Myhill-Nerode Theorem

- Let Σ be a finite alphabet.
- Let $L \subseteq \Sigma^*$.
- Define a binary relation $\equiv_L$ on strings in Σ^* as follows:

$$x \equiv_L y \Longleftrightarrow \forall z \in \Sigma^*, (xz \in L \Leftrightarrow yz \in L)$$

- Show that $\equiv_L$ is an equivalence relation on Σ^*.
- Two strings x and y are said to be *indistinguishable* by L iff $x \equiv_L y$.
- Two strings x and y are said to be *distinguishable* by L iff x and y belong to different equivalence classes; that is, there exists some string z such that exactly one of xz or yz is in L.
- Let $[x] = \{y \mid y \equiv_L x\}$ be the equivalence classes.
- Let i$ndex(L)$ denote the number of equivalence classes.

Myhill-Nerode Theorem

Claim 1: If L is recognized by a DFA with k states then i$ndex(L) \leq k$.

Proof: Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA with k states that recognizes L.

- For each state $q \in Q$, define

$$C_q = \{x \in \Sigma^* \mid \hat{\delta}(q_0, x) = q\}.$$

- Let $x, y \in C_q$ for some $q \in Q$. That is, $\hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)$.
- We have, for all $z \in \Sigma^*$, $\hat{\delta}(q_0, xz) = \delta(\hat{\delta}(q_0, x), z) = \delta(\hat{\delta}(q_0, y), z) = \hat{\delta}(q_0, yz)$.
- That is, for all $z \in \Sigma^*$, it is true that $xz \in L \Leftrightarrow yz \in L$ showing that $x \equiv_L y$.
- That is, i$ndex(L) \leq |Q|$.

NOTE: Define a binary relation $\equiv_M$ on Σ^*:

$$x \equiv_M y \Longleftrightarrow \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y).$$

Then, $\equiv_M$ is an equivalence relation on Σ^* and the equivalence classes are $\{C_q \mid q \in Q\}$.

Myhill-Nerode Theorem

Claim 2: If $index(L)$ is a finite number k then there is a DFA with k states that accepts L.
Proof:

- Define a DFA $M' = (Q', \Sigma, \delta', q_0', F')$ as follows:
  - $Q' = \{[x] \mid x \in \Sigma^*\}$.
  - $q_0 = [\epsilon]$.
  - $\delta'([x], a) = [xa]$.
  - $F' = \{[x] \mid x \in L\}$.
- δ' is well-defined. That is, $\delta'([x], a) = [ya]$ for any $y \in [x]$ and all $a \in \Sigma$.

$$\begin{aligned} x \equiv_L y &\Rightarrow \forall\, z \in \Sigma^*, (xz \in L \Leftrightarrow yz \in L) \\ &\Rightarrow \forall\, a \in \Sigma, u \in \Sigma^*, (xau \in L \Leftrightarrow yau \in L) \\ &\Rightarrow \forall\, a \in \Sigma, (xa \equiv_L ya). \end{aligned}$$

- $x \in L \Leftrightarrow x \in L(M')$.

$$\begin{aligned} x \in L(M') &\Leftrightarrow \hat{\delta}'([\epsilon], x) \in F' \\ &\Leftrightarrow [x] \in F' \\ &\Leftrightarrow x \in L \end{aligned}$$

(We have used the fact that $\hat{\delta}'([\epsilon], x) = [x]$, which fact can be proved by induction on $|x|$.)

Myhill-Nerode Theorem

Claim 3: If L is a regular language then $index(L)$ (which is a finite number) is the size of the smallest DFA that recognizes L.

Proof:

- By Claim 1, $index(L) \ \leq$ the number of states in any DFA for L.
- The number of states in the DFA M' constructed in the proof of Claim 2 is $index(L)$.
- Therefore, M' is a minimum size DFA for L.