Def^n: Given a language $L \subseteq \Sigma^*$, a set $S \subseteq \Sigma^*$ is {distinguishing / distinctive / pairwise distinct / a PD set} for L if **for all** $x, y \in S$, $x \neq y$ "Let any ... be given"

there exists $z \in \Sigma^*$ s.t. $L(xz) \neq L(yz)$.

"Take"

Note: S need not be a subset of L.

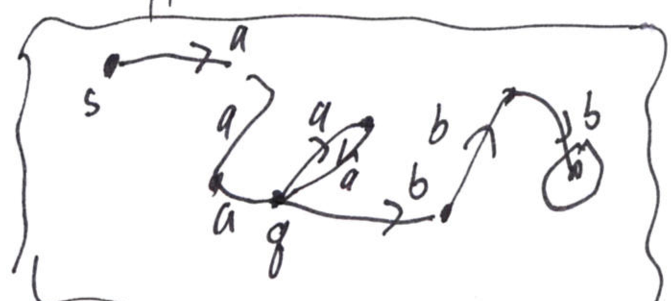
$\Sigma = \{a, b\}$

Example: $L = \{a^n b^n : n \geq 0\}$

$S = \{a^n : n \geq 0\} = a^*$

Consider $x = a^3$, $y = a^5$. Any potential DFA M s.t. $L(M) = L$ must process x, y to different states. If not:

$M =$



Take $z = b^3$. Then $xz \in L$
$xz = a^3 b^3$

But M also accepts $yz = a^5 b^3$ but $yz \notin L$. This "contradicts" $L(M) = L$.

Proof that S is PD for L:

Let any $x, y \in S$, $x \neq y$, **be given**. Then there are natural numbers $m, n \geq 0$, $m \neq n$, such that $x = a^m$ and $y = a^n$. [By defn of S.]

Take $z = b^m$. Then $xz = a^m b^m \in L$, but $yz = a^n b^m \notin L$ since $n \neq m$. Thus $L(xz) \neq L(yz)$. Since $x, y \in S$ were an arbitrary distinct pair, S is PD for L. ☒

Myhill-Nerode Thm, "Part I": If S is PD for L, then any DFA M s.t. $L(M) = L$ needs at least $|S|$-many states, and if S is infinite $\therefore$ no such M exists.

Theorem L is nonregular. [by MNT, so you first need an infinite PD set for L]

Proof: **Take** $S = \underline{\$^*}$. "Clearly S is infinite."

Let any $x, y \in S$, $x \neq y$, be given. Then there are $m, n \in \mathbb{N}$ s.t. (w.l.o.g. $m < n$)
we can helpfully write $x = \underline{\$^m}$ and $y = \underline{\$^n}$ where $\underline{m \neq n}$.

Take $z = \underline{D^n}$. Then $xz \notin L$ because $\underline{xz = \$^m D^n}$ doesn't survive

but $yz \in L$ because $\underline{yz = \$^n D^n \text{ which survives.}}$

Thus $L(xz) \neq L(yz)$. Since $x, y \in S$ were arbitrary, S is PD for L, and since S is infinite, L is nonregular by MNT. $\boxtimes$

MNT: If $(\exists S, |S| = \infty)(\forall x, y \in S, x \neq y)(\exists z) L(xz) \neq L(yz)$, then $L \notin$ REG

Example: $L' = \{x \in \{\$, D\}^* : x$ is a survivable dungeon in the game allowing any # of swords$\}$.

$x = \$D\$\$D\$DD\$ \in L'$

$L'' = \{x \in \{\$, D\}^* : \#\$(x) = \#D(x)\}$. Exact same proof!

$L' = \sim L''$? MNT never cares about switching L and $\tilde{L}$

$L_4 = \{x \in \{\$, D\}^* : x$ is potentially survivable; i.e. $\#\$(x) \geq \#D(x)\}$.

$L_4' = \{x \in \{\$, D\}^* : \#\$(x) > \#D(x)\}$. ...Take $z = D^{n-1}$ $>$

$L_5 = \{x \in \{\$, D\}^* : \#\$(x) \leq \#D(x)\}$. ...Take $z = D^m$ $\quad xz \notin L$, $yz \in L$.

$L_6 = \{x \in \{a, b\}^* : \#a(x) + \#b(x)$ is odd$\}$ __is__ a regular language

The Full MNT: John Myhill UB † 1987 (3)
(1958) Anil Nerode Cornell still alive

<u>Part I</u>: If $\exists$ an inf. PD set S for L, then L is nonregular

<u>Part II</u>: If L is nonregular, then there is an infinite PD set S for L.
<u>Conversely</u>,

Equivalently: If all PD sets S for L are finite, then L <u>is</u> regular.

The import of "Part II" is $\approx$ if L is nonregular, there is always in some sense an MNT proof of that.

Extra
<u>Another Example</u>. (for Tuesday, this or similar).

$L = \{ww : w \in \{0,1\}^*\}$. How should we choose S?

If we just choose $S = 0^*$, it's not clear we know the idea. Well, let any $x, y \in S$, $x \neq y$ be given. Then there are numbers $m, n \in \mathbb{N}$, where <u>wlog</u>. $m < n$, such that $x = 0^m$ and $y = 0^n$. Take $z =$ ___

- If we're on autopilot, we might take $z = 0^m$. Then $xz = 0^m 0^m$ is certainly in L, but what about $yz = 0^n 0^m$? You might be tempted to say "not in L since $n \neq m$" but look: if (say) $m = 3$ and $n = 5$, then $0^n 0^m = 0^{5+3} = 0^8 = 0^4 \cdot 0^4$ by a different "parse", so $yz \in L$ too.
- Instead take $z = \underline{10^m 1}$. Then $xz = 0^m 1 0^m 1 \in L$, but $yz = 0^n 1 0^m 1 \notin L$.

So we win: <u>L is nonregular</u>, but choosing $S = \underline{0^* 1}$ would have put us on-track <u>sooner</u>.