CS F351: Theory of Computation **16 Sep, 2022**

8: More Closure Properties

Scribe: Piyush Mohite

More Closure Properties

0.1 Monoid

A tuple $(S, \cdot, e)$ is known as a *monoid*, if:

- S is a set.
- $\cdot$: is *associative*, i.e., $\forall u, v, w \in S, (w \cdot u) \cdot v = w \cdot (u \cdot v)$
- $e \in S$ is the identity element, i.e., $\forall w \in S, e \cdot w = w \cdot e = w$

Eg: $(\Sigma^{\star}, \cdot, e)$ is a monoid.
Eg: $(\mathbb{N}, +, 0)$ is a monoid. [Also commutative.]
Eg: $(\{e, a\}, \cdot, e)$ is *NOT* a monoid. [Because, if we consider $'a'$ and $'a'$, we get the concatenation $a \cdot a = aa$, which is not a part of the set $\{e, a\}$, since it has to be $SxS \rightarrow S$.]

Specification: (trying to describe what is required in words)

$$\exists x \exists y.(x < y \wedge R_a(x) \wedge R_b(y))$$

$R_a(x)$**:** Tells us that at the position $'x'$ in the word, we have the letter $'a'$.
$R_b(y)$**:** Tells us that at the position $'y'$ in the word, we have the letter $'b'$.

0.2 Homomorphism

A function $h : S_1 \rightarrow S_2$ is called a (monoid) homomorphism from $(S_1, \cdot_1, e_1)$ to $(S_1, \cdot_1, e_1)$, if:

- $h(e_1) = e_2$.
- $\forall u, v \in S_1, h(u \cdot_1 v) = h(u) \cdot_2 h(v)$.

Example: $h : \{a, b\}^* \rightarrow \mathbb{N}$ is defined as $h(w) = |w|$ is a monoid homomorphism from $(\Sigma^*, \cdot, e)$ to $(\mathbb{N}, +, 0)$.

Explanation: $h(e) = |e| = 0$ and $h(u \cdot v) = |u \cdot v| = |u| + |v|$.

It follows from these properties that any homomorphism defined on Σ^* is uniquely determined by it's values on Σ. Example: if $h(a) = ccc$ and $h(b) = dd$, then

$$h(abaab) = h(a)h(a)h(b)h(a)h(b) = cccddcccccccdd$$

If $A \subseteq \Sigma^*$, define

$$h(A) \stackrel{def}{=} \{h(x) \mid x \in A\}$$

and if $B \subseteq \Gamma^*$, define

$$h^{-1}(B) \stackrel{def}{=} \{h(x) \mid x \in B\}$$

The set $h(A)$ is called the image of A under h, and the set $h^{-1}(B)$ is called the preimage of B under h.

Theorem 1. *Let h be a monoid homomorphism from $(\Sigma^*, \cdot, e)$ to $(\Gamma^*, \cdot, e)$. Then:*

1. *If $L \subset \Sigma^*$ is regular, then $h(L) \subseteq \Gamma^*$ is regular.*

$$h(L) := \{h(w) \mid w \in L\}$$

2. *If $L \subseteq \Gamma^*$ is regular, then $h^-1(L) \subseteq \Gamma^*$ is regular.*

$$h^{-1}(L) := \{w \in \Sigma^* \mid h(w) \in L\}$$

Explanation: Any homomorphic image or homomorphic preimage of a regular language is regular.

Example:

$$L_1 := \{e, aa, aaaa, aaaaaa, \ldots, \}$$

$$h(L_1) := \{e, 00, 000, 0000, \ldots, \}$$

Here, if L_1 is regular, $h(L_1)$ is also regular.

Example:

$$h^{-1}(0) = \{a, c\}$$

$$h^{-1}(00) = \{aa, cc, ac, ca\}$$

Now, $h^{-1}(L_1)$ = set of all words of even length having a's or c's.-

$\therefore$ $h^{-1}(L_1)$ is regular if L_1 is regular.