January 31, 2019 10:50 AM

Proving Non-Regularity

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

Pf: By contradiction.
Suppose L is regular.
So, L is accepted by some DFA $M = (Q, \Sigma, \delta, s, A)$

vague idea - any DFA needs to "remember" n

Claim: $\delta^*(s, 0^i) \neq \delta^*(s, 0^j) \quad \forall\, i \neq j$

[Pf: If $\delta^*(s, 0^i) = \delta^*(s, 0^j)$,

then

$$\underbrace{\delta^*(\delta^*(s, 0^i), 1^i)}_{\delta^*(s,\, 0^i 1^i)\,\in A} = \delta^*(\delta^*(s, 0^j), 1^i)$$

$$\delta^*(s, 0^i 1^i) = \delta^*(s, 0^j 1^i)$$

$$\in A \qquad\qquad \notin A$$

$$\boxed{\delta^*(\delta^*(s, x), y) = \delta^*(s, xy)}$$

Contradiction! $\square$]

By claim,

$\delta^*(s, 0^0), \ \delta^*(s, 0^1), \ \delta^*(s, 0^2)$

$\delta^*(s, 0^0)$, $\delta^*(s, 0^1)$, $\delta^*(s, 0^2)$, ...
are all distinct states

$\Rightarrow$ Q infinite:
Contradiction! $\square$

Rmk: can generalize argument ...

Def Given lang. $L \subseteq \Sigma^*$,
$x, y \in \Sigma^*$ are distinguishable if
$\exists w$, $(xw \in L \ \& \ yw \notin L)$
or $(xw \notin L \ \& \ yw \in L)$

A set F is a distinguishing set (also called a fooling set)
if $\forall x, y \in F$ $(x \neq y)$
$\Rightarrow$ x, y are distinguishable.

Thm If L has an infinite fooling set F,
then L is not regular.

Pf: Suppose L is regular, accepted by some DFA $M = (Q, \Sigma, \delta, s, A)$.

Claim: $\forall x, y \in F$ $(x \neq y)$, $\delta^*(s,x) \neq \delta^*(s,y)$

[Pf: If $\delta^*(s,x) = \delta^*(s,y)$,
By def'n of "distinguishable",
$\exists w$, $xw \in L$ & $yw \notin L$
(or vice versa)

$\exists w,$ $xw \in A$, $yw \notin A$ (or vice versa)

Then $\delta^*(\delta^*(s,x), w) = \delta^*(\delta^*(s,y), w)$

$\delta^*(s, xw) = \delta^*(s, yw)$]

$\in A$ $\quad\quad \notin A$

Then $\{ \delta^*(s,x) \mid x \in F \}$ are all distinct

Contra! $\square$

Ex a) $L = \{ x \in \{0,1\}^* \mid \#_0(x) = \#_1(x) \}$ is not regular.

Pf: Let $F = \{ 0^i \mid i \geq 0 \}$.

Given two arbitrary strings x, y in F,

$x = 0^i, \quad y = 0^j, \quad i \neq j$

Pick $w = 1^i$.

$\Rightarrow \quad xw = 0^i 1^i \in L$

$yw = 0^j 1^i \notin L$.

Then F is a fooling set, & infinite. $\square$

b) $L = \{ \text{all palindromes} \}$

$= \{ w \in \{0,1\}^* \mid w = w^R \}$

is not regular.

Pf: Let $F = \{ 0^i \mid i \geq 0 \}$.

Given two arbitrary strings $x, y \in F$ $(x \neq y)$,

$x = 0^i, \quad y = 0^j \quad (i \neq j)$

Given two arbitrary strings $x, y \in F$,

$x = 0^i, \quad y = 0^j \qquad (i \neq j)$

Pick $w = 10^i$

$\Rightarrow \quad xw = 0^i 1 0^i \in L$

$yw = 0^j 1 0^i \notin L$

Then F is a fooling set, & infinite.

c) $L = \{ 0^{n^2} \mid n \geq 0 \}$ is not regular.

Pf: Let $F = \{ 0^i \mid i \geq 0 \}$.

Given two arbitrary strings $x, y \in F$

$x = 0^i, \quad y = 0^j, \qquad i \neq j,$ w.l.o.g. $i < j$.

Pick $w = 0^{j^2 - i}$

Then $xw = 0^{j^2} \in L$

$yw = 0^{j^2 - i + j} \notin L$.

$$j^2 < j^2 - i + j < (j+1)^2$$

Then F is inf. fooling set.

d) $L = \{ 0^p \mid p \text{ prime} \}$ is not regular.

Pf: Let $F = \{ 0^i \mid i \geq 0 \}$

Given $x, y \in F$,

$x = 0^i, \quad y = 0^j, \qquad (i \neq j)$

w.l.o.g. $i < j$

Pick prime $p > i$

Pick prime $p > i$

(try $w = 0^{p-i}$ $\quad$ xw $\quad$ $yw = 0^{p-i+j}$ $\quad$ if not work $p-i+j$ prime

try $w = 0^{p+j-2i}$ $\quad$ $xw = 0^{p-i+j}$ $\quad$ $yw = 0^{p+\underline{2j-2i}}$

. . . .)

let k be smallest s.t.

$p + k(j-i)$ is composite

$(1 \leq k \leq p)$

pick $w = 0^{p+(k-1)(j-i)-i}$

$$xw = 0^{p+(k-1)(j-i)} \in L$$

$$yw = 0^{p+(k-1)(j-i)-i+j}$$

$$= 0^{p+k(j-i)} \notin L. \quad \square$$

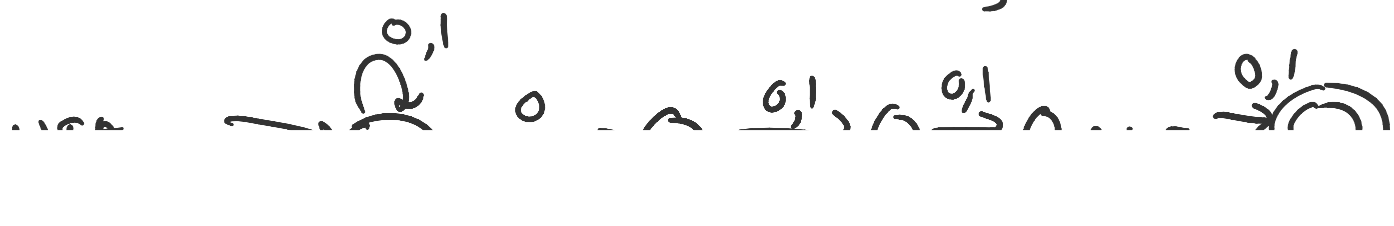
$\exists$ inf. fooling set

Extension: If L has a fooling set F of size n, then any DFA for L has $\geq n$ states.

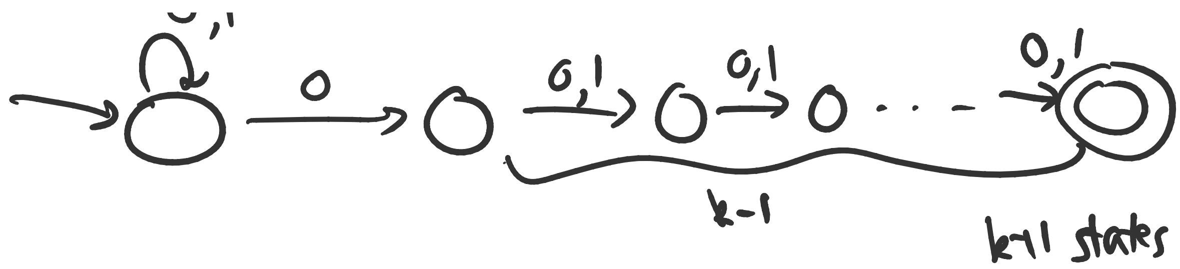
Pf: same!

Ex $\quad$ k const.

$L_k = \{ x \in \{0,1\}^* \mid k^{th}$ symbol from right is $0 \}$



NFA



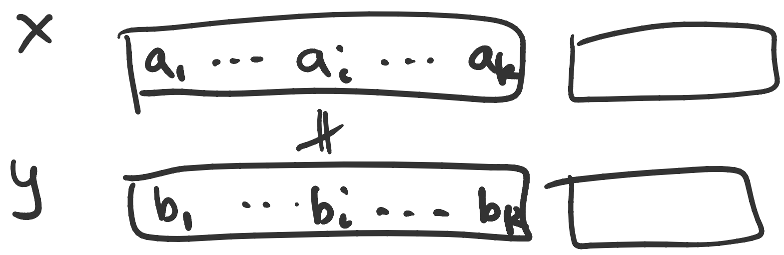
Let $F = \{ x \in \{0,1\}^* \mid \; |x| = k \}$
is a fooling set of size 2^k

(Let $x, y \in F$, $|x| = |y| = k$, $x \neq y$

$x = a_1 a_2 \cdots a_k$

$y = b_1 b_2 \cdots b_k$, $\quad a_i \neq b_i$

$a_i = 1, \; b_i = 0$



Pick $w = 0^{i-1}$

$xw \in L$

$yw \notin L$.)

$\Rightarrow$ any DFA requires $\geq 2^k$ states.

Further Extension: (Myhill-Nerode Thm)

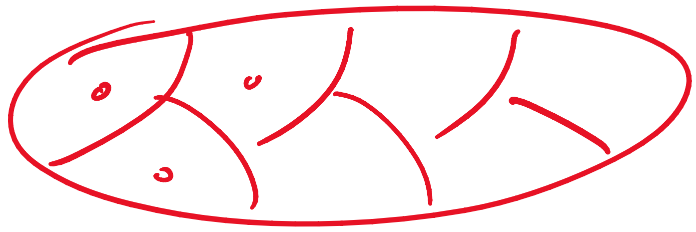
max fooling set size $=$ min # states

equiv classes for $\equiv_L$

Write $x \equiv_L y$ iff x, y not distinguishable

equiv. relation

partition into equiv classes



Σ^*