Distinguishability

Defn (Distinguishability)

Let $L \subseteq \Sigma^*$ be any language.

Two strings $x, y \in \Sigma^*$ are said to be **distinguishable (w.r.t L)** if $\exists\, z \in \Sigma^*$ s.t

$xz \in L$ and $yz \notin L$

Lemma: Let L be regular and $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA accepting L.

If $x, y \in \Sigma^*$ are distinguishable (w.r.t L), then

$$\hat{\delta}(q_0, x) \neq \hat{\delta}(q_0, y)$$

Proof: Suppose not. Let z be s.t

$xz \in L$ and $yz \notin L$. Then

$\hat{\delta}(q_0, xz) \in F$ but

$$\begin{aligned}
\hat{\delta}(q_0, xz) &= \hat{\delta}(\hat{\delta}(q_0, x), z) \\
&= \hat{\delta}(\hat{\delta}(q_0, y), z) \\
&= \hat{\delta}(q_0, yz)
\end{aligned}$$

But $yz \notin L$ so it can't be the case that $\hat{\delta}(q_0, yz) \in F$

Defn: A set S is said to be distinguishable if $\forall\, x \neq y \in S$, x, y are distinguishable

Theorem: Let $L \subseteq \Sigma^*$ be a regular language and let W be a distinguishable set (w.r.t L). If $M = (Q, \Sigma, \delta, q_0, F)$ is a DFA accepting L,

then $|Q| \geq |W|$

Corollary: Let $L \subseteq \Sigma^*$ be any language. If $\exists$ an infinite set W that is distinguishable w.r.t L, then L is not regular.

Examples

1. $L = \{0^n 1^n \mid n \geq 0\}$ is not regular

$W = \{0^n \mid n \geq 0\}$

$x = 0^i$ & $y = 0^j$

if $z = 0^i$ then $xz \in L$ & $yz \notin L$

- Sufficient to show that

$L = \{w \mid \#1(w) = \#0(w)\}$ is not regular

② $L = \{ w \mid$ the third last symbol from the end for w is a $0 \}$

- Any DFA for L requires at least 8 states

$W = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$x = 000 \qquad y = 001$

if $z = 11 \qquad xz = 00011 \in L \qquad yz = 00111 \notin L$

$x = 010 \qquad y = 100$

if $z = \varepsilon \qquad xz = 010 \in L \qquad yz = 100 \notin L$

③ $L = \{ 0^p \mid p$ is a prime$\}$

$W = L$: $\quad x = 0^p \quad y = 0^q \qquad q > p$

$\{ p + k(q-p) \mid 0 \leq k \leq p \}$

if $k = 0$, then $p + k(q-p)$ is prime

if $k = p$, then $p + k(q-p) = p(1 + q - p)$ and is not a prime.

$\exists\, i$ s.t $p + i(q-p)$ is prime and $p + (i+1)(q-p)$ is not prime

$0^p \cdot 0^{i(q-p)}$ is prime

$0^q\, 0^{i(q-p)} = 0^p \cdot 0^{(i+1)(q-p)}$ is not a prime

Indistinguishability as an equivalence relation

$x \equiv_L y$ if $\forall z \in \Sigma^*$ $xz \in L \iff yz \in L$

1 $\equiv_L$ is an equivalence relation

- reflexive: $x \equiv_L x$
- Symmetric: $x \equiv_L y \Rightarrow y \equiv_L x$
- transitive: $w \equiv_L x$ & $x \equiv_L y \Rightarrow w \equiv_L y$

$[\equiv_L]$ - equivalence classes of $\equiv_L$ partition Σ^*