Alphabets and Words

We are going to be interested in the relationships:

Machines $\longleftrightarrow$ Languages $\leftrightarrow$ Algebra.

In particular, we will focus on:

Automata $\longleftrightarrow$ Regular Languages $\leftrightarrow$ Monoids.

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

We define $A^+ = \bigcup_{i\geq 1} A^i$ to be the set of all non-empty words over A, and define $A^* = A^+ \cup \{\lambda\}$ where λ is the empty string.

A language over A is a subset of A^*. and language L is finite iff $|L| < \infty$ and cofinite iff $|L^c| = |A^* \setminus L| < \infty$. All the string and language operations we know from MFCS carry over.

A^* is a monoid with identity λ, called the free monoid on A.

Automata

Recall from MFCS that a FSA is a 5-tuple:

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

where transition function $\delta : Q \times A \to Q$ can be extended in the obvious way to give $\delta : Q \times A^* \to Q$.

The language recognised by $\mathcal{A}$ is:

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

A language $L \subseteq A^*$ is recognisable iff there exists a FSA $\mathcal{A}$ s.t. $L = L(\mathcal{A})$, and we write $L \in \mathrm{Rec}\, A^*$.

We note that $A^* \in \mathrm{Rec}\, A^*$ and all singleton languages lie in $\mathrm{Rec}\, A^*$.

Lemmas

$$\boxed{L \in Rec\, A^* \Rightarrow L^c \in Rec\, A^*}$$

Proof:

Let $\mathcal{A}^c = (A, Q, \delta, q_0, F^c)$. Then:

$$\begin{aligned} w \in L(\mathcal{A}^c) &\text{ iff } \delta(q_0, w) \in F^c \\ &\text{ iff } \delta(q_0, w) \notin F \\ &\text{ iff } w \notin L(\mathcal{A}) \\ &\text{ iff } w \in L^c. \end{aligned}$$

□

$$\boxed{L, K \in Rec\, A^* \Rightarrow L \cup K \in Rec\, A^*}$$

Proof:

From MFCS, adding non-determinism to FSAs can be done wlog, and without increasing power. So, we can take the union of the states, transition relations, initial states, and final states. Then:

$$\begin{aligned} w \in L \cup K &\text{ iff } w \in L \text{ or } w \in K \\ &\text{ iff path } q_0 \xRightarrow{w} q \text{ or } p_0 \xRightarrow{w} p \\ &\quad \text{for } q_0 \in I_A, q \in F_A, p_0 \in I_B, p \in F_B \\ &\text{ iff path } r_0 \xRightarrow{w} r \text{ for } r_0 \in I, r \in F \\ &\quad \text{since } Q \cap P = \emptyset \\ &\text{ iff } w \in L. \end{aligned}$$

□

More Lemmas

$$\boxed{L, K \in \mathrm{Rec}\, A^* \Rightarrow L \cap K \in \mathrm{Rec}\, A^*.}$$

Proof:

Clearly $L \cap K = (L^c \cap K^c)^c$.

By our previous results, L^c and K^c are in $\mathrm{Rec}\, A^*$, and so is $L^c \cap K^c$, and so is $(L^c \cap K^c)^c$, and we are done. $\square$

$$\boxed{L, K \in \mathrm{Rec}\, A^* \Rightarrow L \setminus K \in \mathrm{Rec}\, A^*.}$$

Proof:

Clearly $L \setminus K = L \cap K^c$.

By our previous results, $K^c \in \mathrm{Rec}\, A^*$, and then so is $L \cap K^c$. $\square$

Remarks

We remark that Rec A^* is not closed under infinite union or intersection.

For example, consider the language:

$$L_i = \{a^i b^i\}.$$

Taking the infinite union:

$$L = \bigcup_{i\geq 1} L_i = \{a^n b^n \mid n \geq 1\},$$

but we know by the pumping lemma, that L is actually context-free.

We can see with finitely many applications, that:

$$L \text{ finite} \Rightarrow L \in \text{Rec } A^*$$
$$L \text{ cofinite} \Rightarrow L \in \text{Rec } A^*.$$

If L finite, then $L = \emptyset$ or $L = \{w_1, \ldots, w_i\}$, $w_i \in A^*$. We know $\emptyset, w_i \in \text{Rec } A^*$, therefore:

$$L = \{w_1\} \cup \{w_2\} \cup \cdots \cup \{w_n\}$$

is recognisable. Similarly, L cofinite $\Rightarrow$ L^c finite $\Rightarrow L^c \in \text{Rec } A$. But, since $L = (L^c)^c$, then L is recognisable too.

Additional Results

We provide two more results, without proof.

$$\boxed{L, K \in \mathrm{Rec}\, A^* \Rightarrow LK \in \mathrm{Rec}\, A^*}$$

$$\boxed{L \in \mathrm{Rec}\, A^* \Rightarrow L^* \in \mathrm{Rec}\, A^*}$$

Rational Operations

The rational operations on languages over A are union ($L, K \mapsto L \cup K$), product ($L, K \mapsto LK$), and star ($L \mapsto L^*$).

$L \subseteq A^*$ is <u>rational</u> iff L is finite or L can be obtained by applying rational operations a finite number of times. $\mathrm{Rat}\, A^*$ is the set of rational languages over A.

$$\boxed{\mathrm{Rat}\, A^* \subseteq \mathrm{Rec}\, A^*}$$

Kleene's Theorem

$$\boxed{\text{Rat } A^* = \text{Rec } A^*}$$

Proof:

We already know that Rat $A^* \subseteq$ Rec A^*.

It is possible to show by induction on the size of the transition relation of some NDFA accepting $L \in$ Rec A^* that Rat $A^* \supseteq$ Rec A^*, however, we will skip over this to save time.

Rational Expressions

A rational expression for a language L over A is one that expresses L using only finite languages and the rational operations a finite number of times.

Returning to Monoids

Recall that a <u>monoid</u> is a non-empty set M, together with an associative binary operation, and equipped with a two-sided identity.

Let M be a monoid, and $T \subseteq M$.

Then, T is a <u>submonoid</u> iff:

(1) $1 \in T$,
(2) $a, b \in T \Rightarrow ab \in T$,

and we write $T \leq M$.

Let M be a monoid, and $X \subseteq M$. Then:

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

Notice that $1 \in \langle X \rangle$, and $\langle X \rangle$ is closed under multiplication, so is a submonoid.

We say that $\langle X \rangle$ is the submonoid of M generated by X.

For example:

(1) $\mathbb{N} = \langle P \rangle$ where P is the set of primes

(2) $A^* = \langle A \rangle$.

Transformation Monoids

If X is some non-empty set, then:

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

is a monoid under functional composition with identity I_X, and is called the "full transformation monoid on X".

From now onwards, we will be using postfix notation for functional application, and if $X = \{1, 2, \dots, n\}$, we write $\mathcal{T}_n$ for $\mathcal{T}_X$ and I_n for I_X.

It is also convenient to adopt the "two-row" notation for elements of $\mathcal{T}_n$.

For example, if $\alpha \in \mathcal{T}_4$ is given by:

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

then we can write:

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

Finally, we note that $|\mathcal{T}_n| = n^n$.

The new Notation

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

With our old notation, we have:
$$(\alpha \circ \beta)(n) = \alpha(\beta(n))$$

so
$$\begin{aligned} 1 &\mapsto 2 \mapsto 1 \\ 2 &\mapsto 1 \mapsto 1 \\ 3 &\mapsto 3 \mapsto 2 \\ 4 &\mapsto 3 \mapsto 2. \end{aligned}$$

With our new notation, we have:
$$n\beta\alpha = n\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 2 \end{pmatrix}.$$

Similarly $\underset{\longleftarrow}{\alpha \circ \beta \circ \gamma} \equiv \underset{\longrightarrow}{\gamma\beta\alpha}$.

Constant Functions

For any $x \in X$, $c_x : X \to X$ is given by:

$$y c_x = x$$

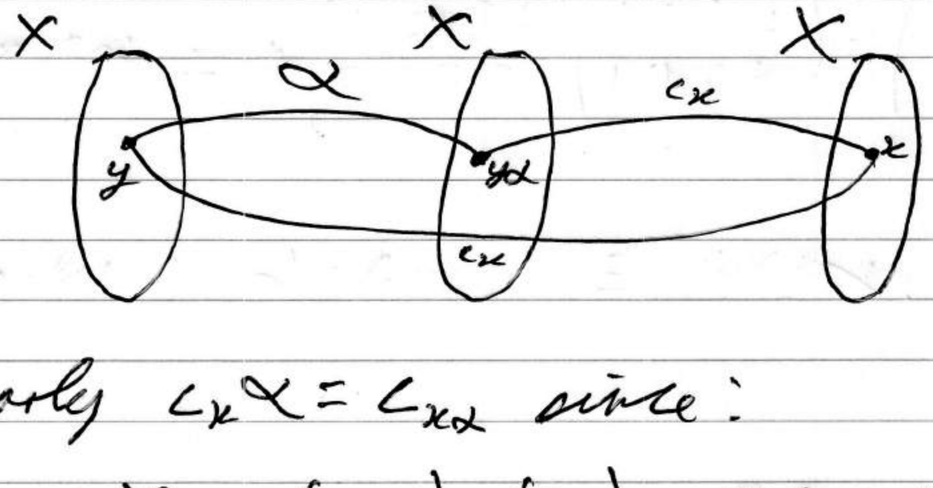
for $y \in X$, and is called the "constant function on x".

For example:

$$c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{pmatrix} \in T_4.$$

Note that $\alpha c_x = c_x$ for all $\alpha \in T_X$, since:

$$\forall y \in X, \; y(\alpha c_x) = (y\alpha) c_x = x = y c_x.$$



Similarly $c_x \alpha = c_{x\alpha}$ since:

$$\forall y \in X, \; y(c_x\alpha) = (yc_x)\alpha = x\alpha = y c_{x\alpha}.$$

Lemma

$\boxed{\begin{array}{l}\text{Let } \mathcal{A} = (A, Q, \delta, q_0, F) \text{ be a FSA.} \\ \text{For each } w \in A^*\text{, let } \sigma_w \in T_Q \text{ be defined by:} \\ \qquad q\sigma_w = \delta(q, w). \\ \text{We claim that for all } w, v \in A^*\text{:} \\ \qquad \sigma_w \sigma_v = \sigma_{wv}.\end{array}}$

Proof:

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

thus $\sigma_w \sigma_v = \sigma_{wv}$. $\square$

We note that:

$$q\sigma_\lambda = \delta(q, \lambda) = q = q I_Q,$$

so we have submonoid:

$$M(\mathcal{A}) = \{\sigma_w \mid w \in A^*\} \leq T_Q.$$

Transition Monoid

In fact, we call:

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

the transition monoid of FSA A.

Lemma

$$\boxed{M(A) = \langle \sigma_a \mid a \in A \rangle \text{ and is finite.}}$$

Proof:

Let $w = a_1 a_2 \cdots a_n \in A^*$ where $a_i \in A$.

Then:

$$\sigma_w = \sigma_{a_1 a_2 \cdots a_n} = \sigma_{a_1} \sigma_{a_2} \cdots \sigma_{a_n}$$

by recursive application of our previous result.

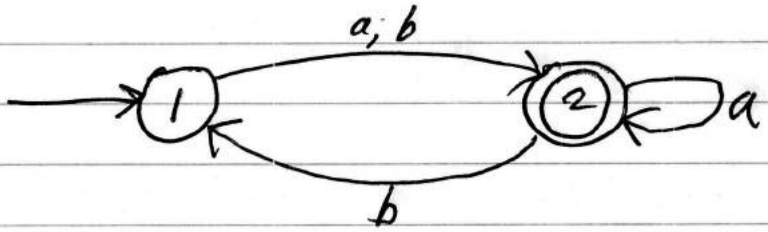
It is easy to see that $M(A)$ is finite:

$$|M(A)| \leq |T_Q| = |Q|^{|Q|} < \infty$$

since $M(A) \leq T_Q$ and $|Q| < \infty$. $\square$

Example 1

Let $A = \{a, b\}$ and $Q = \{1, 2\}$.



Then:

	1	2
σ_a	2	2
σ_b	2	1

We now calculate all products until we don't obtain any new elements:

$$\sigma_a = c_2$$

$$\sigma_{a^2} = \sigma_a \sigma_a = c_2 c_2 = c_2 \left(= \sigma_b \sigma_a = \alpha \sigma_a\right)$$

$$\sigma_{b^2} = \sigma_b \sigma_b = I_Q$$

$$\sigma_a \sigma_b = c_2 \sigma_b = c_1.$$

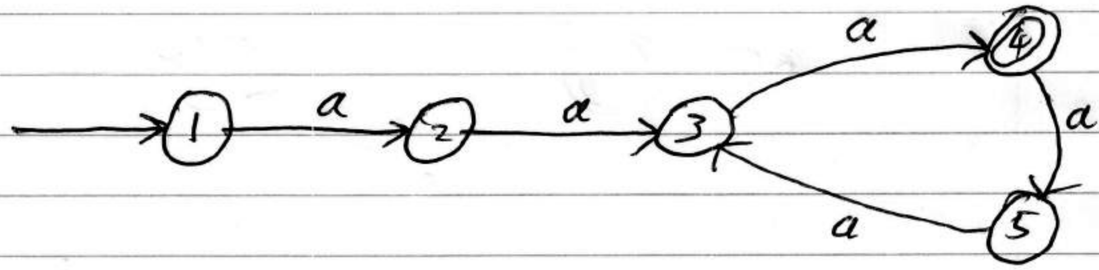
So, $M(A) = \{I_Q, \sigma_b, c_2, c_1\}$ with:

	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 2

Let $A = \{a\}$, $Q = \{1,2,3,4,5\}$.



We have $M(A) = \langle \sigma_a \rangle$, but we know this must be finite, so, we can calculate powers until we get a repeat.

N.B. $\sigma_{a^n} = \sigma_a^{\,n}$.

	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

the same

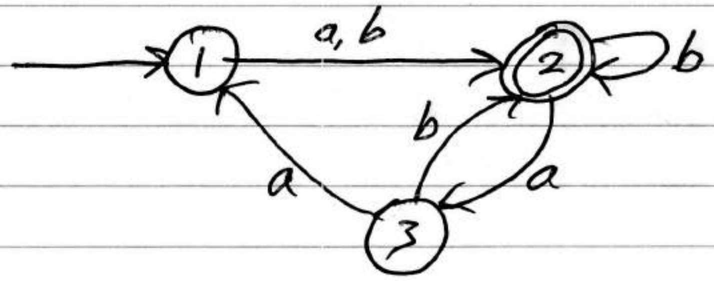
So $M(A) = \{I, \sigma_a, \sigma_a^2, \sigma_a^3, \sigma_a^4\}$ with:

	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

N.B. $\{\sigma_a^2, \sigma_a^3, \sigma_a^4\} \leq M(A)$.

Example 3

Let $A = \{a, b\}$, $Q = \{1, 2, 3\}$.



Then:

	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

where $\sigma_b = c_2$, $\sigma_b\sigma_a = c_3$, $\sigma_b\sigma_a^2 = c_1$.

So, $M(\mathcal{A}) = \{I, \sigma_a, \sigma_a^2, c_1, c_2, c_3\}$ with:

	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

N.B. $\{I, \sigma_a, \sigma_a^2\} \leq M(\mathcal{A})$.