CSE 396 Lecture Thu Mar. 1 Spring 2018 (i)

My off. Hrs 1–3pm today

Top Hat # 8738

Def^n: Given any language L (not nec. regular), define

$$x \equiv_L y \text{ if for all } z \in \Sigma^*,\ \underbrace{xz \in L}_{L(xz)} \Leftrightarrow \underbrace{yz \in L}_{L(yz)}.$$

$L(xz) = L(yz)$ $\quad L(x) = \begin{cases} 1 & \text{if } x \ldots \\ 0 & \text{if } x \ldots \end{cases}$ characteristic function of L

This is an equivalence relation

Observe: If L is regular and $x \equiv_L y$, then it is OK for a DFA M to process x and y from s to the same state p.

for L, i.e. s.t. $L(M) = L$.

Conversely, if M does process x and y to the same state p, then we better have $x \equiv_L y$ (else we can't have $L(M) = L$)

Hence, if $x \not\equiv_L y$ then if M processes x from s to p and processes y from s to q, the states p, q must differ.

Def^n: A subset $S \subseteq \Sigma^*$ is pairwise distinct ~~distinctive~~ (PD) for the language L if for all $x, y \in S$ with $x \neq y$, $\boxed{x \not\equiv_L y.}$

Observe: If L has a PD set S of size $\boxed{17}$ then any DFA M s.t. $L(M) = L$ needs to process all members of S to different states, and hence M needs (at least) $\boxed{17}$ states.

(if any)

Thus: If L has a PD set S of size $\boxed{\infty}$ then any DFA M s.t. $L(M) = L$ needs ... $\boxed{\infty}$ many states.

Contradiction in terms! $\therefore$ If L has an inf. PD set, it has no DFA. so L is not regular.

UB 1987 Anil, Cornell MSI 1958

Myhill-Nerode Theorem (first part): Let L be any lang.

If There Exists a subset $S \subseteq \Sigma^*$ such that S is infinite and

S is PD for L: For All $x, y \in S$ $(x \neq y)$

There Exists a $z \in \Sigma^*$ st. $L(xz) \neq L(yz)$ $\quad x \not\sim_L y$

then L is not regular.

(Second part is the converse.)

Given any language L to prove nonregular, we can execute the following "proof script":

Take $S =$ ________. [Verify that S is infinite, usually quick]

Let any $x, y \in S$, $x \neq y$, be given. Then we can (without loss of generality) helpfully represent $x =$ ____, $y =$ ____. based on the form of the S we took

Take $z =$ ______. Then $L(xz) \neq L(yz)$ because ____
fill in reasoning: $xz =$ ___ $\in L$ but yz ___ $\notin L$ or vice-versa.

Thus S is a PD set for L, and since S is infinite, L is non-regular by MNT. ☒

Applications / Examples: $L_1 = \{0^n 1^n : n \geq 0\}$ (text) $\quad L_3 =$ "Spears & Dragons holding any # of spears."

$L_2 = \{xx : x \in \{0,1\}^*\}$

L_1: Take $S = \underline{0^*} = \{0^n : n \geq 0\}$. Clearly S is infinite.

Let any $x, y \in S$, $x \neq y$ be given. By the form of S, we can write $x = 0^m$, $y = 0^n$ where $m \neq n$ [understand: $m \geq 0$, $n \geq 0$]

Side note: Wlog (without loss of generality) we can suppose x is the shorter of x and y so we can assume $m < n$.

Take $\underline{z = 1^m}$.

Then $xz = 0^m 1^m \in L_1$

but $yz = 0^n 1^m \notin L_1$ because $n \neq m$.

Note: $L_1 = \{w : w$ can be written as $w = 0^{r_1} 1^{r_2}$ where $r_1 = r_2\}$

Since $x, y \in S$ are arbitrary → Hence S is PD for L_1, and since S is infinite, L_1 is not regular.

How about $L_1' = \{x \in \{0,1\}^* : \#0(x) = \#1(x)\}$? Same proof.

L_2: Take $S = 0^*$, clearly infinite. Let any $x, y \in S$, $x \neq y$, be given. Then $x = 0^m$, $y = 0^n$ where $n > m$ wlog. Take $z = 0^m$? Then $xz = 0^m 0^m \in L_2$ but $yz = 0^m 0^n$ ~~$\notin L_2$ since~~ $n > m$

No: could be $x = 000$, $y = 00000$ ($n = 5$) $yz = 00000 \cdot 000 = 0000 \cdot 0000 \in L_2$ after all!

Fix: Take $\underline{z = 10^m 1}$. Then

$xz = 0^m 10^m 1 = 0^m 1 \cdot 0^m 1 \in L_2$ but

$yz = 0^n 10^m 1 \notin L_2$ because it can't be written as a double-word by n ... ☒

Could have expressed the intuition better by taking $S = \underline{0^* 1}$ to begin with.

L_3: Take $S = \$^*$ Clearly infinite. Let any $x, y \in S$, $x \neq y$ be given. Then $x = \$^m$, $y = \$^n$ where $n > m$ wlog. Take $\underline{z = D^n}$.

Then $xz = \$^m D^n \notin L_3$ since $n > m$ Kills, but $yz \in L_3$. ☒