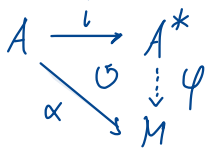
10.10.2019

Prop.: Σ alphabet, M submonoid of Σ^*, G min. gen. set of M (assumed finite)

M is free iff $\underbrace{g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_k \text{ for } g_i, h_j \in G \text{ implies } n=k \text{ and } g_i = h_i \ \forall i}_{(*)}$

Proof: ($\Leftarrow$) last week

($\Rightarrow$) Assume M is free, ... φ bijection in



Claim 1: For all $a \in A$, $\alpha(a) \in G$

By contradiction, assume $\exists a \in A$ s.t. $\varphi(a) \notin G$.

$\varphi(a) \in M$ (by definition), and G generates M. So $\exists k \geq 2$ and $g_1, \ldots, g_k \in G$ s.t.

$\varphi(a) = g_1 g_2 \cdots g_k$ ($k \neq 1$ since $\varphi(a) \notin G$ and $k \neq 0$ since $\varphi(\varepsilon) =$ neutral + φ bijection)

$a = \varphi^{-1}(g_1 g_2 \cdots g_k)$

$= \varphi^{-1}(g_1)\varphi^{-1}(g_2)\cdots\varphi^{-1}(g_k)$ (φ isomorphism)

Each $\varphi^{-1}(g_i) \neq \varepsilon$ (since $g_i \in G$, $g_i \neq \varepsilon$ and $\varphi(\varepsilon) = \varepsilon$ and φ is a bijection).

So, $|a| = 1$, $|\varphi^{-1}(g_1)\cdots\varphi^{-1}(g_k)| \geq 2$, a contradiction.

Claim 2: $\forall g \in G$, $\varphi^{-1}(g) \in A$

By contradiction, assume $\exists g \in G$ s.t. $\varphi^{-1}(g) \notin A$.

So, $\exists k \geq 2$, $a_1, \ldots, a_k \in A$ s.t. $\varphi^{-1}(g) = a_1 \cdots a_k$, i.e., $g = \varphi(a_1)\cdots\varphi(a_k)$

By claim 1, each $\varphi(a_i) \in G$. By assumption, each $\varphi(a_i) \neq g$.

Hence, $G \setminus \{g\}$ is generating M, contradicting the minimality of G.

Claim 3: α is a bijection between A and G

Recall that $\alpha(a) = \varphi(a)$ $\forall a \in A$.

From claim 1, $\alpha(A) \subseteq G$.

From claim 2, α is surjective.

Injectivity of α follows from that of $\varphi : A^* \longrightarrow M$.

Assume for $a, b \in A$, $\alpha(a) = \alpha(b)$. Then $\varphi(a) = \varphi(b)$, so $a = b$.

Proof that claim 3 implies (*):

Let $n, k \geq 0$, $g_1, g_2, \dots, g_n, h_1, h_2, \dots, h_k \in G$ be s.t. $g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_k$.

↳ preimage by φ, φ^{-1} morphism, $\varphi^{-1} = \alpha^{-1}$ (α is a bijection)

$\Rightarrow \alpha^{-1}(g_1) \cdots \alpha^{-1}(g_n) = \alpha^{-1}(h_1) \cdots \alpha^{-1}(h_k)$

This is an equality between words, each $\alpha^{-1}(g_i)$ or $\alpha^{-1}(h_j)$ being a letter.

So, $n = k$ and $\alpha^{-1}(g_i) = \alpha^{-1}(h_i)$ $\forall 1 \leq i \leq n$ and hence, $g_i = h_i$. This is (*). □

Prop.: A submonoid M of Σ^* is free exactly when $\forall w \in \Sigma^*$: $w \in M$ iff $\exists p, s \in M$ s.t. $pw \in M$ and $ws \in M$

Proof: See exercise sheet 1

4) The defect theorem

Lemma: Let X be a finite subset of Σ^*. There exists a (necessarily unique) smallest free submonoid of Σ^* which contains X.

Rmk.: It also contains X^* (since submonoids are stable by concatenation).

Rmk.: It is sometimes called the free hull of X.

Proof: Σ^* is a free submonoid of Σ^* containing X.

We show that intersections of free submonoids of Σ^* are free. This ensures that the intersection of all free submonoids of Σ^* containing X is defined and is the smallest such free submonoid.

Assume M_i is a free submonoid of Σ^* $\forall i$ in some index set I.

Let $M = \bigcap_{i \in I} M_i$.

M is a submonoid of Σ^* (since it is stable by concatenation).

We prove that M is free using the previous proposition.

- If $w \in M$, then $p = \varepsilon$, $s = \varepsilon \in M$ and so $pw \in M$ and $ws \in M$.
- Let $w \in \Sigma^*$. Assume $\exists p, s \in M$ s.t. $pw \in M$ and $ws \in M$.

  In each M_i, we have $p \in M_i$, $s \in M_i$, $pw \in M_i$, $ws \in M_i$.

  Because M_i is free, the previous prop. ensures that $w \in M_i$. This holds $\forall i \in I$, so $w \in M = \bigcap_{i \in I} M_i$. □

Thm.: (the defect theorem)

Let X be a finite subset of Σ^*. Assume that X is not a code ($\Leftrightarrow X^*$ is not free $\Leftrightarrow \exists$ a non-trivial relation betw. the elements of X)

Then $\exists$ a code $Y \subseteq \Sigma^*$ with strictly fewer elements than X s.t. $X \subseteq Y^*$.

More precisely, we can take Y as the set of generators of the unique smallest free submonoid of Σ^* containing X.

Proof:
- The said set Y is a code, by definition.
- Y generates a submonoid of Σ^* which contains X. In particular, $X \subseteq Y^*$.
- Main part of the proof is to show that $\text{card}(Y) < \text{card}(X)$.

  Wlog, we can assume $\varepsilon \notin X$.

  To prove $\text{card}(Y) < \text{card}(X)$, we show a mapping $\alpha : X \longrightarrow Y$, which is surjective but not injective.