Def: Given a language $L \subseteq \Sigma^*$, a set $S \subseteq \Sigma^*$ is a Po set for $L$ if for all $x, y \in S$, $x \neq y$ there exists $z \in \Sigma^*$ such that $L(xz) \neq L(yz)$.

Note: $S$ need not be a subset of $L$.

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

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

Proof that $S$ is Po 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 $y = a^n$. [Def of $S$]

Take $z = b^n$. Then $xz = a^m b^n \in L$ 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 Po for $L$.

Myhill-Nerode Thm, Part I: If $S$ is Po for $L$, then any DFA $M$ s.t. $L(M) = L$ needs at least $|S| - 1$ many states, and if $S$ is infinite, no such $M$ exists.
Theorem L is non-regular: [by MNT, so you first need an infinite PD set for L]

Proof: Take $S = \{ \} \cdot \{ \}^*$. 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.
we can helpfully write $x = \{ \}^m$ and $y = \{ \}^n$, where $\Delta m \neq \Delta n$.

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

but $yz \in L$ because $yz = \{ \}^n \{ \}^m$ which survives.

Thus $L(xy) \neq L(yz)$. Since $x, y \in S$ were arbitrary, $S$ is PD for $L$, and since $S$ is infinite, $L$ is non-regular by MNT. $\square$

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

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

$x = \{\}^D\{\}\{\}\{\} \notin L'$

$L'' = \{ x \in \{\}, \{\}^* : \#s(x) = \#D(x)^2 \}$, exact same proof $L' = \Delta L''$.

MNT never cares about switching $L$ and $L'$.

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

$L'_4 = \{ x \in \{\}, \{\}^* : \#s(x) > \#D(x)^2 \}$, take $z = \{\}^{D-1}$.

$L_5 = \{ x \in \{\}, \{\}^* : \#s(x) \leq \#D(x)^2 \}$, take $z = \{\}^D$, $yz \notin L$.

$L_6 = \{ x \in \{a,b\}^* : \#a(x) + \#b(x) \text{ is odd} \}$ is a regular language.
The Full MNT: John Myhill UB + 1987
(1958) Anil Nerode Cornell still alive

Part I: If \( \exists \) an ininite PD set \( S \) for \( L \), then \( L \) is nonregular.

Part II: If \( L \) is nonregular, then there is an infinite PD set \( S \) for \( L \).

Conversely, equivalence: If all PD sets \( S \) for \( L \) are finite, then \( L \) is regular.

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

Extra

Another Example. (For Tuesday, this or similar).

\[ L = \frac{1}{2} \text{WW: } W \in \{0,1\}^* \text{?} \] How should we choose \( S \)?

If we just choose \( S = \emptyset \), it's not clear we know the idea. Well, let any \( x_1 \in S \), \( x_2 \) be given. Then there are numbers \( m, n \in \mathbb{N} \), where WLOG \( m \leq n \), such that \( x = 0^m \) and \( y = 0^n \). Take \( z = 0^3 \).

If we're on autopilot, we might take \( z = 0^m \). Then \( xz = 0^m0^m \) is certainly in \( L \), but what about \( yz = 0^n0^n \)? You might be tempted to say "not in \( L \) since \( n \neq m \)" but look: if (say) \( m = 3 \) and \( n = 5 \), then \( 0^30^5 = 0^8 = 0^40^4 \) by a different "parse," so \( yz \in L \) too.

Instead take \( z = 10^m1 \). Then \( xz = 0^m10^m1 \in L \), but \( yz = 0^n10^m1 \) dh. So we win: \( L \) is nonregular, but choosing \( S = 0^m1 \) would have put us on "backstage."