CSE 396 — Lecture Tue Mar 5 — Spr. 2019

Top Hat # 7592

Let $L = \{a^i b^j : i+j \text{ is even}\}$. Defaults: $i, j \geq 0$, so ϵ is in L.

Suppose we try to prove L is not regular. RED = errors.

"Take $S = a^*$, clearly infinite. Let any $x, y \in S$, $x \neq y$ be given. Then we can write $x = a^m$, $y = a^n$ where $n = m+1$. Take $z = bb$. Then $xz = a^m b^2$ and $yz = a^n b^2$. Then $m+2$ is even $\iff$ $n+2$ is odd since $n = m+1$, so $L(xz) \neq L(yz)$. So S is PD for L, ... etc.

ERROR: (x, y) is not a general choice of a pair from S.

where n is parity different from m is the same error.

Try #2: Take $S = (aa)^*$. Also clearly infinite.

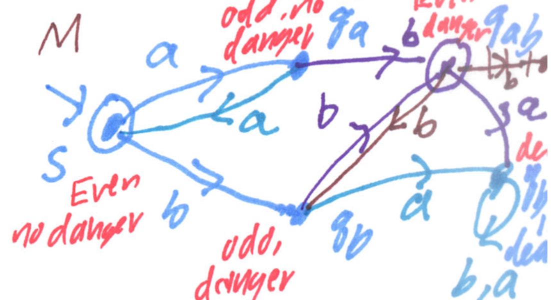
Let any $x, y \in S$, $x \neq y$, be given. Then $x = a^m$, $y = a^n$ where m and n are both even and $n \neq m$. Take $z =$ ______ ?? Not possible to get $L(xz) \neq L(yz)$.

In fact, all strings in S are equivalent w.r. to L.
(with respect)

We did get some information from the first try: $a^{m+1} \not\sim_L a^m$ for all m. Let's put $\underline{\epsilon}$ and $\underline{a}$ into our S representing the "m even" and "m odd" cases. Any more? Consider $x' = \underline{b}$. Now $b \notin L$ and $\epsilon \in L$ so $b \not\sim_L \epsilon$, but is $b \sim_L a$? $L = \{a^i b^j : i+j \text{ is even}\}$, so $ba \notin L$ while $aa \in L$. So $b \not\sim_L a$ via $z = a$.

S now $= \{\epsilon, a, b\}$. Is that all? Ah, ba must go to a dead state distinct from the others since none of ϵ, a, or b is dead w.r. to L. Now $S = \{\epsilon, a, b, ba, ab\}$. Yes. M is done so S is done.

Since we do feel that L is regular, we can use S to help design a DFA. All strings in S must go to different states. Now we have 4 states. Do we need any more? Is $aa \sim_L \epsilon$? Yes, so $\delta(q_a, a) = s$ is fine. What about ab? It is in L. But $ab \not\sim_L \epsilon$ by $z = a$. And ab is distinctive from all the other elements of S which are $\notin L$. Is $bb \sim_L a$?



Full Statement of MNT: A language L is regular $\iff$ all PD sets for L are [illegible]

when so, there is a maximum size m of a PD set, and m is the minimum size of a DFA M s.t. $L(M) = L$, and that M is unique of that size. Proof not given.

Def^n:
- A state q is equivalent to itself. (in a DFA M)
- Two states p and q are equivalent if they are both accepting or both rejecting, and for all $c \in \Sigma$, the states $p' = \delta(p,c)$ and $q' = \delta(q,c)$ are equivalent.

Is this definition circular? Yes. but for our purposes it is OK.

Inequivalence, based on $p \not\sim_M q$ if $p \in F \wedge q \notin F$ ~~and~~ or vice-versa, is not circular.

[That is the basis for an algorithm for minimizing DFAs, but it is not on our syllabus.

More MNT Examples: $L_{\$d} = \{x \in \{\$, d\}^* :$ x is a survivable dungeon when you may hold any # of spears ~~\$\$~~ \$ $\}$.

Prove that $L_{\$d}$ is not regular: Take $S = \$^*$. Clearly S is infinite. Let any $x, y \in S$, $x \neq y$ be given. Then there are $m, n \geq 0$ such that $x = \$^m$, $y = \$^n$, and wlog $m < n$. Take $z = d^n$. Then $xz = \$^m d^n \notin L_{\$d}$ because $m < n$ so the player gets killed by the $m+1$st dragon. But $yz = \$^n d^n \in L_{\$d}$. Thus $L_{\$d}(xz) \neq L_{\$d}(yz)$, and since $x, y \in S$ are arbitrary, S is an infinite PD set for $L_{\$d}$. $\square$

What this also means is that in versions where the player may hold up to k spears, a DFA needs separate states for $\$^0 = \epsilon$, $\$$, $\$\$$, $\$\$\$$, $\$^4$, ..., $\$^k$. Plus the dead state makes $k+2$ states, and this is the minimum m.

Abstract Example: Define $L_k = \{x \in \{0,1\}^* : |x| \geq k$ and the kth bit from right is 1$\}$. NFA for L_k has $k+1$ states. How many states does a DFA M need? $m = 2^k$ states.

Claim: $S = \{0,1\}^k$ is a PD set for L_k, of size 2^k, so that many states are needed. Numbered from 0

Let any $x, y \in S$, $x \neq y$ be given. Because $x \neq y$, there is a bit place i s.t. $x_i \neq y_i$. Take $z = 0^i$. wlog suppose "x" is the string such that $x_i = 1$, $y_i = 0$. Then xz has a 1 in the kth from right place, but yz has a 0 there. So $yz \notin L_k$, $xz \in L_k$. Since x, y are arbitrary, S is a PD set for L_k. $\square$