
Note that $\alpha c_x = c_x$ for all $\alpha \in \mathcal{T}_X$, since for all $y \in X$ we have

$$y(\alpha c_x) = (y\alpha)c_x = x = yc_x$$



Also, $c_x\alpha = c_{x\alpha}$ since for all $y \in X$ we have

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



Definition 7.3. Let M be a monoid and $T \subseteq M$. Then T is a *submonoid* if

1. $1 \in T$ and
2. $a, b \in T \Rightarrow ab \in T$

Example $\mathbb{N}$ (under $\times$) is a submonoid of $\mathbb{Z}$ (under $\times$).

Definition 7.4. Let M be a monoid and $X \subseteq M$. Then

$$\langle X \rangle = \{x_1 x_2 \dots x_n \mid n \geqslant 0 \text{ and } x_i \in X\}.$$

Notice that 1 (empty product) lies in $\langle X \rangle$ and if $x_1 x_2 \dots x_n,\ y_1 y_2 \dots y_m \in \langle X \rangle$ (where $x_i, y_i \in X$) then

$$(x_1 x_2 \dots x_n)(y_1 y_2 \dots y_m) = x_1 x_2 \dots x_n y_1 y_2 \dots y_m \in \langle X \rangle.$$

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, under multiplication, $\mathbb{N} = \langle P \rangle$, where P is the set of primes; $A^* = \langle A \rangle$.

7.3. The Transition Monoid of a DFA

We are going to demonstrate how a monoid is associated with a DFA $\mathscr{A}$; this will be denoted $M(\mathscr{A})$ and called the transition monoid *of $\mathscr{A}$.*

Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA. For each $w \in A^*$ let $\sigma_w \in \mathcal{T}_Q$ 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

$$\begin{aligned} q(\sigma_w\sigma_v) &= (q\sigma_w)\sigma_v \\ &= \delta(q,w)\sigma_v \\ &= \delta\big(\delta(q,w),v\big) \\ &= \delta(q,wv) \\ &= q\sigma_{wv}. \end{aligned}$$

Therefore $\sigma_w\sigma_v = \sigma_{wv}$. □

Now we note that $q\sigma_\varepsilon = \delta(q,\varepsilon) = q = qI_Q$ and therefore $\sigma_\varepsilon = I_Q$. Therefore

$$M(\mathscr{A}) = \{\sigma_w \mid w \in A^*\}$$

is a submonoid of $\mathcal{T}_Q$.

DEFINITION 7.5. $M(\mathscr{A})$ is the *transition monoid* of the DFA $\mathscr{A}$.

Note that the initial and final states do not matter for $M(\mathscr{A})$.

Let $w = a_1a_2\dots a_n \in A^*$ where $a_i \in A$. Then

$$\sigma_w = \sigma_{a_1a_2\dots a_n} = \sigma_{a_1}\sigma_{a_2}\dots\sigma_{a_n}.$$

and

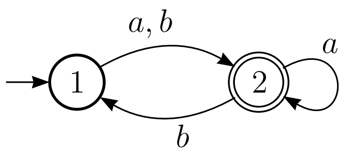
$$\sigma_{a^n} = \sigma_{aa\dots a} = \sigma_a\sigma_a\dots\sigma_a = \sigma_a^n.$$

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

$$|M(\mathscr{A})| \leqslant |\mathcal{T}_Q| = |Q|^{|Q|} < \infty.$$

<u>Examples of Finding Transition Monoids</u>

EXAMPLE 7.6. $A = \{a, b\}$ and $Q = \{1, 2\}$; $\mathscr{A}$:



	1	2
σ_a	2	2
σ_b	2	1

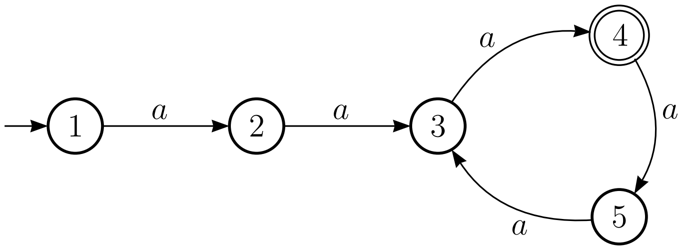
Calculate σ_a, σ_b – then calculate all products until we don't obtain any new elements
Now we have

$$\begin{aligned}
\sigma_a &= c_2, \\
\sigma_{a^2} &= \sigma_a\sigma_a = c_2 = \sigma_b\sigma_a = \alpha\sigma_a \text{ for all } \alpha, \\
\sigma_{b^2} &= \sigma_b\sigma_b = I_Q, \\
\sigma_a\sigma_b &= c_2\sigma_b = c_1.
\end{aligned}$$

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

	I	σ_b	c_2	c_1
I	I	σ_b	c_2	c_1
σ_b	σ_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

EXAMPLE 7.7. $A = \{a\}$, $Q = \{1, 2, 3, 4, 5\}$ and $\mathscr{A}$:



We have that $M(\mathscr{A}) = \langle \sigma_a \rangle = \{\sigma_a^n \mid n \geqslant 0\}$.

We have

$$\sigma_a^m \sigma_a^n = \sigma_a^{m+n} = \sigma_a^{n+m} = \sigma_a^n \sigma_a^m.$$

Calculate $\sigma_a, \sigma_a^2 = \sigma_{a^2}, \sigma_a^3, \ldots$..until we get a repeat.
We see that

$$\begin{aligned}
\sigma_a^5 &= \sigma_a^2, \\
\sigma_a^6 &= \sigma_a^5\sigma_a = \sigma_a^2\sigma_a = \sigma_a^3 \\
\sigma_a^7 &= \sigma_a^6\sigma_a = \sigma_a^3\sigma_a = \sigma_a^4,
\end{aligned}$$

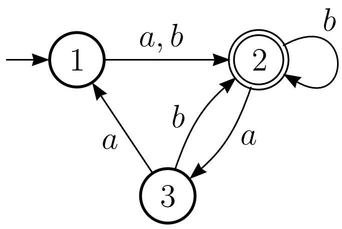
etc.
Hence $M(\mathscr{A}) = \{I, \sigma_a, \sigma_a^2, \sigma_a^3, \sigma_a^4\}$ and has table

	1	2	3	4	5
σ_a	2	3	4	5	3
σ_a^2	3	4	5	3	4
σ_a^3	4	5	3	4	5
σ_a^4	5	3	4	5	3
σ_a^5	3	4	5	3	4

	I	σ_a	σ_a^2	σ_a^3	σ_a^4
I	I	σ_a	σ_a^2	σ_a^3	σ_a^4
σ_a	σ_a	σ_a^2	σ_a^3	σ_a^4	σ_a^2
σ_a^2	σ_a^2	σ_a^3	σ_a^4	σ_a^2	σ_a^3
σ_a^3	σ_a^3	σ_a^4	σ_a^2	σ_a^3	σ_a^4
σ_a^4	σ_a^4	σ_a^2	σ_a^3	σ_a^4	σ_a^2

Note. We have that $T = \{\sigma_a^2, \sigma_a^3, \sigma_a^4\}$ is a 3 element 'subgroup' of $M(\mathscr{A})$.

EXAMPLE 7.8. $A = \{a, b\}$, $Q = \{1, 2, 3\}$ and $\mathscr{A}$:



We now have our table of transitions to be

	1	2	3
σ_a	2	3	1
σ_b	2	2	2
σ_a^2	3	1	2
$\sigma_b\sigma_a$	3	3	3
$\sigma_b\sigma_a^2$	1	1	1
σ_a^3	1	2	3

$$\sigma_b = c_2 \qquad \sigma_b\sigma_a = c_3 \qquad \sigma_b\sigma_a^2 = c_1$$

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

	I	σ_a	σ_a^2	c_1	c_2	c_3
I	I	σ_a	σ_a^2	c_1	c_2	c_3
σ_a	σ_a	σ_a^2	I	c_1	c_2	c_3
σ_a^2	σ_a^2	I	σ_a	c_1	c_2	c_3
c_1	c_1	c_2	c_3	c_1	c_2	c_3
c_2	c_2	c_3	c_1	c_1	c_2	c_3
c_3	c_3	c_1	c_2	c_1	c_2	c_3

Now $\{I, \sigma_a, \sigma_a^2\}$ is a 3 element 'subgroup' and $\{I\}, \{c_1\}, \{c_2\}, \{c_3\}$ are trivial 'subgroups'.

8. The Syntactic Monoid of a Language

Given any language L, we are going to calculate a monoid, denoted $M(L)$, from L; $M(L)$ is the Syntactic Monoid of L.

Let L be a language over A. For $u \in A^*$ define

$$C_L(u) = \big\{(w, z) \in A^* \times A^* \mid wuz \in L\big\}$$

the *context* of u. We will see that for a recognisable language L and a reduced DFA $\mathscr{A}$ recognising L, we have that for any $u, v \in A^*$

$$C_L(u) = C_L(v) \text{ if and only if } \sigma_u = \sigma_v.$$

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 8.1. *$u \sim_L u'$ and $v \sim_L v' \Rightarrow uv \sim_L u'v'$.*

Proof. Suppose $u \sim_L u'$ and $v \sim_L v'$. Then

$$\begin{aligned}(w,z)\in C_L(uv) &\Leftrightarrow wuvz\in L\\ &\Leftrightarrow wu(vz)\in L\\ &\Leftrightarrow (w,vz)\in C_L(u)\\ &\Leftrightarrow (w,vz)\in C_L(u')\\ &\Leftrightarrow wu'vz\in L\\ &\Leftrightarrow (wu')vz\in L\\ &\Leftrightarrow (wu',z)\in C_L(v)\\ &\Leftrightarrow (wu',z)\in C_L(v')\\ &\Leftrightarrow wu'v'z\in L\\ &\Leftrightarrow (w,z)\in C_L(u'v').\end{aligned}$$

Hence we have $C_L(uv) = C_L(u'v')$ and so $uv \sim_L u'v'$. □

Now set $M(L) = \big\{[w] \mid w \in A^*\big\}$ 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 Lemma 8.1,

$$uv \sim_L u'v'$$

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

Lemma 8.2. *$M(L)$ is a monoid under this binary operation.*

Proof. For all $[u], [v], [w] \in M(L)$ we have

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

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. □

Definition 8.3.
- $\sim_L$ 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 $(\varepsilon, \varepsilon) \in C_L(u) = C_L(v)$ and so $v = \varepsilon v \varepsilon \Rightarrow v \in L$. Therefore L is a union of $\sim_L$-classes.

Calculation of $M(L)$

Example 8.4. Take $A = \{a, b\}$ and $L = A$. For $w \in A^*$ with $|w| > 1$, we have

$$\begin{aligned}
C_L(w) &= \emptyset, \\
C_L(\varepsilon) &= \big\{(\varepsilon, a), (a, \varepsilon), (\varepsilon, b), (b, \varepsilon)\big\}, \\
C_L(a) &= \big\{(\varepsilon, \varepsilon)\big\} = C_L(b).
\end{aligned}$$

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

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

So the multiplication table of our monoid is

$$\begin{array}{c|ccc}
 & 1 & L & T \\ \hline
1 & 1 & L & T \\
L & L & T & T \\
T & T & T & T
\end{array}$$

because we have

$$\begin{aligned}
LL &= [a][a] = [a^2] = T, \\
LT &= [a][a^2] = [a^3] = TL = T.
\end{aligned}$$

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

Example 8.5. $A = \{a, b\}$ and $L = \{ba, ab\}$. Now the contexts are

$$\begin{aligned}
C_L(\varepsilon) &= \big\{(\varepsilon, ba), (b, a), (ba, \varepsilon), (\varepsilon, ab), (a, b), (ab, \varepsilon)\big\} \\
C_L(a) &= \big\{(b, \varepsilon), (\varepsilon, b)\big\} \\
C_L(b) &= \big\{(\varepsilon, a), (a, \varepsilon)\big\} \\
C_L(ba) &= \big\{(\varepsilon, \varepsilon)\big\} = C_L(ab) \\
C_L(a^2) &= \emptyset = C_L(b^2) = C_L(w)
\end{aligned}$$

for all w with $|w| \geqslant 3$. So, there exists 5 $\sim_L$-classes:

$$[\varepsilon] = \{\varepsilon\} = 1 \quad [a] = \{a\} = P \quad [b] = \{b\} = Q$$

$$[ab] = \{ab, ba\} = L \quad [a^2] = \{a^2, b^2, w \mid |w| \geqslant 3\} = 0.$$

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

	1	P	Q	L	0
1	1	P	Q	L	0
P	P	0	L	0	0
Q	Q	L	0	0	0
L	L	0	0	0	0
0	0	0	0	0	0

We know the above because

$$\begin{aligned} P^2 &= [a][a] = [a^2] = 0, \\ PQ &= [a][b] = [ab] = L, \\ PL &= [a^2b] = 0, \text{ etc} \end{aligned}$$

We now show how syntactic monoids are related to transition monoids.

Proposition 8.6. *Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a reduced DFA and let $L = L(\mathscr{A})$. Then for any $u, v \in A^*$ we have*

$$\sigma_u = \sigma_v \Leftrightarrow [u] = [v]$$

where $[w]$ is the $\sim_L$-class of w.

Proof. We have that

$$\begin{aligned}
u \sim_L v &\Leftrightarrow C_L(u) = C_L(v), \\
&\Leftrightarrow \forall\, w, z \in A^*, \\
&\qquad \big((w,z) \in C_L(u) \Leftrightarrow (w,z) \in C_L(v)\big), \\
&\Leftrightarrow \forall\, w, z \in A^*, \\
&\qquad \big(wuz \in L \Leftrightarrow wvz \in L\big), \\
&\Leftrightarrow \forall\, w, z \in A^*, \\
&\qquad \delta(q_0, wuz) \in F \Leftrightarrow \delta(q_0, wvz) \in F \\
&\Leftrightarrow \forall w, z \in A^*, \\
&\qquad \delta\big(\delta(q_0, w), uz\big) \in F \Leftrightarrow \delta\big(\delta(q_0, w), vz\big) \in F \\
&\Leftrightarrow \forall\, q \in Q\, \forall\, z \in A^*, \\
&\qquad \delta(q, uz) \in F \Leftrightarrow \delta(q, vz) \in F \text{ by accessibility} \\
&\Leftrightarrow \forall\, q \in Q\, \forall\, z \in A^*, \\
&\qquad \delta\big(\delta(q, u), z\big) \in F \Leftrightarrow \delta\big(\delta(q, v), z\big) \in F \\
&\Leftrightarrow \forall q \in Q, \delta(q, u) \sim \delta(q, v) \\
&\Leftrightarrow \forall\, q \in Q, \delta(q, u) = \delta(q, v) \text{ as } \mathscr{A} \text{ is reduced} \\
&\Leftrightarrow \forall\, q \in Q, q\sigma_u = q\sigma_v \\
&\Leftrightarrow \sigma_u = \sigma_v
\end{aligned}$$

□

Corollary 8.7. *Let $L \in \operatorname{Rec} A^*$. Then $M(L)$ is finite.*

Proof. Let $L \in \operatorname{Rec} A^*$. Find a DFA $\mathscr{A}$ with $L = L(\mathscr{A})$, reduce $\mathscr{A}$ to $\overline{\mathscr{A}}$ so that $L = L(\overline{\mathscr{A}})$. Find $M(\overline{\mathscr{A}})$. From Proposition 8.6 we have that

$$|M(L)| = |M(\overline{\mathscr{A}})| < \infty.$$

□

We will later show a converse to Corollary 8.7.

Let $L \in \operatorname{Rec} A^*$; we know that $M(L)$ is finite. How do we calculate it? Either *directly* by finding *contexts*; or we find a DFA $\mathscr{A}$ with $L = L(\mathscr{A})$, reduce $\mathscr{A}$ to $\overline{\mathscr{A}}$ so that $L = L(\overline{\mathscr{A}})$ also, and find $M(\overline{\mathscr{A}})$. Then use the following. First, a definition.

Definition 8.8. Let M, N be monoids with identities 1_M and 1_N. A map $\theta : M \to N$ is a *(monoid) morphism* if

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

If in addition θ is a bijection, then θ is an *isomorphism*.

Theorem 8.9. *If $L = L(\mathscr{A})$ for a* reduced *DFA $\mathscr{A}$, then $M(L) \cong M(\mathscr{A})$, i.e. there exists an isomorphism $\theta : M(L) \to M(\mathscr{A})$.*

Proof. We have

$$\begin{aligned} M(L) &= \big\{[u] \mid u \in A^*\big\} \text{ where } u \sim_L v \Leftrightarrow C_L(u) = C_L(v), \\ M(\mathscr{A}) &= \{\sigma_u \mid u \in A^*\} \text{ where } q\sigma_u = \delta(q, u). \end{aligned}$$

From Proposition 8.6, $\theta : M(L) \to M(\mathscr{A})$ given by $[u]\theta = \sigma_u$ is a bijection. Let $[u], [v] \in M(L)$. Then

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

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

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

Therefore θ is a morphism and hence an isomorphism as required. □

9. Recognition by a Monoid

We now show how finite monoids determine recognisable languages.
First, an example of a morphism:

Example 9.1. Let $\theta : A^* \to \mathbb{N}^0$ (under $+$) be given by

$$w\theta = |w|.$$

Then $\varepsilon\theta = |\varepsilon| = 0$ (and remember 0 is the identity of $\mathbb{N}^0$) and for all $v, w \in A^*$,

$$(vw)\theta = |vw| = |v| + |w| = v\theta + w\theta.$$

Thus θ is a morphism.

Above, once we know that every letter *is sent to 1, then, for θ to be a morphism, every word of length n has to be sent to n lots of 1, hence n. We now build on that idea to answer:*

Theorem 9.2. 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

$$\varepsilon\theta = 1$$
$$(a_1 \dots a_n)\theta = a_1\varphi \dots a_n\varphi, \ \ a_i \in A.$$

Clearly θ is well-defined. We check that θ is a morphism:

$$(\varepsilon v)\theta = v\theta = 1(v\theta) = (\varepsilon\theta)(v\theta),$$

for any $v \in A^*$, and similarly

$$(v\varepsilon)\theta = (v\theta)(\varepsilon\theta).$$

Finally, if $w = a_1 \dots a_m, v = b_1 \dots b_n \in A^*$ where $m, n \geq 1, a_i, b_j \in A, 1 \leq i \leq m, 1 \leq j \leq n$, then

$$\begin{aligned}
(wv)\theta &= ((a_1 \dots a_m)(b_1 \dots b_n))\theta \\
&= (a_1 \dots a_m b_1 \dots b_n)\theta \\
&= a_1\varphi \dots a_m\varphi b_1\varphi \dots b_n\varphi \\
&= (a_1\varphi \dots a_m\varphi)(b_1\varphi \dots b_n\varphi) \\
&= w\theta v\theta.
\end{aligned}$$

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 $w = a_1a_2 \dots a_n$, $a_i \in A$, $n \geqslant 1$ we have

$$\begin{aligned}
w\psi = (a_1 \dots a_n)\psi &= a_1\psi \dots a_n\psi && (\psi \text{ is a morphism}) \\
&= a_1\varphi \dots a_n\varphi && (a_i\psi = a_i\varphi) \\
&= (a_1 \dots a_n)\theta && (\text{definition of } \theta) \\
&= w\theta.
\end{aligned}$$

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

Thus, to define a morphism *from A^* to any monoid, it is* enough *to say where the letters are sent. The word 'free' refers to this property of A^*.*

For convenience we recall some notation regarding 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 θ. The notation $S\theta^{-1}$ does NOT imply the function θ^{-1} exists.

Remark. We will be interested in the condition $R = (R\theta)\theta^{-1}$. Note that this is equivalent to $R = S\theta^{-1}$ for some $S \subseteq B$.
We always have that $R \subseteq (R\theta)\theta^{-1}$, since if $r \in R$ then $r\theta \in R\theta$ so $r \in (R\theta)\theta^{-1}$.
For $R = (R\theta)\theta^{-1}$, we need that $w \in (R\theta)\theta^{-1} \Rightarrow w \in R$, i.e.

$$w\theta \in R\theta \Rightarrow w \in R$$

i.e.

$$w\theta = v\theta,\ \text{some } v \in R \Rightarrow w \in R.$$

Definition 9.3. 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 $L = (L\theta)\theta^{-1}$.

Theorem 9.4. *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

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

Hence ν_L is a morphism.
We know $L \subseteq (L\nu_L)\nu_L^{-1}$. 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 ν_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 $M(L)$. □

Theorem 9.5. *The following are equivalent for a language $L \subseteq A^*$:*

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

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 $\mathscr{A} = (A, M, \delta, 1, L\theta)$ where $\delta(m, a) = m(a\theta)$. We check that $\delta(m, w) = m(w\theta)$ for all $w \in A^*$.
First, $\delta(m, \varepsilon) = m$ by the definition of the extension of δ. Next, θ is a monoid morphism, and so $\varepsilon\theta = 1$. Thus

$$\delta(m, \varepsilon) = m = m1 = m(\varepsilon\theta).$$

Let $|w| = k+1$ with $k \geq 0$ and assume that $\delta(m, v) = m(v\theta)$ for all $v \in A^*$ of length k. Now $w = va$ for some $a \in A$ and $v \in A^*$ with $|v| = k$ and so

$$\begin{aligned}
\delta(m, w) &= \delta(\delta(m, v), a) \\
&= \delta(m(v\theta), a) && \text{(by the induction hypothesis)} \\
&= m(v\theta)(a\theta) && \text{(by definition of } \delta\text{)} \\
&= m(va)\theta && \text{(since } \theta \text{ is a morphism)} \\
&= m(w\theta).
\end{aligned}$$

Hence, by induction, $\delta(m, w) = m(w\theta)$ for all $w \in A^*$ of positive length.
Then

$$\begin{aligned}
w \in L(\mathscr{A}) &\Leftrightarrow \delta(1, w) \in L\theta, \\
&\Leftrightarrow 1(w\theta) \in L\theta, \\
&\Leftrightarrow w\theta \in L\theta, \\
&\Leftrightarrow w \in (L\theta)\theta^{-1}, \\
&\Leftrightarrow w \in L \text{ as } (L\theta)\theta^{-1} = L.
\end{aligned}$$

Hence $L(\mathscr{A}) = L$ so L is recognised by $\mathscr{A}$ and hence $L \in \operatorname{Rec} A^*$.

(iii) $\Rightarrow$ (i): If $L \in \operatorname{Rec} A^*$ then $L = L(\mathscr{A})$ for some reduced DFA $\mathscr{A}$. By Theorem 8.9, $M(L) \cong M(\mathscr{A})$ so that $M(L)$ is finite as $M(\mathscr{A})$ is.
Hence all statements are equivalent. □

We have now proved the following

Theorem 9.6. Summary *Let L be a language over A^*. The following are equivalent:*

(i) *L is recognisable ($L \in \operatorname{Rec} A^*$; $L = L(\mathscr{A})$ for some DFA $\mathscr{A}$);*
(ii) *$L = L(\mathscr{A})$ for some NDA $\mathscr{A}$;*
(iii) *L is rational ($L \in \operatorname{Rat} A^*$);*
(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***.

9.1. How do Monoids help us?

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

Definition 9.7. $w^{-1}L = \{v \in A^* \mid wv \in L\}$.

Example 9.8. $L \in \operatorname{Rec} A^* \Rightarrow w^{-1}L \in \operatorname{Rec} A^*$ for any $w \in A^*$.

Proof. $L \in \operatorname{Rec} A^* \Rightarrow L$ 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 $\big((w^{-1}L)\theta\big)\theta^{-1} = w^{-1}L$. We know

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

Now

$$\begin{aligned} v \in \big((w^{-1}L)\theta\big)\theta^{-1} &\Rightarrow v\theta \in (w^{-1}L)\theta, \\ &\Rightarrow v\theta = x\theta, \text{ for some } x \in w^{-1}L, \\ &\Rightarrow v\theta = x\theta, \text{ for some } x \text{ with } wx \in L. \end{aligned}$$

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

Recall: To find an example of a language with a pumping length that was not recognisable, we needed that

$$L = \{a^n b^p \mid n \geqslant 1, p \text{ prime}\} \notin \operatorname{Rec} A^*.$$

We argued that $K = \{a^n b^p \mid n \geqslant 0, p \text{ prime}\} \notin \operatorname{Rec} A^*$.
We have that $u \in a^{-1}L \Leftrightarrow au \in L \Leftrightarrow u \in K$. Hence $a^{-1}L = K$. If $L \in \operatorname{Rec} A^*$, then we would have $a^{-1}L \in \operatorname{Rec} A^*$, i.e. $K \in \operatorname{Rec} A^*$ – a contradiction. Hence $L \notin \operatorname{Rec} A^*$ as required.

We can also use monoids to show closure properties under Boolean operations:

Example 9.9. $L, K \in \operatorname{Rec} A^* \Rightarrow L \cap K \in \operatorname{Rec} A^*$.

Proof. There exists finite monoids M, N and morphisms $\theta : A^* \to M$ and $\psi : A^* \to N$ 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 $\varphi : A^* \to M \times N$ by $w\varphi = (w\theta, w\psi)$. Check φ is a morphism. We know $L \cap K \subseteq \big((L \cap K)\varphi\big)\varphi^{-1}$. Let $w \in \big((L \cap K)\varphi\big)\varphi^{-1}$. 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 $u \in L$, $w \in (L\theta)\theta^{-1} = L$ and as $u \in K$, $w \in (K\psi)\psi^{-1} = K$. Hence $w \in L \cap K$ so that $\big((L \cap K)\varphi\big)\varphi^{-1} \subseteq L \cap K$. Hence $L \cap K = \big((L \cap K)\varphi\big)\varphi^{-1}$ and $L \cap K$ is recognisable by $M \times N$, hence $L \cap K \in \operatorname{Rec} A^*$. □

10. Schützenbergers Theorem

Having shown how monoids determine the class of recognisable (regular) languages, we now give one way in which monoids can be used to pick out important classes of recognisable languages.

Definition 10.1. $L \subseteq A^*$ 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 $L \in \operatorname{Rec} A^*$ (as $\operatorname{Rec} A^*$ contains the finite languages and is closed under Boolean operations and product). By Kleene's Theorem, L star-free implies $L \in \operatorname{Rat} A^*$.

Example 10.2. (a) $\{ab, a, bab\}, \emptyset, \{\varepsilon\}$ are finite, hence star-free.
(b) $\{ab, a\}^c\{ba, aba\} \cup \big(\{aa\}^c \cap \{bb\}^c\big)$ 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) $L = \{x \in A^* \mid |x|_a \geqslant 1\} = A^*aA^* = \emptyset^c a\emptyset^c$ 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 10.3. Let M be a monoid and let $G \subseteq M$ then G is a subgroup of M if

1. G is closed, i.e. $a, b \in G \Rightarrow ab \in G$;
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 10.4. Let M be a monoid, then $e \in M$ is *idempotent* if $e = e^2$. We denote by $E(M)$ the set of idempotents of M.

Notice that $1 \in E(M)$. If G is a group, then only the identity of G has this property, as

$$e = e^2 \Rightarrow 1_G e = ee \Rightarrow 1_G = e,$$

as we can cancel in G.

Example 10.5. (i) $e \in E(M) \Rightarrow \{e\}$ is a subgroup, a trivial subgroup with identity e.

(ii) $\mathcal{S}_X$ is a subgroup of $\mathcal{T}_X$.

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

(iv) Let $M = \{I, \alpha, 0\}$ have table

	I	α	0
I	I	α	0
α	α	I	0
0	0	0	0

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

(v) From Example 7.7 we found $M(\mathscr{A})$

	I	σ_a	σ_{a^2}	σ_{a^3}	σ_{a^4}
I	I	σ_a	σ_{a^2}	σ_{a^3}	σ_{a^4}
σ_a	σ_a	σ_{a^2}	σ_{a^3}	σ_{a^4}	σ_{a^2}
σ_{a^2}	σ_{a^2}	σ_{a^3}	σ_{a^4}	σ_{a^2}	σ_{a^3}
σ_{a^3}	σ_{a^3}	σ_{a^4}	σ_{a^2}	σ_{a^3}	σ_{a^4}
σ_{a^4}	σ_{a^4}	σ_{a^2}	σ_{a^3}	σ_{a^4}	σ_{a^2}

Let $T = \{\sigma_{a^2}, \sigma_{a^3}, \sigma_{a^4}\}$. By inspection:

T is closed;

σ_{a^3} is the identity;

$(\sigma_{a^3})^2 = \sigma_{a^3}$ and $\sigma_{a^2}\sigma_{a^4} = \sigma_{a^3} = \sigma_{a^4}\sigma_{a^2}$ so that σ_{a^2} and σ_{a^4} are mutually inverse.

Hence T is a subgroup of $M(\mathscr{A})$.

Definition 10.6. A finite monoid M is *aperiodic* if all of its subgroups are trivial.

Example 10.7. Let $M = \{1, 0\}$ with table

	1	0
1	1	0
0	0	0

Notice that $e = e^2$ for every $e \in M$. Since any subgroup contains exactly one idempotent, M is aperiodic.

Clearly the monoids in Example 10.5 (iv) and (v) are not aperiodic.

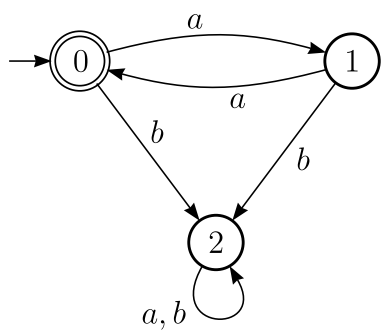
Theorem 10.8. Schützenberger's Theorem *A language L is star-free $\Leftrightarrow$ $M(L)$ is finite and aperiodic.*

Proof. No proof in this course. $\square$

10.1. Examples to illustrate Schützenberger's Theorem

EXAMPLE 10.9. Let $A = \{a, b\}$. Then $L = (aa)^*$ is not star-free.

We have $L = L(\mathscr{A})$ where $\mathscr{A}$ is:



We show that $\mathscr{A}$ is reduced.
The $\sim$-classes are

$$\begin{array}{ll} \sim_0 -\text{classes}: & \{0\}, \{1, 2\}, \\ \sim_1 -\text{classes}: & \{0\}, \{1\}, \{2\} \\ & \text{as } \delta(1, a) = 0 \not\sim_0 2 = \delta(2, a). \end{array}$$

Hence $\sim = \sim_1$ and the $\sim$-classes are $\{0\}, \{1\}, \{2\}$ and so $\mathscr{A}$ is reduced.
From Theorem 8.9 we have that $M(L) \cong M(\mathscr{A})$, so that clearly $M(L)$ is finite.
The table for $M(\mathscr{A})$ is

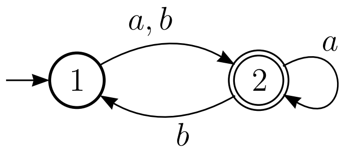
	0	1	2
σ_a	1	0	2
σ_b	2	2	2
σ_{a^2}	0	1	2

Notice that $\sigma_b = c_2$ and $c_2\alpha = c_2 = \alpha c_2$ for all α.
Hence $M(\mathscr{A}) = \{I, \sigma_a, c_2\}$ and has table

	I	σ_a	c_2
I	I	σ_a	c_2
σ_a	σ_a	I	c_2
c_2	c_2	c_2	c_2

As $\{I, \sigma_a\}$ is a non-trivial subgroup, $M(L)$ and hence $M(\mathscr{A})$ is not aperiodic. By Schützenberger's theorem, L is not star-free.

Example 10.10. Recall Example 7.6
$A = \{a, b\}$ and $Q = \{1, 2\}$; $\mathscr{A}$:



We have

$$L(\mathscr{A}) = Aa^*(bAa^*)^*.$$

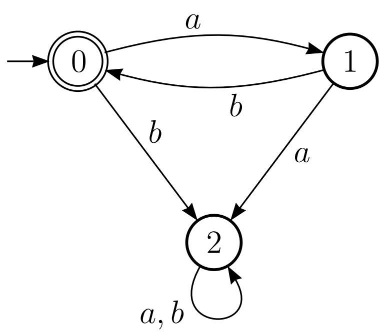
We have $M(\mathscr{A}) = \{I_Q, \sigma_b, c_2, c_1\}$, which has multiplication table

	I	σ_b	c_2	c_1
I	I	σ_b	c_2	c_1
σ_b	σ_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

Now, $\mathscr{A}$ is reduced, as it has two states and a one-state DFA can only accept A^* or $\emptyset$. Thus $M(L) \cong M(\mathscr{A})$.
Clearly $M(\mathscr{A})$ is not aperiodic as $\{I, \sigma_b\}$ is a non-trivial subgroup. By Schützenberger's theorem, L is not star-free.

Example 10.11. Consider $L = (ab)^* \subseteq \{a, b\}^*$. We have already seen that L is $*$-free. We now use L as an illustration of Schützenberger's theorem.

First, note that $L = L(\mathscr{A})$ for the DFA $\mathscr{A}$ given by:



We show that $\mathscr{A}$ is reduced. The $\sim$-classes are

$$\begin{array}{rl} \sim_0 -\text{classes}: & \{0\}, \{1, 2\}, \\ \sim_1 -\text{classes}: & \{0\}, \{1\}, \{2\} \\ & \text{as } \delta(1, b) = 0 \not\sim_0 2 = \delta(2, b). \end{array}$$

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

	0	1	2
σ_a	1	2	2
σ_b	2	0	2
$\sigma_{a^2} = \sigma_{b^2} = c_2$	2	2	2
$\sigma_a \sigma_b$	0	2	2
$\sigma_b \sigma_a$	2	1	2

Notice that $c_2 \alpha = c_2 = \alpha c_2$ for all α. Further, $\sigma_a \sigma_b \sigma_a = \sigma_a$ and $\sigma_b \sigma_a \sigma_b = \sigma_b$.

It follows that

$$M(\mathscr{A}) = \{I, \sigma_a, \sigma_b, \sigma_{ab}, \sigma_{ba}, c_2\}$$

and has table:

	I	σ_a	σ_b	σ_{ab}	σ_{ba}	c_2
I	I	σ_a	σ_b	σ_{ab}	σ_{ba}	c_2
σ_a	σ_a	c_2	σ_{ab}	c_2	σ_a	c_2
σ_b	σ_b	σ_{ba}	c_2	σ_b	c_2	c_2
σ_{ab}	σ_{ab}	σ_a	c_2	σ_{ab}	c_2	c_2
σ_{ba}	σ_{ba}	c_2	σ_b	c_2	σ_{ba}	c_2
c_2	c_2	c_2	c_2	c_2	c_2	c_2

We claim that $M(\mathscr{A})$ is aperiodic. First, any subgroup has to have an identity, which must be an idempotent of $M(\mathscr{A})$. The idempotents are:

$$I, \sigma_{ab}, \sigma_{ba}, c_2.$$

The idempotent I does not appear in any row other than the first, so no element has an inverse with respect to I. Thus the only subgroup with I as identity is $\{I\}$.

Given that c_2 is a zero for our multiplication the only subgroup containing c_2 is $\{c_2\}$.

Consider σ_{ab}: if α lies in a subgroup with identity σ_{ab}, then there is a β with $\alpha\beta = \sigma_{ab}$, i.e. σ_{ab} lies in the row of α. We notice that σ_{ab} only appears in rows indexed by σ_a and σ_{ab}. But, if σ_a lies in a subgroup, then $(\sigma_a)^2 = c_2$ lies in the same subgroup. So if σ_a lies in a subgroup with identity σ_{ab}, then c_2 would also be in this subgroup. However, c_2 is idempotent and different from σ_{ab}. It follows that the only subgroup with σ_{ab} as identity is $\{\sigma_{ab}\}$.

The argument for σ_{ba} is similar.

Thus $M(L)$ is aperiodic. By Schützenberger's theorem, L is star-free.

Department of Mathematics
Formal Languages and Automata 2021/22
Exercises

Section 1: Fundamental Concepts

1. Let $K = \{ab, aba\}$, $L = \{aa, ba\}$ and $M = \{a\}$. Write down the following:

   (a) KL;
   (b) LM;
   (c) KM;
   (d) $KL \cup KM$;
   (e) $L \cup M$;
   (f) $K(L \cup M)$;
   (g) $(KL)M$;
   (h) $K(LM)$.

   Notice that for this *choice of* K, L *and* M*, we have that*
   $$KL \cup KM = K(L \cup M) \text{ and } (KL)M = K(LM).$$

2. Let A be a finite alphabet and K, L, M be any subsets of A^*. Prove that
   $$K(L \cup M) = KL \cup KM.$$

3. Let A be a finite alphabet and K, L, M be any subsets of A^*. Prove that
   $$K(L \cap M) \subseteq KL \cap KM.$$
   Using $A = \{a, b\}$, find examples of subsets K, L, M of A^* such that
   $$K(L \cap M) \neq KL \cap KM.$$

4. Let L be a subset of A^* where A is an alphabet. Verify the following:
   (a) $L^*L^* = L^*$,
   (b) $L^{**} = L^*$, where $L^{**} = (L^*)^*$,
   (c) $L^* = \{\varepsilon\} \cup LL^* = \{\varepsilon\} \cup L^*L$.

5. Let A be an alphabet. Show that if $L = \{u^h\}$ and $K = \{u^\ell\}$ for some word $u \in A^*$ and $h, \ell \in \mathbb{N}^0$, then $LK = KL$.
   Do we always have $LK = KL$, for arbitrary languages L, K over A?

6. A word $w \in A^*$ is a *factor* of a word x if $x = uwv$ for some words $u, v \in A^*$. Let $A = \{a, b\}$ and let
   $$L = \{ab^k, a^2b^k : k \geq 1\}^* \setminus \{\varepsilon\}.$$
   Show that L is the set of words that start with a, end with b and contain no factor of a^3.

7. Show that for languages L, K, M over A,

$$L(KM) = (LK)M.$$

Now explain why $\mathcal{L}(A)$ is a monoid, where $\mathcal{L}(A)$ is the set of languages over A.

8. Show that the identity of monoid is always unique, i.e. if M is a monoid and $1, 1' \in M$ with

$$1\,a = a = a\,1 \text{ and } 1'\,a = a = a\,1' \text{ for all } a \in M,$$

then $1 = 1'$.

9. Let M be a monoid. An element $e \in M$ is *idempotent* if $e^2 = e$.
Show that the identity $1 \in M$ is idempotent.
   (*a*) Find an example of a monoid M with two elements such that 1 is the only idempotent.
   (*b*) Find an example of a monoid M with two elements such that every element of M is idempotent.

10. For any non-empty set X, $\mathcal{T}_X$ denotes the set of all maps from X to X. Explain why $\mathcal{T}_X$ is a monoid under composition of functions with identity I_X (the identity map on X).
Show that if $|X| \geq 2$ then $\mathcal{T}_X$ has an idempotent ε such that $\varepsilon \neq I_X$.
($\mathcal{T}_X$ is called the *full transformation monoid* on X - we will need this monoid later on in the module).

Section 2: Automata: DFAs

1. *This question is asking you to prove the δ-Lemma.*
Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA. Show that for any $u, v \in A^*$ and $q \in Q$,

$$\delta(q, uv) = \delta(\delta(q, u), v).$$

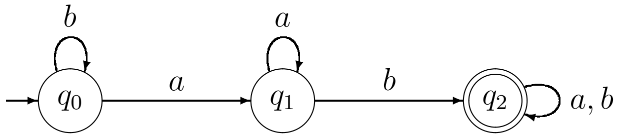
Hint: use induction on the length of v.

2. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA. Explain why $\varepsilon \in L(\mathscr{A})$ if and only if $q_0 \in F$.

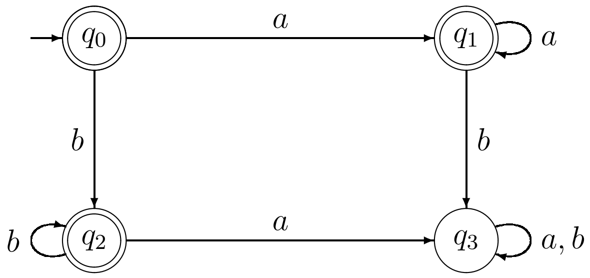
3. Let $A = \{a, b\}$. For each of the following languages, write down a DFA which accepts it.
   (*a*) $L = \{x \in A^* : |x|_a \leqslant 3\}$,
   (*b*) $L = \{x \in A^* : |x|_a \geqslant 3\}$,
   (*c*) $L = \{x \in A^* : |x| \equiv 0 \pmod 4\}$,
   (*d*) $L = \{ab^2xb : x \in A^*\}$,
   (*e*) $L = \{abwba \in A^* : w \in A^*\}$.

4. Describe the language recognised by $\mathscr{A}$ for each of the following DFAs $\mathscr{A}$ (you do not have to provide justification):

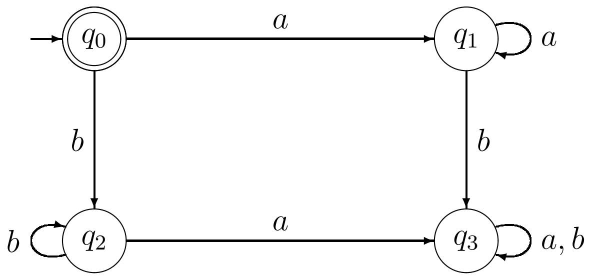
(a)



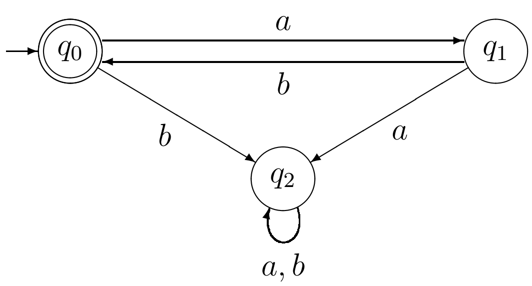
(b)



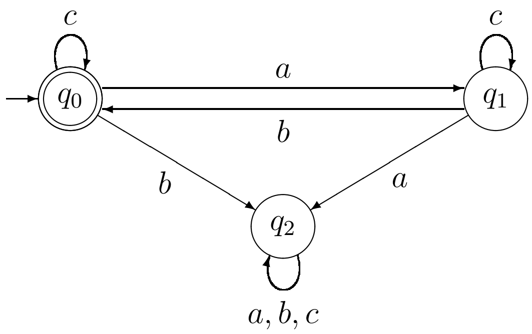
(c)



5. Let $A = \{a, b\}$. What is the language recognised by the DFA $\mathscr{A}$ below? Try to write down a formal argument justifying your answer.



6. Let $A = \{a, b, c\}$. What is the language recognised by the DFA $\mathscr{B}$ below? (You do not need to justify your answer, but please be careful to write it down in a syntactically correct form - I hope you have already attempted a justification for Question 5!).



7. Use the pumping lemma to prove that the following languages are not recognisable.
   (a) $L = \{a^n b^{3n} : n \geqslant 0\}$,
   (b) $L = \{w^3 : w \in \{a, b\}^*\}$,
   (c) $L = \{a^{n^2} : n \geqslant 1\}$.

Section 3: Automata - NDAs

1. Let $L = \{a, b\}^*\{aaa, bbb\}\{a, b\}^*$. Find an NDA which recognises L.

2. Find an NDA which recognises the set L of non-empty words w over $A = \{a, b, c\}$ such that the last letter of w occurs at least twice in w, that is,

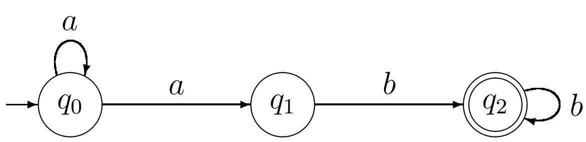
$$L = \{w \in A^+ : w = w'd \Rightarrow |w|_d \geq 2, d \in A\}.$$

   Write down an expression for L (in terms of Boolean operations, product and star).

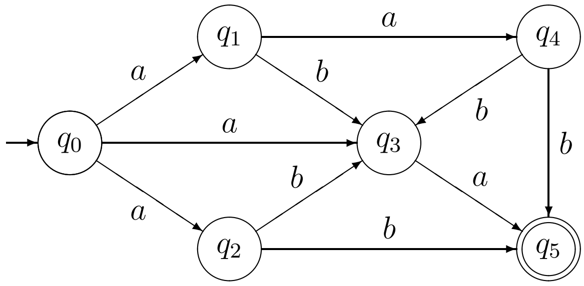
3. Let $\mathscr{A} = (A, Q, E, I, F)$ be an NDA. Show that $\varepsilon \in L(\mathscr{A})$ if and only if $I \cap F \neq \emptyset$.

4. For each NDA below use the standard technique to find (and draw the state transition diagram of) a DFA $\mathscr{B}$ which recognises the same language.
   Be sure to show your calculations.

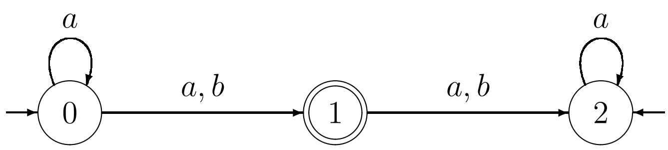
(a)



(b)



(c)



Section 4: Closure properties of Rec A^*

1. Explain from closure properties of Rec A^* why

$$K = \{a^m b^n : m, n \geqslant 0\}$$

is in Rec$\{a, b\}^*$. Now find an NDA that recognises K.

2. Let A be an alphabet and let $B \subseteq A$. Show that for $L \subseteq B^*$ we have $L \in \operatorname{Rec} A^*$ if and only if $L \in \operatorname{Rec} B^*$.

So, in considering whether or not a language is recognisable, we do not need to worry which alphabet we use, provided it contains all letters occurring in any word in the language concerned.

3. Let $A = \{a, b, c\}$. Recall that

$$L = \{a^n b^n : n \geq 0\}$$

is not recognisable.

(a) Let k be a fixed positive integer and let

$$L_k = \{a^n b^n : n \geqslant k\}.$$

Using closure properties of Rec A^* show that $L_k \notin \operatorname{Rec} A^*$.

(b) Now let

$$L' = \{a^n b^n c^m : m, n \geq 0\}.$$

Again using closure properties of Rec A^*, show that $L' \notin \operatorname{Rec} A^*$.

4. Let $A = \{a, b, c, d\}$. Let
$$L = \{w \in A^* : w = c^i v d^j : i, j \geq 0, v \in \{a, b\}^*, 3|v|_a = |v|_b\}.$$
Without using the Pumping Lemma, show that L is not recognisable.

5. Let $A = \{a, b, c\}$ and let $L = \{a^m b^p c^n : m, n \geq 0, p \text{ prime}\}$. Without using the Pumping Lemma, prove that L is not recognisable.

6. (a) Let A be an alphabet. Prove that $\operatorname{Rec} A^*$ is *not* closed under infinite union. Hint: Note that any language is a union of one-element sets.
   (b) Let I be a nonempty set and for each $i \in I$, let L_i be a language over the alphabet A. Prove that $\bigcup_{i \in I} L_i = (\bigcap_{i \in I} L_i^c)^c$.
   (c) Deduce that $\operatorname{Rec} A^*$ is *not* closed under infinite intersection.

7. Let A be an alphabet. In this question we show how the closure of $\operatorname{Rec} A^*$ under intersection and union can be proved using DFAs.
   Let $L = L(\mathscr{A})$ and $K = L(\mathscr{B})$ where $\mathscr{A} = (A, Q, \delta, q_0, F)$ and $\mathscr{B} = (A, P, \sigma, p_0, T)$ are DFAs. Define DFAs $\mathscr{A} \times \mathscr{B}$ and $\mathscr{A} \sqcup \mathscr{B}$ as follows:
$$\mathscr{A} \times \mathscr{B} = (A, Q \times P, \rho, (q_0, p_0), F \times T)$$
   and
$$\mathscr{A} \sqcup \mathscr{B} = (A, Q \times P, \rho, (q_0, p_0), (F \times P) \cup (Q \times T)).$$
   where $\rho((q, p), a) = (\delta(q, a), \sigma(p, a))$ for $(q, p) \in Q \times P, a \in A$.
   (a) Show that $\rho((q, p), w) = (\delta(q, w), \sigma(p, w))$ for all $(q, p) \in Q \times P$ and all $w \in A^*$. (This works for both the new DFAs.)
   (b) Now show that $L \cap K = L(\mathscr{A} \times \mathscr{B})$.

8. Find DFAs (i.e., draw the state transition graphs), each with two states, which recognise the languages L_0 and L_1 where
$$L_0 = \{w \in \{a, b\}^* : |w|_a \equiv 0 \pmod 2\} \text{ and } L_1 = \{w \in \{a, b\}^* : |w|_b \equiv 1 \pmod 2\}.$$
   Using Question 7 draw the state transition graph of a DFA that recognises the language L where
$$L = \{w \in \{a, b\}^* : |w|_a \equiv 0 \pmod 2, |w|_b \equiv 1 \pmod 2\}.$$

Section 5: Rational operations and Kleene's theorem

1. Let A be a finite alphabet. Explain why if $L_i \in \operatorname{Rat} A^*$ for $1 \leq i \leq n$, then
$$L_1 \cap L_2 \cap \ldots \cap L_n \in \operatorname{Rat} A^*.$$
   [Hint. Use Kleene's Theorem and closure results for $\operatorname{Rec} A^*$.]

2. Give rational expressions for each of the following languages over $\{a, b\}$.
   (a) L is the set of all words which contain exactly 3 a's;
   (b) L is the set of all words which contain exactly 2 a's or exactly 3 a's;
   (c) L is the set of all words which end in a double letter (i.e. in the square of a letter);
   (d) L is the set of all words in which a appears only in blocks of multiples of 3.

3. Give a rational expression for the language L over $\{a, b\}$, where L is the set of all words which do not contain a factor aaa. Justify your equality.

4. Use Kleene's Theorem to show that the following subsets of $\{a, b\}^*$ are recognisable.
   (a) $\{a^{2m}b^{2n} : m \geq 0, n \geq 0\}$,
   (b) $\{a^m ba^{3n} : m \geq 0, n \geq 0\}$,
   (c) $\{w \in \{a, b\}^* : |w|_a \leq 2 \text{ or } |w|_b = 1\}$.

5. Prove that $(L^*K^*)^* = (L \cup K)^*$.
   Hint: you may assume that $U^* \subseteq V^*$ for any languages U, V with $U \subseteq V$, that if $U_i \subseteq V_i$ for $i = 1, 2$, then $U_1U_2 \subseteq V_1V_2$, and results of Exercises 1.

6. Consider the alphabet $\{a, b\}$. Show that the language $(ab)^*$ can be expressed in terms of finite languages, Boolean operations and product (we will later call such languages 'star-free').

Section 6: Reduced DFAs

1. Recall that if $\mathscr{A} = (A, Q, \delta, q_0, F)$ and $\mathscr{B} = (A, P, \sigma, p_0, T)$ are DFAs, then $\mathscr{A}$ is *isomorphic* to $\mathscr{B}$ if there exists a bijection $\theta : Q \to P$ such that $q_0\theta = p_0$, $F\theta = T$ and

$$\delta(q, a)\theta = \sigma(q\theta, a) \qquad \forall\, q \in Q, a \in A.$$

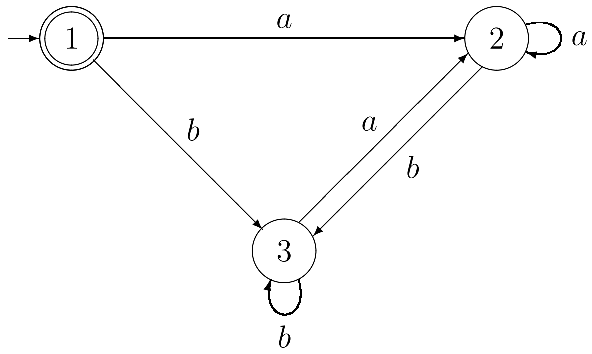
   Show that, if θ is as above, then for any $(q, w) \in Q \times A^*$ we have

$$\delta(q, w)\theta = \sigma(q\theta, w).$$

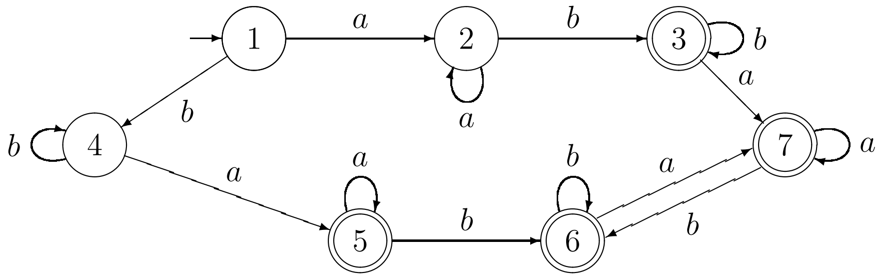
2. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA. Indicate how you would show that $L(\mathscr{A}) = L(\mathscr{B})$ for an *accessible* DFA $\mathscr{B}$.

3. For each of the following DFAs $\mathscr{A}$, calculate a sequence $\sim_0, \sim_1, \sim_2, \ldots$ of equivalence relations on the set of states, explaining how $\sim_{n+1}$ is defined in terms of $\sim_n$. Hence find a reduced DFA $\mathscr{B}$ which recognises the same language as $\mathscr{A}$.

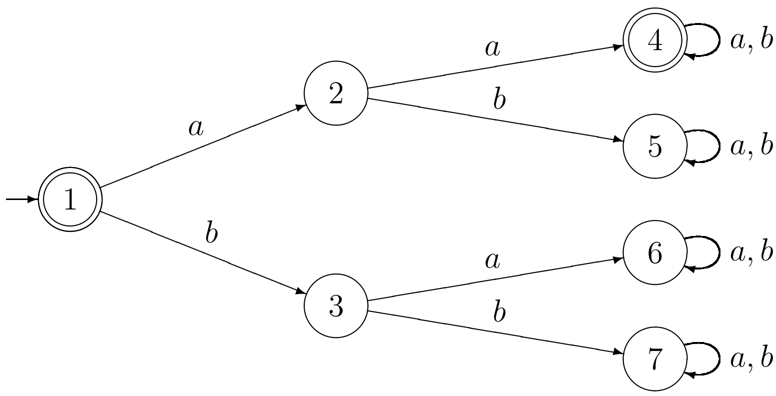
(a)



(b)



(c)



Aside: Some exercises on functions

The remaining questions are essentially a development of material you met concerning functions in Core Algebra. One difference: for a function $\theta : A \to B$ *and* $a \in A$ *we write* $a\theta$ *instead of* $\theta(a)$.

4. Let $\theta : A \to B$. For any $R \subseteq A$ and $S \subseteq B$ we define

$$R\theta = \{r\theta : r \in R\} \text{ and } S\theta^{-1} = \{a \in A : a\theta \in S\}.$$

This notation *does not* imply that the inverse function θ^{-1} exists. Now let $R_1, R_2 \subseteq A$ and let $S_1, S_2 \subseteq B$. We will show in Revision of Functions that

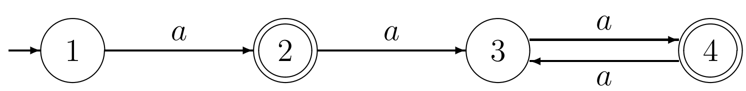
$$(S_1 \cup S_2)\theta^{-1} = S_1\theta^{-1} \cup S_2\theta^{-1}.$$

Prove the following:
(i) $(R_1 \cup R_2)\theta = R_1\theta \cup R_2\theta$;
(ii) $(R_1 \cap R_2)\theta \subseteq R_1\theta \cap R_2\theta$;
(iii) $(S_1 \cap S_2)\theta^{-1} = S_1\theta^{-1} \cap S_2\theta^{-1}$;
(iv) $S_1^c\theta^{-1} = (S_1\theta^{-1})^c$;
(v) $(S_1 \setminus S_2)\theta^{-1} = S_1\theta^{-1} \setminus S_2\theta^{-1}$ (hint: use (iii) and (iv)).
Find an example to show the inclusion in (ii) may be strict.

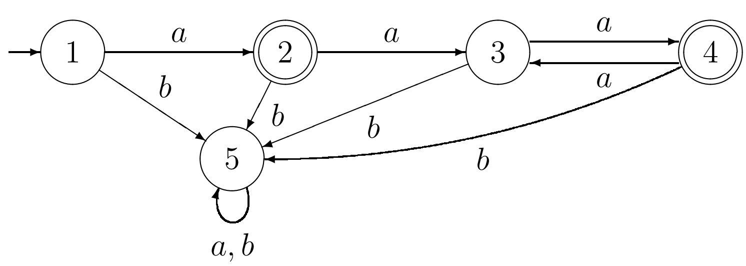
5. Let $\theta : X \to Y$ be a function from X to Y.
   (a) Prove that, if $L \subseteq X$, then $L \subseteq (L\theta)\theta^{-1}$. Find an example to show that the inclusion may be strict.
   (b) Prove that, if $K \subseteq Y$, then $(K\theta^{-1})\theta \subseteq K$. Find an example to show that the inclusion may be strict.
   (c) Prove that for $L \subseteq X$, we have $L = (L\theta)\theta^{-1}$ if and only if $L = P\theta^{-1}$ for some $P \subseteq Y$.
   The idea that $L = (L\theta)\theta^{-1}$ *is an important one at the end of the module. Please keep thinking about it (draw pictures!) until you can see what it is saying.*

Section 7: Monoids and transition monoids

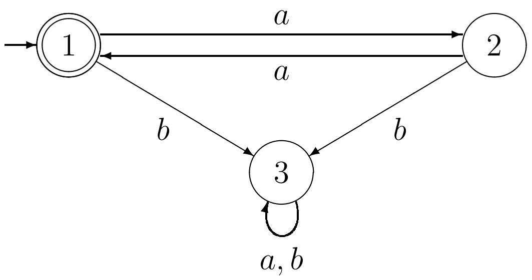
1. Calculate $M(\mathscr{A})$ for the following DFA:



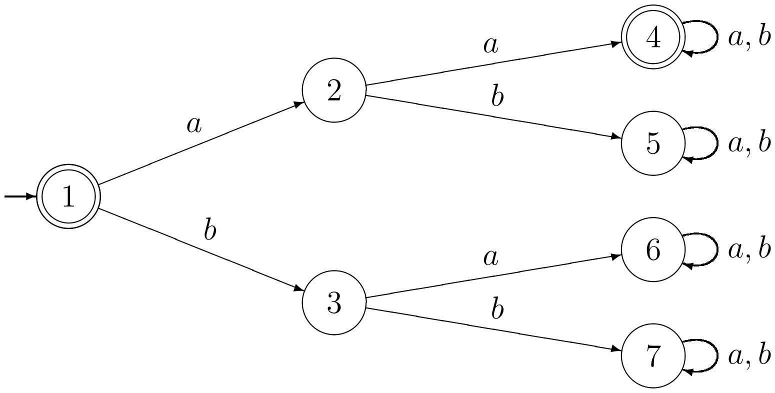
(it has four elements).
Now calculate $M(\mathscr{B})$ for the following DFA:



2. Find the transition monoids of the DFAs given below:



(a)



(b)

3. (a) Show that a submonoid of a finite group is a subgroup.
   (b) Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA. Show that $M(\mathscr{A})$ is a subgroup of $\mathcal{S}_Q$, the symmetric group on Q, if and only if each σ_a is a bijection.

4. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ and $\mathscr{B} = (A, P, \tau, p_0, T)$ be DFAs and suppose that they are isomorphic via $\theta : Q \to P$. Denote the elements of $M(\mathscr{A})$ and $M(\mathscr{B})$ by $\sigma_w^{\mathscr{A}}$ and $\sigma_w^{\mathscr{B}}$, respectively. Show that

$$\psi : M(\mathscr{A}) \to M(\mathscr{B})$$

given by

$$\sigma_w^{\mathscr{A}}\psi = \sigma_w^{\mathscr{B}}$$

is an isomorphism.

5. (a) An equivalence relation ρ on a monoid M is a *congruence* if

$$a\,\rho\,b, c\,\rho\,d \text{ implies that } ac\,\rho\,bd.$$

A relation ρ on a monoid M is *left (right) compatible* if

$$a\,\rho\,b \Rightarrow ca\,\rho\,cb\,(ac\,\rho\,bc)$$

for all $a, b, c \in S$. A left (right) compatible equivalence relation is called a *left (right) congruence.*

Show that a relation ρ on a monoid S is a congruence if and only if it is a left congruence and a right congruence.

(*b*) Let $M/\rho = \{[m] : m \in M\}$. Show that M/ρ is a monoid with identity $[1]$ under $[m][n] = [mn]$.

Section 8: The syntactic monoid of a language

1. Let X be a set, let Y be a subset of X and let ρ be an equivalence relation on X. Note that Y is a union of ρ-classes if and only if $x \in Y$, $x \,\rho\, y$ implies that $y \in Y$.

   We show in lectures that if $L \subseteq A^*$, then L is a union of $\sim_L$-classes. Now show that if ρ is a congruence on A^* such that L is a union of ρ-classes, then $u \,\rho\, v$ implies that $u \sim_L v$.

2. Let $A = \{a, b\}$ and $L = \{a^2, b^2\}$. Calculate the syntactic monoid $M(L)$ of L, giving the elements and the multiplication table.

3. Let $A = \{a, b\}$ and $L = aA^*a$. Calculate the syntactic monoid $M(L)$ of L, giving the elements and the multiplication table.

4. Suppose that L is a language over A, ρ is a congruence on A^* and L is a union of ρ-classes. Suppose also that A^*/ρ is finite. Show that $L \in \operatorname{Rec} A^*$.

Section 9: Recognition by a monoid

1. Let M be the monoid given by the following multiplication table.

	1	m	p
1	1	m	p
m	m	m	p
p	p	m	p

   Let $A = \{a, b\}$ and define a monoid homomorphism $\theta : A^* \to M$ by $a\theta = m$ and $b\theta = p$. By using this homomorphism, show that the languages L and $L \cup \{\varepsilon\}$ are recognised by M where $L = A^*b$.

2. Let $A = \{a\}$ and let $M = \{1, x, x^2\}$ where $x^3 = 1$ be the three element cyclic group. Let $\theta : A^* \to M$ be the homomorphism determined by $a\theta = x$. (So $\varepsilon\theta = 1$, $a^2\theta = (a\theta)(a\theta) = x^2$, $a^3\theta = (a^2\theta)(a\theta) = 1$, $a^4\theta = (a^3\theta)(a\theta) = x$, etc.) For which of the following sets L do we have $L = (L\theta)\theta^{-1}$? *Recall that this is equivalent to $L = P\theta^{-1}$ for some $P \subseteq M$.*

   (*a*) $L = \{a^k : k \geqslant 4\}$,
   (*b*) $L = \{a^n : n \geqslant 0 \text{ and } 3 \nmid n\}$,

(c) $L = \{a^n : n \geqslant 0 \text{ and } n \equiv 2 (\text{mod } 3)\}$,
(d) $L = \{a^4, a^6, a^8, \dots\}$.

3. Let $K, L \subseteq A^*$. Define LK^{-1} by

$$LK^{-1} = \{v \in A^* : \exists u \in K \text{ such that } vu \in L\}.$$

Suppose that L is recognised by the monoid M. Prove that LK^{-1} is also recognised by M. (Hint: there is a monoid homomorphism $\theta : A^* \to M$ such that $L = (L\theta)\theta^{-1}$; show that $((LK^{-1})\theta)\theta^{-1} = LK^{-1}$.)

4. Let A be a finite alphabet and L, K be subsets of A^*. Put

$$P = \{w \in A^* : uw^2v \in L \text{ for some } u, v \in K\}.$$

Show that if L is recognised by the monoid M, then P is also recognised by M.

5. Let $\mathscr{A} = (A, Q, \delta, q_0, F)$ be a DFA (assumed to be accessible) and let $\overline{\mathscr{A}} = (A, \overline{Q}, \overline{\delta}, \overline{q_0}, \overline{F})$ be the reduced DFA obtained from $\mathscr{A}$ in the usual way. For $w \in A^*$, let $\sigma_w : Q \to Q$ and $\tau_w : \overline{Q} \to \overline{Q}$ be given by $q\sigma_w = \delta(q, w)$ and $[q]\tau_w = \overline{\delta}([q], w)$ respectively so that $M(\mathscr{A}) = \{\sigma_w : w \in A^*\}$ and $M(\overline{\mathscr{A}}) = \{\tau_w : w \in A^*\}$. Show that $\theta : M(\mathscr{A}) \to M(\overline{\mathscr{A}})$ defined by $\sigma_w\theta = \tau_w$ is well defined and a monoid homomorphism.

6. Let $L \subseteq A^*$ be a language recognised by a monoid M via a morphism $\theta : A^* \to M$ such that θ is onto. Show that there exists a monoid morphism $\psi : M \to M(L)$.

Section 10: Schützenberger's Theorem

There are no specific exercises for Section 10. The notes and videos themselves contain a number of worked examples which illustrate the concepts of the section and revise earlier work.