§1 05-07

Lemma 1.1 (Pumping Lemma)

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

Not possible to recognize this language with finite automaton because it would require unbounded memory. Non regular languages could recognize this.

Suppose we have putative (generally considered or reputed to be) DFA that recognizes L. Then we can pick a word with a block of a with length greater that the number of states in the machine. This means that the machine will have to repeat a state. This rests on the pigeon hole principle.

The idea is that now you can exploit this loop as many times as you'd like by inserting the string that brings you about the loop.

Now for the lemma. Let L be a regular language. Then

$$\exists p > 0 \text{ such that } \forall w \in \Sigma^* \mid w \in L \wedge |w| \geq p$$
$$\exists x, y, z \in \Sigma^* \text{ such that } w = xyz,\ |xy| \leq p,\ |y| > 0$$
$$\forall i \in \mathbb{N},\ xy^i z \in L$$

An intuition for this is that y is the word that takes you through the loop, so you can repeat it as many times as you'd like.
Given a DFA for L choose p to be strictly greater than the number of states in the DFA. If $|w| \geq p \wedge w \in L$ then as the automaton changes state it must hit the same state twice while reading the first p letters, when p is greater than the number of states in the machine. □

Definition 1.2 (Finite Language)**.** A finite language is one containing a finite number of words.

Fact 1.3. Every finite language is regular. The p that you choose is longer than any word in the language. So then a finite language would have no words of length greater than p.

Fact 1.4. L regular $\Rightarrow$ L can be pumped. Contrapositive is that L cannot be pumped $\Rightarrow$ L not regular.

Note that it is not true that L can be pumped $\Rightarrow$ L regular.

Lemma 1.5 (Pumping Lemma Contrapositive)

$$L \subseteq \Sigma^* \ s.t. \ \forall p > 0$$
$$\exists w \in L \ with \ |w| \geq p \ s.t.$$
$$\forall x, y, z \in \Sigma^* \ with \ w = xyz, \ |xy| \leq p \wedge |y| > 0$$
$$\exists i \in \mathbb{N} \ s.t. \ xy^i z \notin L$$
$$\Rightarrow L \text{ is not regular}$$

Use games to deconstruct this statement. You and the devil. You play the $\exists$ quantifiers, and the devil plays the $\forall$ quantifiers. You must come up with a strategy to win every game.

The obvious first move is represented by a symbolic p. Your first move is explicit. The devil's move in step 3 must be analyzed by an exhaustive case analysis. Your last move must specify a response for all cases.

Example 1.6
$L = \{a^n b^n \mid n \geq 0\}$

1. Demon choses $p > 0$
2. You chose $w = a^p b^p$
3. The devil is constrained by $|xy| \leq p$ to choose y to consist exlucisvely of a's. So $y = a^k$ for some $0 < k \leq p$.
4. I choose $i = 2$. Didn't quite catch the rest

Thus L is not regular.

Example 1.7
$L = \{a^q \mid q \text{ a prime number}\}$

Demon picks $p > 0$. I pick a^n where $n > p$, n is a prime. Demon has to pick $y = a^k$ where $0 < k \leq p$. I pick $i > 1$, deferring the exact choice. New string $xy^i z$ is $a^{n+(i-1)k}$. Choose $i = n + 1$. Then $a^{n+nk} = a^{n(1+k)}$ which is not a prime number so L is not regular.

Example 1.8

$L = \{a^n b^m \mid n \neq m\}$

Wants you have a stock of languages that you know are not regular, you don't always have to do pumping. This example is hard to do directly with the pumping lemma.

$\overline{L}$ (L complement) is a big mess. But $\overline{L} \cap a^* b^* = \{a^n b^n \mid n \geq 0\}$. This is not a regular language to L is not regular.

Example 1.9

$L = \{a^i b^i \mid i > j\}$.

Example 1.10

$L = \{x + y = z \mid xyz \in \{0,1\}^* \wedge \text{the equation is valid}\}$

Demon picks p. I pick

$$\underbrace{111 \cdots 1}_{p}$$

Definition 1.11. If $S \subseteq \mathbb{N}$, define $unary(S) = \{1^n \mid n \in S\}$. $binary(S) = \{w \in \{0,1\}^* \mid w \text{read as a binary number is in} S\}\}$

If $binary(S)$ is regular does that mean $unary(S)$ is regular? No. Consider $S = \{2^n \mid n \geq 1\}$. Then binary is regular because 100^* is clearly regular. $unary(S) = \{1^{2^p}\}$ is not regular because you can pump to a non power of 2.

§1.1 Kleene Algebras

Definition 1.12 (Semi-ring)**.** A set with 2 operations. S: the carrier of the semi-ring. $+ : S \times S \to S$. $\times : S \times S \to S$. $0 : S$, $1 : S$. $(S, +, 0)$ forms a commutative monoid. $(S, x, 1)$ forms a monoid. $\times$ distributes over $+$. 0 annihilates with x i.e. $a \times 0 = 0 \times a = 0$.

Semi-ring is similar to a ring, but doesn't require that each element has an additive inverse. i.e. if $(S, +, 0)$ forms a group then it produces a ring instead of a semi-ring.

Example 1.13

$(\mathbb{N}, 0, 1, +, \times)$. This forms a semi ring, because we don't have the negative integers for the additive inverses. $(\mathbb{Z}, 0, 1, +, \times)$ would form a ring.

$\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z},\ i^2 = -1\}$ is the ring of Gaussian integers.

Example 1.14

$n \times n$ matrices over $\mathbb{N}$. Multiply by matrix multiplication and add componentwise.

Example 1.15

An idempotent semiring J is a semi ring such that $\forall x \in J, x^2 = x$. $(T, F, \vee, \wedge)$.

idempotent is an element which is unchanged in value when multiplied or otherwise operated on by itself.

Example 1.16

If we have any semiring, the set of $n \times n$ matrices with entries in this semiring form a semi-ring.

Definition 1.17 (Kleene Algebras). $K = (S, +, \cdot, 0, 1, *)$.

1. $(S, +, 0)$: commutative monoid
2. $(S, \cdot, 1)$: monoid
3. $(S, +, \cdot, 0, 1)$ forms an idempotent semiring.
4. $$1 + aa^* = a^*$$ $$a + a^* a = a^*$$
5. We introduce a partial order $a \leq b := a + b = b$ (check that this is really a partial order). 2 rules.
$$b + ac \leq c \Rightarrow a * b \leq c$$ $$b + ca \leq c \Rightarrow ba^* \leq c$$

Example 1.18

Let Σ be a finite alphabet $S =$ regular languages $\subseteq \Sigma^*$. $+$ is union. $\cdot$ concatenation. $*$ is kleene star.

Example 1.19

S any set and R the collection of binary relations on S. A binary relation $r \subseteq S \times S$. $+$ is union. $\cdot$ is relational composition. xry means $(x, y) \in r$. $x(r \cdot s)y = \exists z s.t. xrz \wedge zsy$. $0 := \varnothing$. $1 := \{(s, s) \mid s \in S\}$. r^* is the reflexive, transitive closure of r.

graphs are a nice way of picturing relations. r^* is reflexive, transitive closure of r. transitive closure let's you take the paths of the graph. And everything is related to itself. Directed graph because not necessarily symmetric. xr^*y if $\exists n \in \mathbb{N}, z_1, \cdots, z_n s.t. xrz_1 \wedge z_1 r z_2 \cdots z_n r y$. i.e. there exists a path from x to y.

Solving for x. $ax + b = x$. a^*b is the smallest solution. $aa * b + b = (aa * +1)b = a^*b$. Smallest solution means that if x is another solution, then $a^*b \leq x$.

Example 1.20

If K is any kleene algebra, $M_n(K)$ is $n \times n$ matrices with entries in K. Do operations as you would expect about matrices. What the heck is star though? 0 is 0. 1 is 1 along diagonal and 0 everywhere else.

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