(3)

Syntactic Congruence

Let L be a language over A.

For $u \in A^*$, we define the <u>content</u> of u:

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

We define the <u>syntactic congruence</u> of L:

$$u \sim_L v \text{ iff } C_L(u) = C_L(v).$$

Clearly $\sim_L$ is an equivalence on A^*,

Suppose that $u \sim_L v$ and $u' \sim_L v'$, then $uu' \sim_L vv'$.

Proof:

$$\begin{aligned}
(w, z) \in C_L(uu') &\Leftrightarrow wuu'z \in L \\
&\Leftrightarrow (w, u'z) \in C_L(u) \\
&\Leftrightarrow (w, u'z) \in C_L(v) \\
&\Leftrightarrow wvu'z \in L \\
&\Leftrightarrow (wv, z) \in C_L(u') \\
&\Leftrightarrow (wv, z) \in C_L(v') \\
&\Leftrightarrow wvv'z \in L \\
&\Leftrightarrow (w, z) \in C_L(vv')
\end{aligned}$$

and so $C_L(uu') = C_L(vv') \Leftrightarrow uu' \sim vv'$.

□

Syntactic Monoid

We define the <u>syntactic monoid</u> of L:

$$M(L) = \{ [w] \mid w \in A^* \}$$

and define a product on $M(L)$ by:

$$[u][u'] = [uu'].$$

> This product is a well defined binary operation on $M(L)$, and $M(L)$ is a monoid under it.

Proof:

If $[u]=[v]$ and $[u']=[v']$, then $u \sim_L v$ and $u' \sim_L v'$, so by the previous lemma $uu' \sim_L vv'$, so $[uu']=[vv']$, and our product is a well defined operation on $M(L)$.

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

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

so we have associativity, and identity $[\lambda]$:

$$[\lambda][u] = [\lambda u] = [u] = [u\lambda] = [u][\lambda],$$

thus $M(L)$ is a monoid. $\square$

Example 1

Let $A = \{a, b\}$ and $L = A$.

Then, for $w \in A^*$ with $|w| > 1$, we have:

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

$$C_L(\lambda) = \{(\lambda, a), (a, \lambda), (\lambda, b), (b, \lambda)\},$$

$$C_L(a) = \{(\lambda, \lambda)\} = C_L(b).$$

So, there are three $\sim_L$-classes:

$$[\lambda] = \{\lambda\} = 1,$$

$$[a] = \{a, b\} = L,$$

$$[a^2] = \{w \in A^* \mid |w| > 1\} = T.$$

So, the multiplication table of our monoid is:

	1	L	T
1	1	L	T
L	L	T	T
T	T	T	T

because we have:

$$LL = [a^2] = T, \quad LT = [a^3] = T \ (= TL).$$

N.B. $T = 0$

Remarks

If $u \in L$ and $u \sim_L v$, then $v \in L$.

We can see this since:

$$(\lambda, \lambda) \in c_L(u),$$

and so:

$$v = \lambda v \lambda \Rightarrow v \in L.$$

Therefore, L is a union of $\sim_L$-classes.

Example 2

Let $A = \{a, b\}$ and $L = \{ba, ab\}$.

Now, the contexts are:

$$c_L(\lambda) = \{(\lambda, ba), (b, a), (ba, \lambda), (\lambda, ab), (a, b), (ab, \lambda)\},$$

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

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

$$c_L(ba) = \{(\lambda, \lambda)\} = c_L(ab),$$

$$c_L(a^2) = \emptyset = c_L(b^2).$$

Example 2 (continued)

In fact, $C_L(w) = \emptyset$ for all $|w| \geq 3$.

So, there are 5 $\sim_L$-classes:

$$[\lambda] = \{\lambda\} = 1,$$

$$[a] = \{a\} = P,$$

$$[b] = \{b\} = Q,$$

$$[ab] = \{ab, ba\} = L,$$

$$[a^2] = \{a^2, b^2, w \mid |w| \geq 3\} = 0.$$

Thus, the multiplication table is:

	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

because we have:

$$P^2 = [a^2] = 0, \quad PQ = L, \text{ etc.}$$

Monoid Morphisms

Let M, N be monoids with identities 1_M and 1_N. Then a map:

$$\theta : M \to N$$

is a <u>monoid morphism</u> iff:

(1) $(ab)\theta = a\theta\, b\theta$

(2) $1_M\theta = 1_N$.

Example

Let $\theta : A^* \to \mathbb{N}^\circ$ be $w\theta = |w|$.

Then $\lambda\theta = |\lambda| = 0$, and for all $v, w \in A^*$:

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

Thus θ is a monoid morphism.

Free Monoids

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 any $a \in A$.

Proof:

Define $\theta: A^* \to M$ by $\lambda\theta = 1$ and:

$$(a_1 a_2 \cdots a_n)\theta = a_1\varphi\, a_2\varphi \cdots a_n\varphi$$

for $a_i \in A$. Clearly θ is well defined, and is a monoid morphism.

Thus, by definition, for any $a \in A$, we have $a\theta = a\varphi$.

It remains to show uniqueness. Suppose that ψ is a morphism such that $a\psi = a\varphi$ for all $a \in A$.

Then, clearly $\lambda\psi = 1 = \lambda\varphi$.

PTO →

Free Monoids (continued)

Now for:

$$w = a_1 a_2 \cdots a_n$$

where $a_i \in A$ and $n \geq 1$, we have:

$$w\psi = (a_1 \cdots a_n) = a_1\psi \cdots a_n\psi$$

$$= a_1\psi \cdots a_n\psi$$

$$= (a_1 \cdots a_n)\theta$$

$$= w\theta.$$

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

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

More generally, any monoid is called free if it is isomorphic to A^* for some set A. For example $(\mathbb{N}, +)$ is a free monoid.

Recognision by Monoid

Let $L \subseteq A^*$ and M be a monoid.

Then L is recognised by M iff there exists a morphism:

$$\theta : A^* \to M$$

such that:

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

We note that $L = (L\theta)\theta^{-1}$ is equivalent to $L = P\theta^{-1}$ for some $P \subseteq M$, and that we always have $L \subseteq (L\theta)\theta^{-1}$.

Let L be a language over A, and recall that:

$$M(L) = \{[w] \mid w \in A^*\}$$

is the syntactic monoid of L.

Then, L is recognised by $M(L)$.

Proof

Define $\nu_L : A^* \to M(L)$ by $w\nu_L = [w]$.

Then $\lambda \nu_L = [\lambda]$ and $(w\nu)\nu_L = [w\nu] = [w][\nu] = w\nu_L \nu\nu_L$, so ν_L is a morphism.

We know that $L \subseteq (L\nu_L)\nu_L^{-1}$, but it remains to show the reverse inclusion.

Suppose that $w \in (L\nu_L)\nu_L^{-1}$.

Then $w\nu_L \in L\nu_L$, so $w\nu_L = v\nu_L$ for some $v \in L$.

By the definition of ν_L, we thus have $[w] = [v]$, and so $w \sim_L v$.

As $(\lambda, \lambda) \in C_L(v)$, we must have $(\lambda, \lambda) \in C_L(w)$, so that $w \in L$.

Hence, $L \supseteq (L\nu_L)\nu_L^{-1}$ too, and L is recognised by $M(L)$. □

Theorem

The following are equivalent for a language L over A:

(1) $M(L)$ is finite,

(2) L is recognised by a finite monoid,

(3) $L \in \mathrm{Rec}\, A^*$.

Proof (1) $\Rightarrow$ (2):

Clearly this is true by our last result. □

Proof (2) $\Rightarrow$ (3):

Let M be a finite monoid and $\theta : A^* \to M$ a morphism such that $L = (L\theta)\theta^{-1}$.

Let $\mathcal{A} = (A, M, \delta, 1, L\theta)$ where:

$$\delta(m, a) = m(a\theta).$$

It's easy to see that for all $w \in A^*$:

$$\delta(m, w) = m(w\theta).$$

PTO →

Theorem (continued)

Then:

$$w \in L(A) \iff \delta(1, w) \in L\theta$$
$$\iff 1(w\theta) \in L\theta$$
$$\iff w\theta \in L\theta$$
$$\iff w \in (L\theta)\theta^{-1}.$$

But, we know that $L = (L\theta)\theta^{-1}$, so $w \in L$, and L is recognised by A, so $L \in \mathrm{Rec}\, A^*$. □

Proof (3) $\Rightarrow$ (1):

Recall from MFCS that there exists a unique minimal automaton $\bar{A}$ such that $L(\bar{A}) = L(A)$ for any FSA A.

We claim that for $u, v \in A^*$, $u \sim_{M(L)} v \iff \sigma_u = \sigma_v$, for which the proof is omitted due to lack of time.

So, the number of $\sim_L$-classes, $|M(L)|$, is equal to the number of distinct σ_u, which we know is $|M(\bar{A})|$.

But $M(\bar{A}) \subseteq T_Q$, and $|T_Q| < \infty$, so

$$|M(\bar{A})| \leq |T_Q| < \infty,$$

so $M(\bar{A})$ is finite and so is $M(L)$. □

Corollary

Let $L = L(A)$ for minimal FSA A.
Then $M(L) \cong M(A)$.

Proof:

From our theorem, $\theta : M(L) \to M(A)$ is a bijection, given by:

$$[u]\theta = \sigma_u.$$

Let $[u], [v] \in M(L)$. Then:

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

and since $1_{M(L)} = [\lambda]$, we have:

$$[\lambda]\theta = \sigma_\lambda = I_Q = 1_{M(A)}.$$

Therefore θ is an isomorphism of monoids, and $M(L) \cong M(A)$.

Example

We can use monoids to show closure properties under Boolean operations, by which I mean $\cup, \cap, ^c$.

$$L, K \in Rec\ A^* \Rightarrow L \cap K \in Rec\ A^*$$

Proof:

There exists finite monoids M, N and morphisms $\theta : A^* \to M$, $\psi : A^* \to N$ s.t.:

$$L = (L\theta)\theta^{-1} \qquad K = (K\psi)\psi^{-1}.$$

It is easy to see that $M \times N$ is a finite monoid, and that $\varphi : A^* \to M \times N$ defined by $w\varphi = (w\theta, w\psi)$ is a morphism.

Let $X = ((L \cap K)\varphi)\varphi^{-1}$. We know that $L \cap K \subseteq X$. Now, let $w \in X$, so $w\varphi \in (L \cap K)\varphi$, so $w\varphi = u\varphi$. Hence, $(w\theta, w\psi) = (u\theta, u\psi)$ and $w\theta = u\theta$, $w\psi = u\psi$.

As $u \in L$, $w \in (L\theta)\theta^{-1} = L$, and as $u \in K$, $w \in (K\psi)\psi^{-1} = K$. Thus $w \in L \cap K$, and $X \subseteq L \cap K$, so $L \cap K = X$, and $L \cap K$ is recognisable by $M \times N$.

Hence, $L \cap K \in Rec\ A^*$.

Star-Free Languages

$L \subseteq A^*$ is <u>star-free</u> iff it is finite or can be obtained by applying Boolean operations a finite number of times.

> If X is the set of all star-free languages over A, then $X \subset Rat\ A^*$.

Examples

All finite languages are star-free, such as $\{ab, a, bab\}$, $\emptyset$, $\{\lambda\}$.

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

Actually, A^* is star-free, since $A^* = \emptyset^c$.

Finally:

$$L = \{x \in A^* \mid |x|_a \geq 1\} = A^* a A^* = \emptyset^c a \emptyset^c$$

is star-free.

Subgroups

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

Then, G is a <u>subgroup</u> of M iff:

(1) $a, b \in G \Rightarrow ab \in G$,

(2) $\exists e \in G, \forall a \in G, ea = a = ae$,

(3) $\forall a \in G, \exists b \in G, ab = e = ba$.

Let $E(M)$ be the set of idempotent elements. Then $e \in E(M) \Rightarrow \{e\}$ is a subgroup of M, a <u>trivial</u> subgroup.

S_n is a subgroup of T_n, and $GL_n(\mathbb{R})$ is a subgroup of $M_n(\mathbb{R})$.

Theorem

A language L is star-free iff:

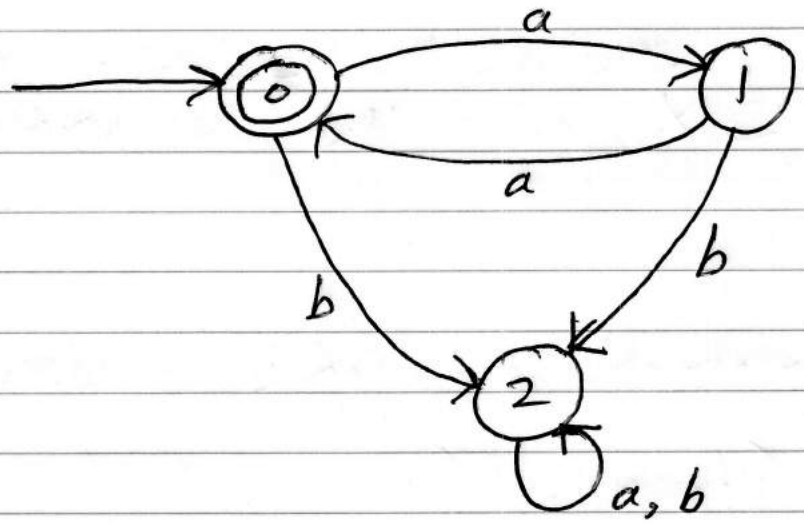
(1) $M(L)$ is finite,

(2) All subgroups of $M(L)$ are trivial.

Example

Is language $L = \{ a^{2n} \mid n \geq 0 \}$ over alphabet $A = \{a, b\}$ star-free?

We construct an FSA (minimal):



Since $M(A) \cong M(L)$, in order to compute the $\sim_L$-classes, we can compute the elements of $M(L)$ to give us an equivalent transition table:

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

where

$\sigma_b = c_2$

and

$c_2 \alpha = c_2 = \alpha c_2$.

So, $M(A) = \{ I, \sigma_a, c_2 \}$, but $H = \{ I, \sigma_a \}$ is a non-trivial subgroup, so by our theorem, L is not star-free.