How to prove nonregularity? Myhill-Nerode theorem

Friday, April 18, 2025 12:49 PM

Question. How do we show that no program can solve a specific problem?

Answer. We need to analyse the structure of programs.
the simpler the better !

Q. What can't a DFA/NFA do ?

counting $\quad L := \{0^n 1^n : n \in \mathbb{N}\}$

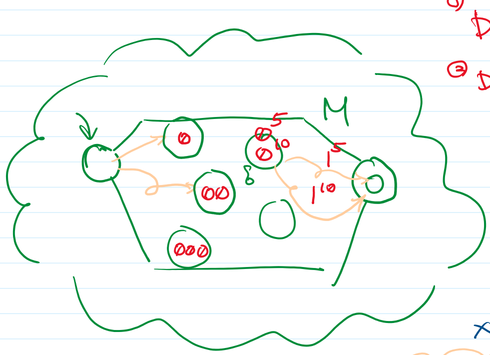
majority

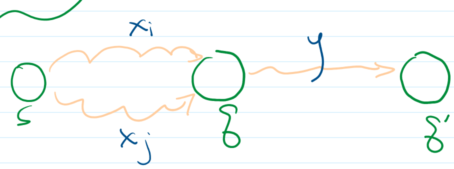
balanced parentheses

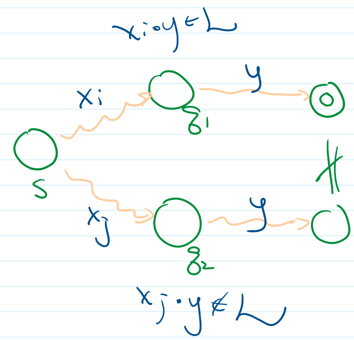
Q. How do we prove this ?

① DFA M is finite !

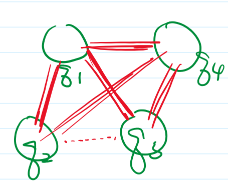
② DFA is deterministic !







Observation. For any DFA M,
If x_i and x_j lead to same state q,
then $\forall$ string $y \in \Sigma^*$
$x_i \cdot y$ and $x_j \cdot y$ lead to same state.



Fooling set : Prefixes $\exists F := \{x_1, x_2, \dots\}$ fooling for L if:
$\forall$ prefixes $x_i \neq x_j$ in F. $\exists$ suffix $y \in \Sigma^*$,
s.t. exactly one of $x_i \cdot y$, $x_j \cdot y \in L$

Intuition every prefix in F needs a new state.

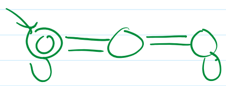
example. $L := \{$ binary integers divisible by $3 \}$

$F := \{0, 1, 10\}$

$(0, 1)$: $y = \varepsilon$ $\quad 0 \cdot \varepsilon \in L$, $\; 1 \cdot \varepsilon \notin L$

$(0, 10)$: $y = \varepsilon$

$(1, 10)$: $y = 1$ $\quad 1 \cdot 1 \in L$, $\; 10 \cdot 1 \notin L$



example. $L := \{0^n 1^n : n \geq 0\}$

$F := \{0, 00, 000 \ldots\} = \{0^n : n \in \mathbb{N}\}$.

Claim F is fooling.

$\forall x_i, x_j \in F$ $\quad \exists$ suffix $y := 1^j$ $\quad 0^i \cdot 1^j \notin L$, $\; 0^j \cdot 1^j \in L$

$0^i \; 0^j$
$(i < j)$

$L' := \{0^n 1^m : n \leq m\}$

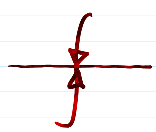
$F := \{0^n : n \in N\}$

$\forall 0^i, 0^j \; (i<j) \quad \exists y := 1^i \quad 0^i 1^i \in L$, $\; 0^j 1^i \notin L$

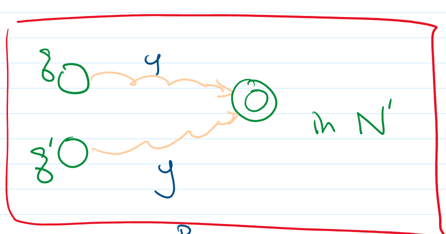
Prop. If L has a fooling set of infinite size, then L is not regular.

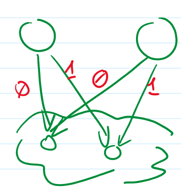
Myhill-Nerode Thm. For regular language L,

max fooling set size $=$ min DFA size.

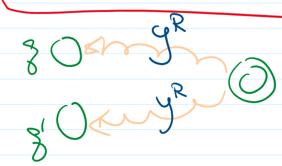


BRZOZOWSKI-MINIMIZATION(N):
- ***input:*** NFA N recogizing language L
- reverse N and obtain N^R, recognizing $rev(L)$
- turn N^R into DFA M^R
- reverse M^R and obtain N', recognizing L
- turn N' into DFA M
- return M





Indistinguishable states :



DFA!
$M \; M^R$

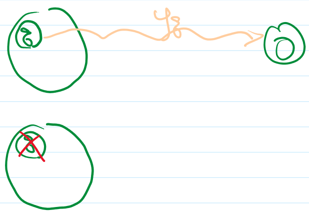
Claim No two states in N', say q and q', from which accepts the same word.

proof. in DFA M^R, reading y^R leads to the same state.

$\Rightarrow$ in NFA N', from q and q', exactly one of $q \cdot q'$ leads to $\textcircled{o}$ by reading y

$\Rightarrow$ in DFA M, every state is unique & non mergable.

⇒ in DFA M, every state is unique & non mergable.



thus M is minimized. ∎