CS310M: Automata Theory (Minor)

~~Topic 5: Minimizing DFA~~

Topic 6: Pumping Lemma.

Paritosh Pandya

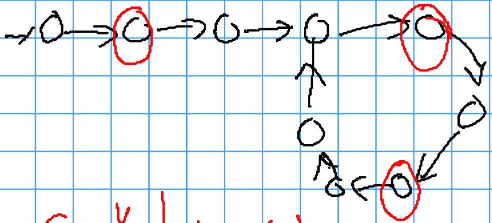
Indian Institute of Technology, Bombay

Course URL: https://cse.iitb.ac.in/∼pandya58/CS310M/automata.html

Autumn, 2021

DFA of a Unary Language

$\Sigma = \{a\}$



$L = \{a^k \mid k \in U \subseteq \mathbb{N}\}$

$U = \{1, 4, 6, 9, 11, \dots\}$

Ultimately Periodic

$\exists n, p.$

$\forall m > n.\ m \in U \iff m + p \in U$

Proving Non-regularity

- Are all languages regular?

Proving Non-regularity

- Are all languages regular?
- $L_1 = \{a^n b^n \mid n \geq 0\}$.

Proving Non-regularity

- Are all languages regular?
- $L_1 = \{a^n b^n \mid n \geq 0\}$.
- Powers of 2 in Binary: $L_2 = \{x \in \{0,1\}^* \mid \hat{x} \text{ is power of } 2\}$.
  Powers of 2 in Unary: $L_3 = \{1^j \mid j \text{ is power of } 2\}$.

Proving Non-regularity

- Are all languages regular?
- $L_1 = \{a^n b^n \mid n \geq 0\}$.
- Powers of 2 in Binary: $L_2 = \{x \in \{0,1\}^* \mid \hat{x} \text{ is power of } 2\}$.
  Powers of 2 in Unary: $L_3 = \{1^j \mid j \text{ is power of } 2\}$.
- How can we tell whether a language is regular?

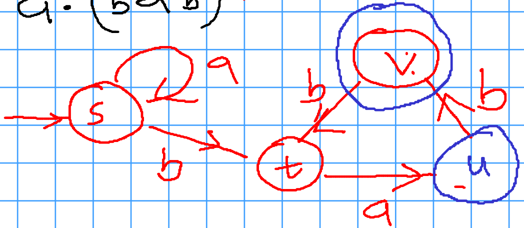
Proving Non-regularity

- Are all languages regular?
- $L_1 = \{a^n b^n \mid n \geq 0\}$.
- Powers of 2 in Binary: $L_2 = \{x \in \{0,1\}^* \mid \hat{x} \text{ is power of } 2\}$.
  Powers of 2 in Unary: $L_3 = \{1^j \mid j \text{ is power of } 2\}$.
- How can we tell whether a language is regular?
- To show that L is regular give ϵ-NFA or Regular expression for it.

- Are all languages regular?
- $L_1 = \{a^n b^n \mid n \geq 0\}$.
- Powers of 2 in Binary: $L_2 = \{x \in \{0,1\}^* \mid \hat{x} \text{ is power of } 2\}$.
  Powers of 2 in Unary: $L_3 = \{1^j \mid j \text{ is power of } 2\}$.
- How can we tell whether a language is regular?
- To show that L is regular give ϵ-NFA or Regular expression for it.
- Proving Non-regularity: Pumping lemma and Myhill-Nerode Theorem.

$a^* \cdot (bab)^+$

$A^+ = A \cdot A^*$



Word aababbab $\in L$

Run:

$s \xrightarrow{a} s \xrightarrow{a} s \xrightarrow{b} t \xrightarrow{a} u \xrightarrow{b} v \xrightarrow{b} t \xrightarrow{a} u \xrightarrow{b} v$

$s \xRightarrow{aab} t \xRightarrow{abb} t \xRightarrow{ab} v$

Key Idea

- Consider a long word w recognized by a DFA with n states. In the run some state must repeat. (Why?)

Key Idea

- Consider a long word w recognized by a DFA with n states. In the run some state must repeat. (Why?)
- How long should w be for this to happen?

Key Idea

- Consider a long word w recognized by a DFA with n states. In the run some state must repeat. (Why?)
- How long should w be for this to happen? $|w| \geq n$
- String between repeating state can be pumped any number of times.

$$s \xRightarrow{x} q \xRightarrow{v} q \xRightarrow{y} f$$
$$s \xRightarrow{x} q \xRightarrow{v} q \xRightarrow{v} q \xRightarrow{y} f$$

$\hat{\delta}(q, x) = t \iff q \xRightarrow{x} t$

Key Idea

- Consider a long word w recognized by a DFA with n states. In the run some state must repeat. (Why?)

- How long should w be for this to happen?
- String between repeating state can be pumped any number of times.
  $s \xrightarrow{x} q \xrightarrow{v} q \xrightarrow{y} f$
  $s \xrightarrow{x} q \xrightarrow{v} q \xrightarrow{v} q \xrightarrow{y} f$

  $w \in L$
- Let $w = x \cdot y \cdot z$ s.t. $|y| \geq n$. Some state during the y part of the run must repeat.

Key Idea

- Consider a long word w recognized by a DFA with n states. In the run some state must repeat. (Why?)

- How long should w be for this to happen?
- String between repeating state can be pumped any number of times.
  $s \xrightarrow{x} q \xrightarrow{v} q \xrightarrow{y} f$
  $s \xrightarrow{x} q \xrightarrow{v} q \xrightarrow{v} q \xrightarrow{y} f$
- Let $w = x \cdot y \cdot z$ s.t. $|y| \geq n$. Some state during the y part of the run must repeat.
- We can break $y = u \cdot v \cdot w$ s.t. state before and after v is the same. Thus, the run has the form
  $s \xrightarrow{x} \underbrace{q_1 \xrightarrow{u} q_2 \xrightarrow{v} q_2 \xrightarrow{w} q_3}_{y} \xrightarrow{z} f.$

Key Idea

- Consider a long word w recognized by a DFA with n states. In the run some state must repeat. (Why?)
- How long should w be for this to happen?
- String between repeating state can be pumped any number of times.
  $s \xrightarrow{x} q \xrightarrow{v} q \xrightarrow{y} f$
  $s \xrightarrow{x} q \xrightarrow{v} q \xrightarrow{v} q \xrightarrow{y} f$
- Let $w = x \cdot y \cdot z$ s.t. $|y| \geq n$. Some state during the y part of the run must repeat.
- We can break $y = u \cdot v \cdot w$ s.t. state before and after v is the same. Thus, the run has the form
  $s \xrightarrow{x} q_1 \xrightarrow{u} q_2 \xrightarrow{v} q_2 \xrightarrow{w} q_3 \xrightarrow{z} f.$
- The string between repeating states can be pumped arbitrary number of times.
  $s \xrightarrow{x} q_1 \xrightarrow{u} q_2 \xrightarrow{v} q_2 \xrightarrow{v} q_2 \xrightarrow{w} q_3 \xrightarrow{z} f.$

Pumping Lemma

Given language L

If L is regular then

$\exists n > 0$ such that

$\forall \;\; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$

$\exists \;\; u, v, w$ s.t. $y = u \cdot v \cdot w$ and $|v| > 0$ s.t.

for all $0 \leq i \;\; (x \cdot u \cdot v^i \cdot w \cdot z \in L)$.

$$\frac{P \Rightarrow Q \qquad \neg P}{\neg Q \Rightarrow \neg P}$$

Contraposition

Pumping Lemma

Given language L

If L is regular then
$\exists n > 0$ such that
$\quad\forall\; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$
$\quad\quad\exists\; u, v, w$ s.t. $y = u \cdot v \cdot w$ and $|v| > 0$ s.t.
$\quad\quad\quad$ for all $0 \leq i\;\; (x \cdot u \cdot v^i \cdot w \cdot z \in L)$.

Contra-positive Form

For a given language L
If $\forall n > 0$ s.t.
$\quad\exists\; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$ s.t.
$\quad\quad\forall\; u, v, w$ with $y = u \cdot v \cdot w$ and $|v| > 0$ we have
$\quad\quad\quad(\exists i \geq 0$ s.t $x \cdot u \cdot v^i \cdot w \cdot z \notin L)$
then L is not regular

Pumping Lemma

Given language L

If L is regular then
$\exists n > 0$ such that
$\forall \; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$
$\exists \; u, v, w$ s.t. $y = u \cdot v \cdot w$ and $|v| > 0$ s.t.
for all $0 \leq i \; (x \cdot u \cdot v^i \cdot w \cdot z \in L)$.

$\Big\}\, P$

Contra-positive Form

For a given language L
If $\forall n > 0$ s.t.
$\exists \; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$ s.t.
$\forall \; u, v, w$ with $y = u \cdot v \cdot w$ and $|v| > 0$ we have
$(\exists i \geq 0$ s.t $x \cdot u \cdot v^i \cdot w \cdot z \notin L)$
then L is not regular

Pumping Lemma in contrapositive form is used to prove that some languages are not regular.

Proving non-regularity

Contra-positive Form

For a given language L

If $\forall n > 0$ s.t.

$\exists \; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$ s.t.

$\forall \; u, v, w$ with $y = u \cdot v \cdot w$ and $|v| > 0$ we have

$(\exists i \geq 0$ s.t $x \cdot u \cdot v^i \cdot w \cdot z \notin L)$

then L is not regular

Proving non-regularity

Contra-positive Form

For a given language L

If $\forall n > 0$ s.t.

$\exists \; x, y, z$ with $x \cdot y \cdot z \in L$ and $|y| \geq n$ s.t.

$\forall \; u, v, w$ with $y = u \cdot v \cdot w$ and $|v| > 0$ we have

$(\exists i \geq 0$ s.t $x \cdot u \cdot v^i \cdot w \cdot z \notin L)$

then L is not regular

Game with Demon

Given language L

- Demon claims L is regular and chooses n.
- You choose a string $xyz \in L$ with $|y| \geq n$.
- Demon partitions $y = uvw$ with $|v| \neq 0$.
- You show that $xu(v^i)wz \notin L$ for some i for your choice.

Example

$L_1 = \{a^k b^k \mid k \geq 0\}$ is not regular.

Proof: Pumping Lemma.

- Demon chooses n.
- $a^n b^n \in L$ $\quad x = \epsilon,\ y = a^n,\ z = b^n$
- $y = a^p . a^q . a^r$ $\quad u = a^p,\ v = a^q,\ w = a^r$
  $\quad\ \ u\ \ v\ \ w$ $\quad p + q + r = n,\ q > 0$
- Choose Pumping Factor 2

$$\epsilon . a^p . a^q . a^q . a^r b^n \notin L$$

$$p + q + q + r = n + q,\ q > 0$$

$\therefore$ L is not regular.

Demon

(me)

Demon

Example

$L_2 = \{w \cdot w \mid w \in \{a, b\}^*\}$ is not regular.

Proof:

$L_3 = \{w \cdot w \mid w \in \{a\}^*\}$

. Demon n

. You chose $x = \epsilon$, $y = a^n$, $z = b \cdot a^n b$

Example

$L = \{a^{2^i} \mid i \geq 0\}$ Powers of 2 in unary

- Demon n
- You $w = a^{2^p}$ where $2^p > n$

$w = x \cdot y \cdot z$ where $x = \epsilon$, $y = a^n$, $z = a^r$

$\therefore$ $y' = a^{n+d}$ $n \geq d > 0$.

$a^{n+d} a^r$ $n+d+r = 2^p$

Example

$L_3 = \{a^i \mid i \text{ is prime}\}$ is not regular.

Proof:

Given n, let i is prime s.t. $i \geq n$

$x = \varepsilon$, $y = a^i$, $z = \varepsilon$

Let $y = u.v.w$ for some u, v, w

then, let $v = a^k$,

where if k is odd, $uv^2w = a^{even}$

M1: if k is even, let m be a prime s.t. $k \not\equiv 0 \bmod m$.

Then $\exists N$ s.t. $kN \equiv -(n-k) \bmod m$

M2: $uv^{i+1}w = a^{2i}$