Myhill Nerode Theorem

02 February 2021 23:34

(John Myhill & Anil Nerode, 1958)

Exercise 1.51 & 1.52 in the book.

This provides a necessary & sufficient condition for a language to be regular.

<u>Def 1</u>: Let x, y be strings over Σ and L be a language over Σ. We say x, y <u>are distinguishable by L</u> if $\exists z \in \Sigma^*$ such that $xz \in L$ and $yz \notin L$ or vice versa.

If x, y are not distinguishable by L, we say they are <u>indistinguishable by L</u>, <u>$x \equiv_L y$</u>.

<u>Exercise 1</u>: (Problem 1.51) Show that $\equiv_L$ is an equivalence relation.

$x \equiv_L x$

$x \equiv_L y \iff y \equiv_L x$

$x \equiv_L y,\ y \equiv_L w \implies x \equiv_L w$

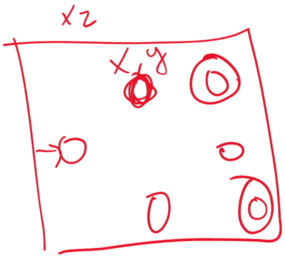
This means $\equiv_L$ partitions Σ^* into equivalence classes.

<u>Def 2</u>: Let L be a language and X be a set of strings. X is <u>pairwise distinguishable</u> by L if every two distinct strings $x, y \in X$ are distinguishable by L.

Def 3: The index of L is the size of the largest set X of strings such that X is pairwise distinguishable by L.

In other words, index of L : No. of equivalence classes of Σ^* as determined by $\equiv_L$.

Theorem (Myhill-Nerode Theorem): language L is regular iff it has a finite index. Moreover, the index of L is equal to the size of the smallest DFA which recognizes L.



Lemma 1: If L is recognized by a DFA with k states, then index$(L) \le k$.

Lemma 2: If index$(L) = k < \infty$, then there exists a DFA with k states that recognizes L.

Proof of MN theorem assuming lemma 1 & lemma 2:

$(\Longrightarrow)$ Suppose L is regular. Then there is a DFA that recognizes L. Consider a smallest DFA that recognizes L. Let this be M and let M have k states. By lemma 1, index$(L) \le k$.

... of the smallest DFA

M have k states. By ...

$$\boxed{\text{Index}(L) \le \text{Size of the smallest DFA that recognizes } L.}$$

($\Leftarrow$) Suppose L has finite index, say k. By lemma 2, there exists a DFA with k states that recognizes L. So L is regular.

$$\boxed{\left.\begin{array}{l}\text{Size of the smallest DFA} \\ \text{that recognizes } L\end{array}\right\} \le \text{Index}(L).}$$

$$\text{Index}(L) = \text{Size of the smallest DFA that recognizes } L.$$

Notation: $\delta^*(q,x)$ for $x \in \Sigma^*$ denotes the state reached by the DFA starting from q and reading the string x.

Proof of lemma 1: We will show that any two strings that end in the same state are indistinguishable.

Suppose L is recognized by a DFA M with k states. Suppose, for the sake of contradiction, index$(L) > k$. This means, there exists X such that X is pairwise distinguishable by L, and $|X| > k$.

This means,

pairwise distinguishable by L, and $|X| > k$.

Let q_0 be the starting state of M. By pigeonhole principle, there exists two strings $x, y \in X$, $x \neq y$, such that $\delta^*(q_0, x) = \delta^*(q_0, y)$.

Note that for any $z \in \Sigma^*$.

$$\delta^*(q_0, xz) = \delta^*(\delta^*(q_0, x), z)$$
$$= \delta^*(\delta^*(q_0, y), z) = \delta^*(q_0, yz).$$

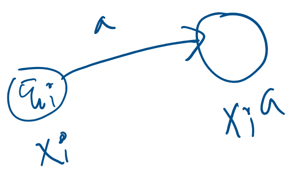
So $xz \in L \iff yz \in L$. So x, y are pairwise indistinguishable. So $x \equiv_L y$. This is a contradiction. So $\text{index}(L) \leq k$.

<u>Proof of lemma 2</u>: Suppose $\text{index}(L) = k < \infty$. We will construct a DFA M with k states that recognizes L. Let $X = \{x_1, x_2 .. x_k\} \subseteq \Sigma^*$ be a set of strings pairwise distinguishable by L.

$M = (Q, \Sigma, \delta, q_0, F)$. $Q = \{q_1, q_2, .. q_k\}$.

Each state $q_i \in Q$ corresponds to $x_i \in X$.

For each $a \in \Sigma$, $\delta(q_i, a)$ is defined as follows.



$x_i a \equiv_L x_j$ for some $x_j \in X$. Else, we can add $\{x_i a\} \cup X$ to get a bigger pairwise distinguishable

$x_i a \equiv_L x_j$ for ...

$\{x_i a\} \cup X$ to get a bigger pairwise distinguishable set. Now set $\delta(q_i, a) = q_j$.

Similarly $\varepsilon \equiv_L x_m$ for some $x_m \in X$. Set $q_0 = q_m$.

Finally, define $F = \{ q_i \mid x_i \in L \}$. Now we need to show that M recognizes L.

<u>Claim</u>: $\delta^*(q_i, w) = q_j \iff x_i w \equiv_L x_j$ for all $w \in \Sigma^*$.

Suppose $x \in L$. Then $x \equiv_L x_i$ for some $x_i \in X \cap L$.

$$x = \varepsilon x \equiv_L x_i \implies \delta^*(q_0, x) = q_i \in F.$$

Therefore x is accepted by M.

Suppose $x \notin L$. Then $x \equiv_L x_j$ for some $x_j \in X$, $x_j \notin L$. Similar to above, we get $\delta^*(q_0, x) = q_j$ where $q_j \notin F$. So M does not accept x.

Thus M recognizes L.

<u>Proof of Claim</u>: By induction on $|w|$.

When $|w| = 0$, $w = \varepsilon$.

$$\delta^*(q_i, \varepsilon) = \delta(q_i, \varepsilon) = q_i.$$

When ...

$$\delta^*(q_i, \varepsilon) = \delta(q_i, \varepsilon) = q_i .$$

$$x_i \varepsilon = x_i \equiv_L x_i .$$ Claim is true.

When $|w| = 1$, $w = a \in \Sigma$.

Let $\delta^*(q_i, a) = \delta(q_i, a) = q_j$

By defn of δ, we have $x_i a \equiv_L x_j$.

So claim is true.

When $|w| = l > 1$. Let $w = va$ where $|w| = |v| + 1$.
and $a \in \Sigma$.

$$\delta^*(q_i, w) = \delta^*(\delta^*(q_i, v), a) = \delta(q_{j_1}, a)$$
$$= q_{j_2}$$

where $q_{j_1} = \delta^*(q_i, v)$.

By induction, we have, $x_{j_1} \equiv_L x_i v$
and $x_{j_2} \equiv_L x_{j_1} a$

$$x_{j_2} \equiv_L x_{j_1} a \equiv_L x_i v a = x_i w .$$

So claim holds for w, $|w| > 1$ as well.

Example: $A = \{0^n 1^n \mid n \geq 0\}$.

Consider $x_i = 0^i$ for $i = 0, 1, 2, 3 \ldots$

... is pairwise distinguishable

Consider $x_i = 0$ for $i = 0, 1, 2,$

The set $X = \{ x_i \mid i \geq 0 \}$ is pairwise distinguishable by A.

Given x_i, x_j such that $i \neq j$.

Consider $z_i = 1^i$. $x_i z_i \in A$. $x_j z_i \notin A$.

z_i distinguishes x_i and x_j. So X is an infinite set pairwise distinguishable by A.

Thus A is not regular.