The Pumping Lemma

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

Suppose we have a potential DFA that supposedly recognizes L.

PIGEON-HOLE PRINCIPLE
FORMAL STATEMENT of the PUMPING LEMMA:

Let L be a regular language.

$\exists p > 0 \in \mathbb{N}$ $\forall w \in \Sigma^*$ if $|w| \geq p$

$\exists x, y, z \in \Sigma^*$ $w = xyz$, $|xy| \leq p$, $|y| > 0$

$\forall i \in \mathbb{N}$ $xy^iz \in L$

Proof Idea: Given a DFA for L choose p to be strictly greater than the number of states in the DFA.

If $|w| \geq p$ $w \in L$ then on the corresponding accepting state q must hit the same state twice on which reading the first p letters of w.

Every finite language is regular.

L regular $\Rightarrow$ L can be pumped

It does NOT say

L can be pumped $\Rightarrow$ L regular.

CONTRAPOSITIVE:

L cannot be pumped $\Rightarrow$ L is regular.

Suppose $L = \{a^n \mid n \in \mathbb{N}\}$

$\forall p \in \mathbb{N}$ $\exists w \in L$ $|w| \geq p$

$\forall x, y, z \in \Sigma^*$ with $w = xyz$, $|xy| \leq p$, $|y| > 0$

$\exists i \in \mathbb{N}$ $xy^iz \notin L$

$\Rightarrow$ L is not regular.

Use this NOT to disprove the statement: If pumping fails $\frac{\text{yes}}{\text{no}}$ and the third $\frac{\text{yes}}{\text{no}}$ then L is regular.

Try the Σ pumping lemma. Pumping the Σ pumping lemma. You must come up with a winning strategy.

Choose first letter to be a prime represented by a symbol. Every prime must be explicit. The divisor is never an explicit. The divisor is never stored in the state. Pumping by an indeterminate divisor.

Your last move must specify a witness for all cases.

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

Choose $p = 2$.

(a) Given choose $|w| \geq 2$.

(b) Given choose $w = a^2 b^2$

(c) The choice is constrained by $|xy| \leq 2$. The choice is constrained by $|y| > 0$. The choice is constrained by $x = a^n$ for $n \geq 0$. $y = a^m$ for $m \geq 1$, $z = b^2$.

(d) I choose $i = 2$

$$xy^2z = a^n a^{2m} b^2$$
$$= a^{n+2m} b^2$$

Then L is not regular.

EXAMPLE 2: $L = \{a^n \mid n \text{ is a prime number}\}$

Choose $p = 2$.

Choose $w = a^2$ where $|w| \geq p$, w is a prime.

Given w I need $y = a^m$ where $0 < m \leq p$

I pick $i > 1$, exact choice is deferred.

Given w is a prime $\Rightarrow$ $|w|$ is odd. Given $i > 1$ $|w|$ is even.

$a^{|w|+(i-1)|y|} = a^{|w|(1+(i-1))}$ not a prime number so L is not regular.

EXAMPLE 3: $L = \{a^n b^n \mid n \in \mathbb{N}\}$

Hard to do directly with the pumping lemma.

L is actually a big union

$L = \bigcup_{n \in \mathbb{N}} \{a^n b^n\} = \bigcup_{n \in \mathbb{N}} \{a^n\}$

This is not regular as L is not regular.

EXAMPLE 4: $L = \{a^n b^n \mid n > 1\}$

Pick choose $p = 2$.

Choose choose $w = a^2 b^2$.

Pick choose $y = a^2 \in a^+ b^+$

Pick choose $i = 0$

resulting $= a^2 b^2 b^{2i}$ $\Rightarrow$ L is not regular.

EXAMPLE 5: $L = \{a^n b^n \mid n \in \mathbb{N}\}$

I will choose L is not regular.

$L = a^n b^n$

Given choose p.

I choose $\geq p+1$, p a prime $\in \mathbb{N}$

$w = a^{2p} b^{2p}$

Given w I have to choose $y = a^k$ $0 < k \leq p$.

I choose $i = 0$ so now

$xz = a^{2p+p} b^{2p}$

$p \cdot k > (p+1) \cdot k > 0$

$\gcd(2p+k, p) = 1$

$xz \notin a^+ b^+$ $\Rightarrow$ L is not regular.

EXAMPLE 7: $L = \{\varepsilon^n \mid n \in \mathbb{N}\}$

$L = \{\varepsilon, \varepsilon\varepsilon, \varepsilon\varepsilon\varepsilon, \ldots\}$

Given pick p.

Choose pick ε^p

Given pick $x, y, z \in \Sigma^*$ $|xy| \leq p$

$|y| > 0$ $xz \in L$

$\Rightarrow y = \varepsilon^k$ $\varepsilon^{p-k} \in L$ $0 < k \leq p$

Choose pick $i = 2$

$xy^2z = \varepsilon^p$

$\varepsilon^{p+k} \in \varepsilon^+ \varepsilon^+$ $\varepsilon^{2p} \in \varepsilon^+ \varepsilon^+$ $\varepsilon^{2p+k} \in \varepsilon^+ \varepsilon^+$

ε^p is actually between two consecutive powers of 2 hence it cannot be a power of 2.

L is not regular.

FOLLOW UP: Given $\Sigma \subseteq \mathbb{N}$ we define winning$(S) = \{\varepsilon^n \mid n \in S\}$

winning$(S) = \{\varepsilon^n \mid n \in \mathbb{N}\}$ $\frac{\text{yes and no}}{\text{no}}$ $\frac{\text{yes}}{\text{no}}$

If winning(S) is regular then winning(S) have to be regular?

No! $S = \{2^n \mid n \in \mathbb{N}\}$

winning$(S) = \varepsilon^*$

winning(S) we just showed is not regular.

What about the other way?

KLEENE ALGEBRAS

Ring?

Semi-ring: Rock with 2 operations

S: carrier of the semi-ring

$+ : S \times S \to S$

$\times : S \times S \to S$

$0 : S$, $1 : S$

$(S, +, 0)$ commutative monoid

$(S, \times, 1)$ monoid

$\times$ distributes over $+$

0 annihilates with $\times$

$x \times 0 = 0 \times x = 0$

If $(S, +, 0)$ forms a group then we have a ring.

Ex 1 $(\mathbb{N}, 0, 1, +, \times)$ semi-ring

$(\mathbb{Z}, 0, 1, +, \times)$ ring

$E \subseteq \Sigma : \{x \mid x \in \Sigma\}$, $\{\varepsilon, \cdot\}$

Ring of Cartesian Products.

Ex 2 Given rock $\mathbb{N}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ multiply by matrix multiplication & add component wise

Ex 3 An idempotent semi-ring S is a semi-ring s.t.

$\forall x \in S$ $x^2 = x$.

$(T, \vee, \wedge)$

Ex 4 If have ring semi-ring the set of $n \times n$ matrices form a semi-ring.

Def Kleene Algebra

$K = (S, +, \cdot, 0, 1, *)$

$(S, +, 0)$ commutative monoid

$(S, \cdot, 1)$ monoid

$(S, +, \cdot, 0, 1)$ forms an idempotent semi-ring.

semi-ring $\times$ now $\cdot$ operator.

$1 + a a^* = a^*$

$1 + a^* a = a^*$

We introduce a partial order

$a \leq b := a + b = b$

(You need to check that this is really a partial order, say $\leq$)

a b c

$b + ac \leq c \Rightarrow a^* b \leq c$

$b + ca \leq c \Rightarrow b a^* \leq c$

Examples

① Let Σ be a finite alphabet

S = regular languages $\subseteq \Sigma^*$

$+$ = $\cup$

$\cdot$ = concatenation

$*$ = Kleene star

② S any set $\& B$ $\&$ the collection of binary relations $S \times S$

$+$ union

$\cdot$ relational composition

$x \cdot y$ is now $(x \circ y) \circ x$

$x(a,b) = 3y \in S$ $x(a,y)$ & $y(y,b)$

0

$1 = \{(x,y) \mid x \in S\}$

x^* reflexive transitive closure of x.

$x \cdot x^* y$ JoeM, $B_1 - B_2 \Rightarrow$

$x \cdot B_1 + B_2 \cdot B_1 \Rightarrow B_1 + B_2 \cdot B_1 \Rightarrow B_1 + B_2 \cdot B_1$

Equation $a b x + K = x$ unsolvable

solve for x.

$a^* b$ is the "smallest" solution.

$a \cdot a^* b + b = (a \cdot a^* + 1) b$

$= a^* b$

If K is a unique solution the $a^* b \in K$.

Example: Let K a any Kleene algebra define $M_n(K)$ to be $n \times n$ matrices with entries in K.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & \ldots \\ \ldots & \ldots \end{pmatrix}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + b'c & \ldots \\ \ldots & \ldots \end{pmatrix}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} (a+bd^*c)^* & (a+bd^*c)^* bd^* \\ (d+ca^*b)^* ca^* & (d+ca^*b)^* \end{pmatrix}$

Now we can solve matrix-vector equations

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} X + \begin{pmatrix} e \\ f \end{pmatrix}$$

matrix vectors

This can be used to construct the regular expression associated with a DFA.

Dexter Kozen has developed & extended the theory immediately including probabilistic extensions.