Categories & Algebras 3

Automata and Monoids II

Graham Campbell

Summer 2017

Syntactic Congruence

Let L be a language over A.

Definition (Context)

For $u \in A^*$, we define the context of u:

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

Definition (Congruence)

We define the syntactic congruence of L:

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

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

Syntactic Monoid

Lemma

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

Definition (Syntactic monoid)

We define the syntactic monoid of L:

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

and define a product on $M(L)$ by $[u][u'] = [uu']$.

Lemma

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

Example 1

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

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

1. $C_L(w) = \emptyset$,
2. $C_L(\lambda) = \{(\lambda, a), (a, \lambda), (\lambda, b), (b, \lambda)\}$,
3. $C_L(a) = \{(\lambda, \lambda)\} = C_L(b)$.

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

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

Example 2

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

Then, the contexts are:

1. $C_L(\lambda) = \{(\lambda, ba), (b, a), (ba, \lambda), (\lambda, ab), (a, b), (ab, \lambda)\}$,
2. $C_L(a) = \{(b, \lambda), (\lambda, b)\}$,
3. $C_L(b) = \{(a, \lambda), (\lambda, a)\}$,
4. $C_L(ab) = \{(\lambda, \lambda)\} = C_L(ba)$,
5. $C_L(a^2) = \emptyset = C_L(b^2)$.

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

Monoid Morphisms

Definition

Let M, N be monoids. Then map $\theta : M \to N$ is a morphism iff:

1. $(ab)\theta = a\theta b\theta$,
2. $1_M\theta = 1_N$.

Example

Let $\theta : A^* \to \mathbb{N}^0$ 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

Theorem

Let A be an alphabet, M a monoid, and $\varphi : A \to M$ a function.

Them, there exists a unique morphism $\theta : A^* \to M$ s.t.

$$\forall a \in A, a\theta = a\varphi.$$

Thus, to define a morphism from A^* to any monoid, it is enough to simply 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 $\mathbb{N}^0$ is a free monoid.

Recognition by Monoid

Definition (Recognision)

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

Lemma

Let L be a language over A.

Then, L is recognised by $M(L) = \{[w] \mid w \in A^*\}$.

Regular Languages

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

We say such languages are regular.

Corollary

Let $L = L(\mathcal{A})$ for minimal FSA $\mathcal{A}$.

Then, $M(L) \cong M(\mathcal{A})$.

Applications

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

Lemma

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

We can define a new class of languages using these operations.

Definition (Star-Free)

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

Lemma

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

Subgroups

Definition (Subgroup)

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

Then, G is a subgroup of M iff:

1. $a, b \in G \Rightarrow ab \in G$,
2. $\exists e \in G, \forall a \in G, ea = ae$,
3. $\forall a \in G, \exists b \in G, ab = e = ba$.

Lemma

Let $E(M)$ denote the set of idempotent elements of monoid M.

Then, $e \in E(M) \Rightarrow \{e\}$ is a subgroup.

Schutzenberger's Theorem

Theorem

A language L is star-free iff:

1. *$M(L)$ is finite,*
2. *All subgroups of $M(L)$ are trivial.*

Example

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

Remark: In general, the problem of testing if an element behaves as an identity is actually undecidable! However, in the case of finite sets, we're fine. See the **Undecidable Problems** lecture.