Pumping Lemma

To prove that a language is regular $\equiv$ DFA, NFA, Reg Exp, Linear grammar

There must be languages that are not regular.

How to prove certain languages to be not regular.

PL → used to prove non-regularity

↳ pigeon-hole principle

proof by contradiction

Assume that a DFA exists $\Rightarrow$ a contradiction

Example: $L = \{a^n b^n \mid n \geq 0\} \subseteq \{a, b\}^*$

→ Assume that D is a DFA with $\mathcal{L}(D) = L$.

Intuition: ϵ, ab, aabb, aaabbb, ..., $\underbrace{aa\ldots a}_{n}\underbrace{bb\ldots b}_{n}$

DFA → no external memory

→ finitely many states → a finite amount of memory

k states → $\log_2 k$ bits of memory

n can be very large → all these cannot be remembered

Formal proof $\mathcal{L}(D) = L$. Let k be the number of states of D.

↳ a finite positive integer

$n = \lceil k/2 \rceil$

$\alpha = a^n b^n = a^{\lceil k/2 \rceil} b^{\lceil k/2 \rceil} \in L$ $\quad |\alpha| = \lceil k/2 \rceil + \lceil k/2 \rceil \geq k$

D must accept α.

$$S \xrightarrow{a} p_1 \xrightarrow{a} p_2 \to \cdots \xrightarrow{a} p_n \xrightarrow{b} p_{n+1} \xrightarrow{b} p_{n+2} \to \cdots \xrightarrow{b} p_{2n}$$

$S = p_0$; $p_{2n} = r \in F$

$2n+1$ states $p_0, p_1, p_2, \ldots, p_{2n}$

k is the no. of states of D

$n = \lceil k/2 \rceil \geq \frac{k}{2}$

$2n \geq k$.

$\geq k+1 > k$

Some state must repeat

We must have $p_i = p_j$ for $0 \leq i < j \leq 2n$

[by the pigeon-hole principle]

$$S \xrightarrow{u} p_i \xrightarrow{v} p_j = p_i \xrightarrow{w} r \in F$$

$\alpha = a^n b^n = uvw$

$\hat{\delta}(s, u) = p_i$

$\hat{\delta}(p_i, v) = p_j = p_i$

$\hat{\delta}(p_i, w) = r$

$\alpha' = uw$

$\hat{\delta}(s, uw)$

$= \hat{\delta}(\hat{\delta}(s, u), w)$

$= \hat{\delta}(p_i, w) = r \in F$

D also accepts $\alpha' = uw$

$\alpha'' = uvvw = uv^2w$

$\hat{\delta}(s, uv^2w) = \hat{\delta}(\hat{\delta}(s, u), v^2w) = \hat{\delta}(p_i, v^2w)$

$= \hat{\delta}(\hat{\delta}(p_i, v), vw) = \hat{\delta}(p_i, vw) = \hat{\delta}(\hat{\delta}(p_i, v), w)$

$= \hat{\delta}(p_i, w) = r \in F$ D also accepts $\alpha'' = uv^2w$

Contradictions ?

$\alpha = a^n b^n = uvw \qquad |v| > 0$

v: non-empty string

$\alpha' = uw \in L$

If Case 3 occurs, we may have $v = a^{\ell} b^{\ell}$

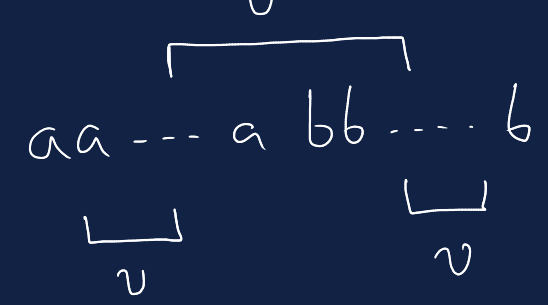
$\alpha' = uw = a^{n-\ell} b^{n-\ell} \in L$ [no contradiction]

✓ Case 1 : $\#a(\alpha') < \#b(\alpha')$ $\quad \alpha' \notin L$ ↯

✓ Case 2 : $\#a(\alpha') > \#b(\alpha')$ $\quad \alpha' \notin L$ ↯

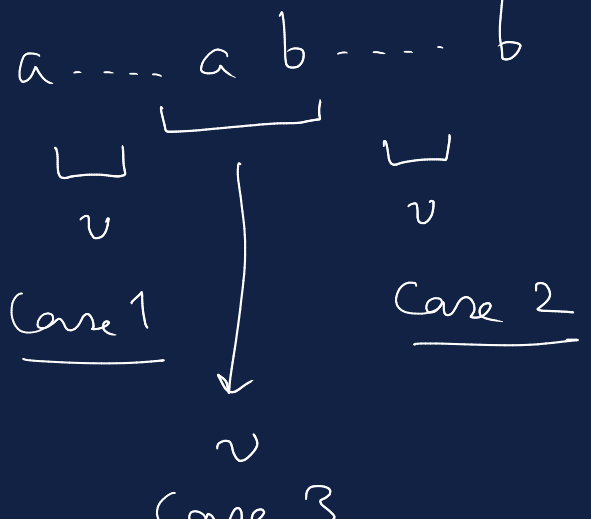
The proof fails.

Case 3



Case 1 Case 2

$\alpha'' = uv^2w$



Case 1:

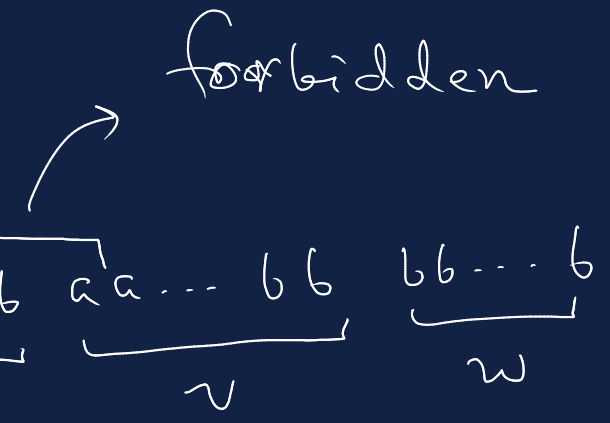
$\#a(\alpha'') > \#b(\alpha'')$ ↙

Case 2:

$\#a(\alpha'') < \#b(\alpha'')$ ↙

Case 3: α'' contains the substring ba.

$\alpha'' \notin L$ ↙



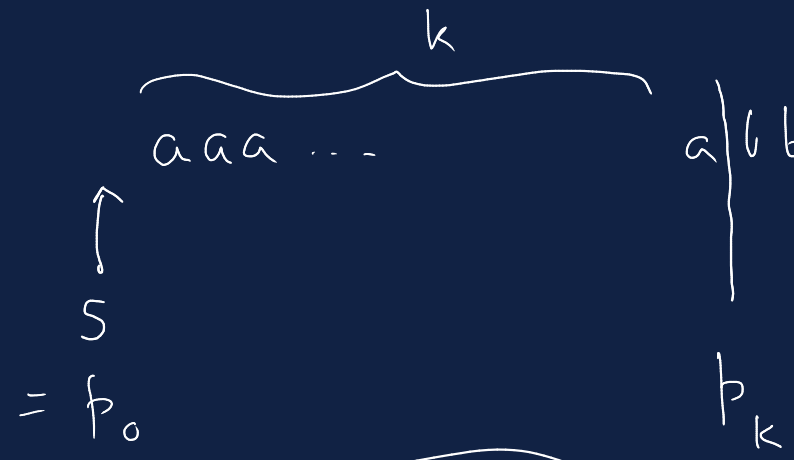
No such D can exist

$\Rightarrow$ L is not regular.

Simplified proof

$\alpha = a^k b^k$ ⟵ better than $a^{\lceil k/2 \rceil} b^{\lceil k/2 \rceil}$

$|\alpha| = 2k \geq k+1$



$\alpha = uvw$

$|uw| \leq k$

$1 \leq |w| \leq k$

pump out v

$i=0 \longrightarrow \alpha' = uw$

pump in v

$\alpha'' = uv^2w$

$i=2$

Both lead to contradiction

$i=1$

$\alpha_1 = \alpha$

$\alpha_i = uv^iw \in L$ for all $i \geq 0$.

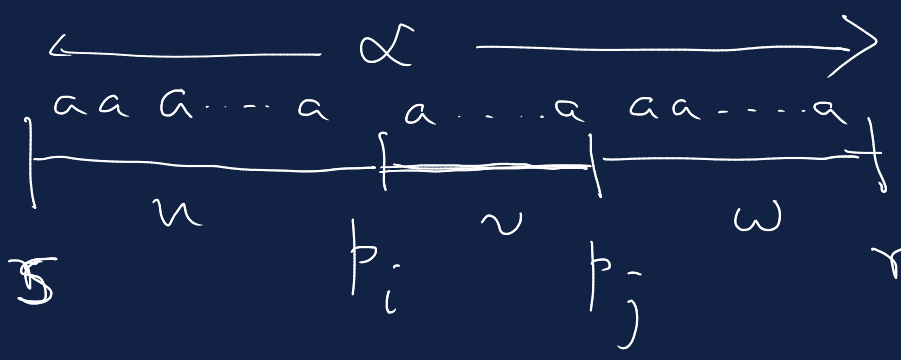
Example : $L = \{ a^{n^2} \mid n \geq 0 \}$

$= \{ \epsilon, a, aaaa, aaaaaaaaa, \ldots \}$

$\alpha(D) = L$ $\quad k \rightarrow$ # states of D. $(k \in \mathbb{N})$

$\alpha = a^{k^2} \in L \Rightarrow D$ accepts α.

$|\alpha| = k^2 \geq k$



$p_0, p_1, p_2, \ldots, p_{k^2}$

$k^2 + 1 \geq k + 1 > k$

PHP : $p_i = p_j$ $\quad i < j$

$v = a^l, \quad l \geq 1$

$\alpha_i = a^{k^2-l}\, a^{il}$ is accepted by D for all $i \geq 0$.

$\alpha_2 = a^{k^2-l}\, a^{2l} = a^{k^2+l}$ is accepted by D.

$1 \leq l \leq k$

$k^2 + l \leq k^2 + k < (k+1)^2$

D accepts α_2 which is not of the form a^{n^2}

Pumping Lemma (for regular languages)

Let L be a regular language. Then there exists a positive constant integer k (→ pumping lemma constant (PLC)) such that for any string $xyz \in L$ with $|y| \geq k$, we have the decomposition

$$y = uvw$$

satisfying the following three conditions:

(1) $|v| > 0$ (non-empty)

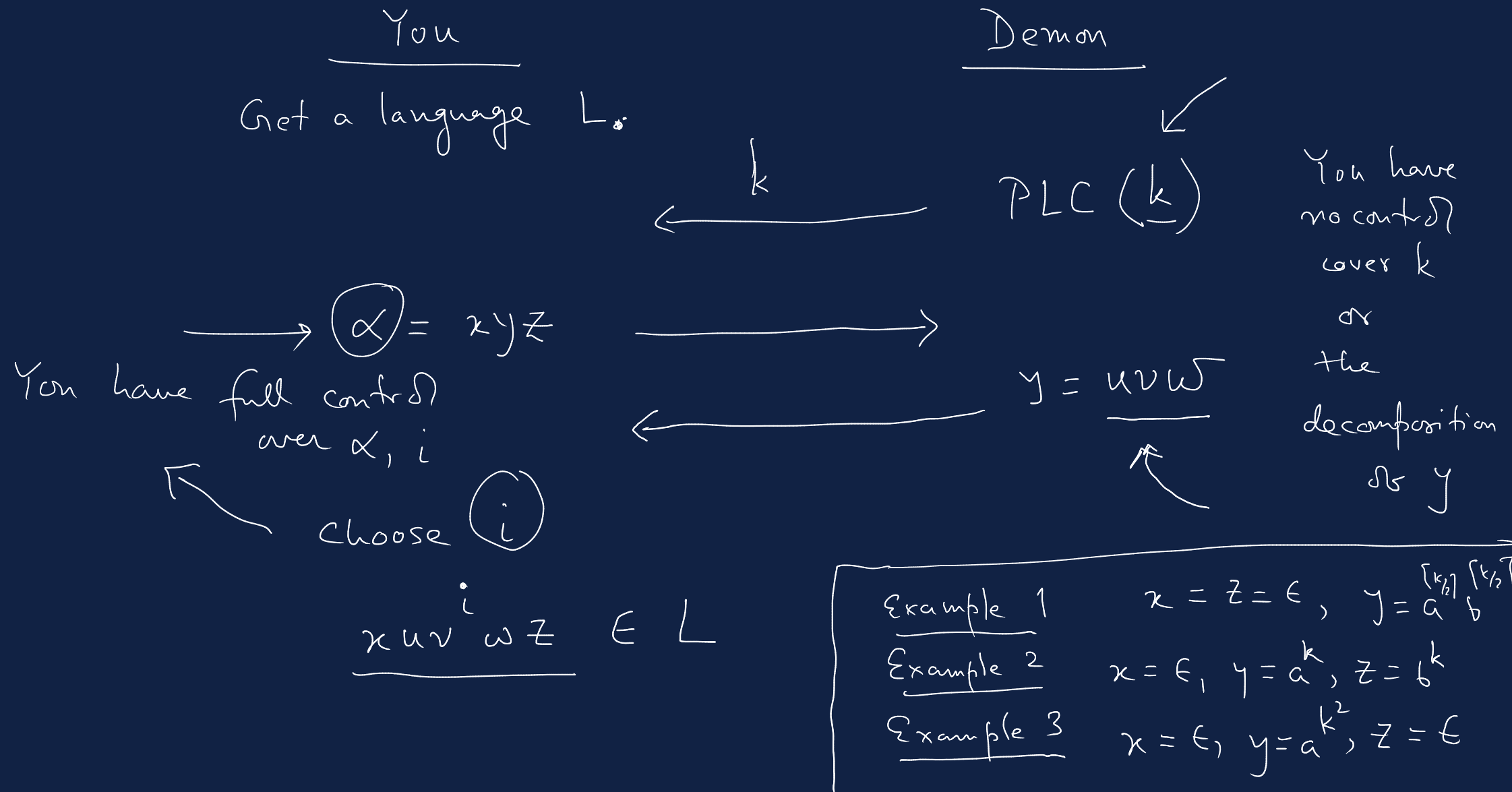
(2) $|uv| \leq k$

(3) $xuv^i wz \in L$ for all $i \geq 0$.

v → pumped out once
→ pumped in as many times as we want.

Proof: Do it.

Game with a demon



Example 1 $x = z = \epsilon$, $y = a^{\lceil k/2 \rceil} b^{\lceil k/2 \rceil}$

Example 2 $x = \epsilon$, $y = a^k$, $z = b^k$

Example 3 $x = \epsilon$, $y = a^{k^2}$, $z = \epsilon$