§1. Right-linear Grammars & NFAs

Let $L(\text{REX})$ be the class of all languages that can be described by regular expressions, $L(\text{RLG})$ those that can be generated by right-linear grammars, and $L(\text{NFA})$ (resp. $L(\text{OAS-NFA})$) those that can be recognized by NFAs (resp. DFAs).

Our main aim in this chapter is to first show that $L(\text{RLG}) = L(\text{NFA}) = L(\text{OAS-NFA}) = L(\text{REX})$.

We have already seen that $L(\text{DFA}) = L(\text{NFA})$ because every DFA is a special NFA, so $L(\text{DFA}) \subseteq L(\text{NFA})$; and every NFA is equivalent to a DFA, so $L(\text{NFA}) \subseteq L(\text{DFA})$.

Prop. 1. Let $M = \langle Q, T, \Delta, q_0, A \rangle$ be an NFA. Then we can find an RLG $G = \langle V, T, S, \Rightarrow \rangle$ such that $L(G) = L(M)$.

Proof: Let $V = \emptyset$ and $S = q_0$. The productions in $\Rightarrow$ are constructed from $M$ as follows:

For each $B \in \Delta(M)$ in $M$, we get the production $B \Rightarrow \lambda$.

Also each transition $A \xrightarrow{a} B$ or $A \xrightarrow{a} \lambda$ in $M$, we get the production $A \Rightarrow aB$ or resp. $A \Rightarrow B$.

From the construction of $G$ we can see that $w \in L(M)$ if and only if we can lead you from $q_0$ to an accepting state in $M$ if and only if there is a derivation of $w$ from $S$ in $G$ if and only if $w \in L(G)$. So $d(6)-6$. 
Ex. 10. Let $M$ be the NFA shown on the right.

Then an equivalent RLG $G$ will be as shown below.

$\rightarrow A, A \rightarrow aB, B \rightarrow bB, B \rightarrow C, C \rightarrow aC, C \rightarrow bA, C \rightarrow \lambda$.

Let us consider the string $\psi = abba$. In $M$, $\psi$ is accepted as follows: $\rightarrow A \rightarrow aB \rightarrow B \rightarrow B \rightarrow C \rightarrow C$.

In $G$, $\psi$ can be derived from $A$ as follows.

$\rightarrow A \rightarrow aB \rightarrow abB \rightarrow abbB \rightarrow abbbC \rightarrow abbaC \rightarrow abba$.

Ex. 16. Let $M = \rightarrow$. Then an equiv.

RLG will be as shown below.

$\rightarrow B, B \rightarrow aA, A \rightarrow \lambda, A \rightarrow B, A \rightarrow bC, C \rightarrow \lambda, C \rightarrow bB, C \rightarrow aC$.

Notice that the number of productions in $G$ will be the number of transitions of $M$ plus the number of states in $A(M)$.

Prop. 2. Let $G = (V, T, \{S\}, \delta)$ be an RLG. Then we can find an NFA $M = (Q, T, \Delta, q_0, A)$ such that $L(M) = L(G)$.

Proof: Let $q_0 = S$. We will construct $Q$, $A$, and $\Delta$ from the productions of $G$ as follows. $Q$ will start out being $V$ - but more states will be added as we go along.
(a) For each production in $G$ of the form $B \rightarrow \lambda$, let $B \in A(M)$.
(b) For each production of the form $A \rightarrow B$ in $G$, add the transition $A \rightarrow B$ to $M$.
(c) For each production in $G$ of the form $A \rightarrow a_1 \ldots a_n B$, make an new state and add the transitions $A \rightarrow a_1 \rightarrow a_2 \rightarrow \ldots \rightarrow a_n \rightarrow B$ to $M$.
(d) Finally, make a specially designated accepting state $Z$ in $A(M)$ and for each production in $G$ of the form $A \rightarrow a_1 a_2 \ldots a_k B$, make an new state and add the transitions $A \rightarrow a_1 \rightarrow a_2 \rightarrow \ldots \rightarrow a_k \rightarrow B$ to $M$.

From the construction of $M$, we can see that $L(M) = L(G)$ because each derivation in $G$ of a string $q$ will correspond to an acceptance track of $q$ in $M$.

Ex. 2: Let $G$ be the RLG shown below.

\[ S \rightarrow abS, \quad S \rightarrow A, \quad A \rightarrow baB, \quad A \rightarrow aA, \quad A \rightarrow \lambda, \quad B \rightarrow cC, \quad B \rightarrow ba, \quad C \rightarrow ac, \quad C \rightarrow bC \]

Then an equivalent NFA $M$ will be as below.

![Diagram of NFA](Diagram.png)

The derivation $S \rightarrow abS \rightarrow ab\lambda A \rightarrow ab\lambda aA \rightarrow ab\lambda aI$ in $G$ corresponds to the acceptance track $S \rightarrow 1 \rightarrow \lambda S \rightarrow A \rightarrow A \quad$ in $M$.  

Def. Let $M = \langle Q, \Sigma, \delta, q_0, A \rangle$ be an NFA and $\varphi$ and $\psi$ be strings from $T^*$. Recall that the reaching set $R(\psi)$ is the set of all states that can be reached via $\psi$ when starting at $q_0$. We define the back-tracking set $B(\psi)$ by $B(\psi)$ is the set of all states from which you can start and reach an accepting state via $\psi$.

Qu.1 Given an RLG, $G$, how can we tell if it is ambiguous?

Ans.1 First convert the RLG, $G$, into an equivalent NFA $M$. Then find all the reaching sets and back-tracking sets of $M$. $G$ will be ambiguous $\iff$ there is a reaching set $R(\psi)$ and a back-tracking set $B(\psi)$ such that $|R(\psi) \cap B(\psi)| \geq 2$. The string $\psi\psi$ will have at least two leftmost derivations.

Qu.2 Given an ambiguous RLG, $G$, how can we find an equivalent unambiguous RLG, $G'$?

Ans.2 First convert the RLG, $G$, into an equivalent NFA. Then convert $M$ into an equivalent DFA, $M_{d}$. Finally, convert $M_{d}$ into an equivalent RLG, $G'$. Then $G'$ will be an unambiguous RLG which is equivalent to $G$. The ambiguity was removed in passing from the NFA to the DFA.
Ex.3 (a) Determine whether or not the RLG $G$ below is ambiguous.

$S \rightarrow bA$, $S \rightarrow bB$, $A \rightarrow aB$, $A \rightarrow b$, $A \rightarrow ab$, $B \rightarrow aB$, $B \rightarrow a$.

(b) If $G$ is ambiguous, find an equivalent un-ambiguous RLG, $G'$.

(a) M:

\[ \begin{array}{c}
\text{S} & \rightarrow & b & \rightarrow & A & \rightarrow & b \\
& \rightarrow & b & \rightarrow & B & \rightarrow & a \rightarrow & a \\
& & & \rightarrow & A & \rightarrow & a & \rightarrow & a \\
\end{array} \]

Reaching Sets:

- \{S\} \rightarrow \{A, B\} \rightarrow \{B, Z\} \rightarrow \{\phi\}
- \{S\} \rightarrow \{A\} \rightarrow \{\phi\}
- \{S\} \rightarrow \{\phi\}

Back-tracking Sets:

- \{A, B\} \rightarrow \{A, B\} \rightarrow \{B\} \rightarrow \{Z\}
- \{S\} \rightarrow \{S\} \rightarrow \{\phi\}
- \{S\} \rightarrow \{\phi\}

If we take $\psi = b$ and $\nu = a$, then we see that $R(\psi) = \{A, B\}$ and $B(\nu) = \{A, B\}$. Since

$|R(\psi) \cap B(\nu)| = |\{A, B\} \cap \{A, B\}| = |\{A, B\}| = 2 > 2$

it follows that $G$ is ambiguous. The string $bbaa$ will have at least 2 leftmost derivations in $G$. Indeed, we have:

- $S \Rightarrow bA \Rightarrow baB \Rightarrow baa$ (first leftmost derivation)
- $S \Rightarrow bB \Rightarrow baB \Rightarrow baa$ (2nd leftmost derivation)
(b) We already found the reaching sets of \( M \) in part (a). So it is now easy to find the DFA, \( M_0 \).

Now all we have to do is to convert \( M_0 \) into an equivalent RLG, \( G' \). To make this easier to understand, let \( C = \{ S \} \), \( D = \{ A, B \} \), \( E = \emptyset \), \( F = \{ B, Z \} \) and \( H = \{ \varepsilon \} \). Then \( G' \) is:

- \( C \rightarrow aE \), \( C \rightarrow bD \), \( D \rightarrow aF \), \( D \rightarrow bH \), \( E \rightarrow aE \), \( E \rightarrow bE \), \( F \rightarrow aF \), \( H \rightarrow aE \), \( H \rightarrow bE \), \( F \rightarrow \lambda \), \( H \rightarrow \lambda \),

and we are done. Note that the string \( yyp = baa \) has only one leftmost derivation in \( G' \) because there is only one path from \( \{ S \} = C \) to \( \{ B, Z \} = F \) via baa.

§2. Regular expressions & OAS-NFAs

**Definition.** An OAS-NFA is an NFA with only one accepting state which is different from the initial state.

It is easy to see that any NFA is equivalent to an OAS-NFA. All we have to do is to create a single new accepting state and add \( \lambda \)-transitions from the old accepting states to the single new one.
Prop 3: If $E$ is a regular expression, then we can find an OAS-NFA $M$ such that $L(M) = L(E)$. 

Proof: Recall that a regular expression over $(a_1, \ldots, a_n)$ is defined recursively as follows:
(a) $a_1, \ldots, a_n \lambda$ and $\emptyset$ are regular expressions.
(b) If $E_1$ and $E_2$ are regular expressions then so are $(E_1+E_2)$, $(E_1E_2)$, and $(E_1^*).

To find an OAS-NFA for a reg. expr. $E$, it will suffice to show how to make OAS-NFAs for the reg. expr. in (a); and given OAS-NFAs for $E_1$ & $E_2$, to show how to make OAS-NFAs for $(E_1+E_2)$, $(E_1E_2)$ and $(E_1^*)$.

(a) OAS-NFA for $a_i$:

(b) OAS-NFA for $\lambda$:

(c) OAS-NFA for $\emptyset$:

(b) OAS-NFA for $(E_1+E_2)$:

OAS-NFA for $(E_1E_2)$:

OAS-NFA for $(E_1^*)$: 
Ex.4 Find an OAS-NFA $M$ such that $L(M) = a^* (bc+ca)^*$

$(bc+ca)^*$

Ex.5 Find an OAS-NFA $M$ such that $L(M) = (\emptyset^*)$

Ans: $\emptyset = \text{[Diagram]}$, $(\emptyset^*) = \text{[Diagram]}$

Def: A generalized finite acceptor (GFA) is defined in the same manner as an NFA except that instead of having "$a" or "$\lambda" - transitions, we can have any regular expression serve as a transition.

Ex.6 Below is an example of a GFA
Proposition 4: Let $M$ be an NFA. Then we can find a regular expression $E$ such that $L(M) = E$.

Sketch of Proof: First we convert $M$ into an OAS-NFA $M_1$. Then we view $M_1$ as a GFA and remove the other states beside the initial state and accepting state, one at a time to get a sequence of equivalent simpler & simpler GFAs. At the end, we will get a GFA as shown below with only two states.

Then $L(M) = R_1^* R_2 (R_4 + R_3 R_5^* R_2)^*$.

Ex. 7. Find a regular expression for the language recognized by the NFA $M$ below.

Ans: This NFA is an OAS-NFA, so we don't have to convert it into an OAS-NFA. To view $M$ as a GFA, just add underlines under each transition.
§3

Now from Propositions 1, 2, 3 & 4, we can deduce our first main result.

**Theorem 5. (Main theorem for Regular languages)**

\[ L(RLG) = L(NFA) = L(DFA) = L(DAFS-NFA) = L(REX) \]

**Closure Theorems for regular languages.**

We will now explore some closure results about regular languages.

**Theorem 6. (Closure theorem for Regular languages)**

If \( L_1 \) & \( L_2 \) are regular languages, then so are also the following

(a) \( L_1 \cup L_2 \)  (b) \( L_1 \cdot L_2 \)  (c) \( L_1^* \)

(d) \( L_1^R \)  (e) \( L_1^c \)  (f) \( L_1 \cdot L_2 \)  (g) \( L_1 - L_2 \)

**Proof:** Since \( L_1 \) & \( L_2 \) are regular languages, then by definition, we can find regular expressions \( E_1 \) & \( E_2 \) such that \( L(E_1) = L_1 \) & \( L(E_2) = L_2 \)

Now \( (E_1 + E_2) \) is a regular expression which describes \( L_1 \cup L_2 \). So \( L_1 \cup L_2 \) is a regular language.
(b) \((E_1 \cdot E_2)\) is a regular expression which describes \(L_1 \cdot L_2\). So \(L_1 \cdot L_2\) is a regular language.

c) \((E_1^*)\) is a regular expression which describes \(L^*_1\). So \(L^*_1\) is a regular language.

d) Since \(L_1\) is a regular language, it follows from Theorem 5, the main theorem on reg. lang. that we can find an OAS-NFA \(M\) such that \(L(M) = L_1\).

Now if we make the initial state of \(M\) into the accepting, make the accept state of \(M\) into the initial state, and reverse the direction of each transition, we will get an OAS-NFA \(M^R\) with \(L(M^R) = L_1^R\). So by Theorem 5, \(L_1^R\) is a regular language.

e) First convert \(E_1\) into an equivalent NFA \(M_1\). Then convert \(M_1\) into an equivalent DFA \(M_0\). Now form the complement machine \(M_0^c\) by switching the non-accepting states into accepting states & vice versa. Then convert \(M_0^c\) into an equiv. regular expression \(E^c\). We will then have \(L(E^c) = L(M_0^c) = L(M_0^c)^c = L(M)^c = L(E_1)^c = L_1^c\).

So \(E^c\) will be a regular expression which describes \(L_1^c\). Hence \(L_1^c\) is a regular language.

f) We know that \((L_1 \cap L_2)^c = L_1^c \cup L_2^c\) by De Morgan's Law.

So \(L_1 \cap L_2 = (L_1 \cap L_2)^c = (L_1^c \cup L_2^c)^c\). But \(L_1^c\) & \(L_2^c\) are regular lang. by part (e). So \((L_1^c \cup L_2^c)^c\) is regular by part (a). Thus \(L_1 \cap L_2 = (L_1^c \cup L_2^c)^c\) will be regular by part (e).

9) \(L_1 \cap L_2 = L_1 \cap L_2^c\). By part (e), \(L_2^c\) is regular, so by part (f) \(L_1 \cap L_2^c = L_1 \cap L_2^c\) will a regular language.
Another closure result about regular languages.

**Def.** Let $T_1$ and $T_2$ be alphabets. We say that the function $h: T_1^* \rightarrow T_2^*$ is a **homomorphism** if $h(\alpha \beta) = h(\alpha) h(\beta)$ for any $\alpha, \beta \in T_1^*$.

**Fact 7.** If $h: T_1^* \rightarrow T_2^*$ is a homomorphism, then we must have $h(\lambda) = \lambda$.

**Proof:** We know that $h(\alpha \beta) = h(\alpha) h(\beta)$ for any $\alpha, \beta \in T_1^*$. So in particular since $\lambda = \lambda \lambda$, we get $h(\lambda) = h(\lambda \lambda) = h(\lambda) h(\lambda)$. From this it follows that $h(\lambda) = \lambda$ — because if $h(\lambda) \neq \lambda$, then we cannot have $h(\lambda) = h(\lambda) h(\lambda)$.

It can also be shown that $h$ is completely determined by $h(c_1), h(c_2), \ldots, h(c_n)$ where $T_1 = \{c_1, c_2, \ldots, c_n\}$. Now if $E$ is a regular expression over $T_1$, then $h(E)$ can be defined as the same expression $E$ except that each character $c_i$ is replaced by $h(c_i)$. For example, let $T_1 = \{a, b, c\}$ & $T_2 = \{0, 1\}$.

Put $h(a) = 10$, $h(b) = 11$ & $h(c) = 00$. If $E = a^* (b + ac)^*$, then we will have that $h(E) = (10)^* (11 + 1000)^*$.

**Prop. 8:** If $L$ is a regular language on $T_1$, and $h: T_1^* \rightarrow T_2^*$ is a homomorphism, then $h[L] = \{h(\alpha) : \alpha \in L\}$ is also a regular language.

**Proof:** If $E$ is a reg. expr. for $L$, then $h(E)$ is a reg. expr. for $h[L]$. 
Let \( L = \{ \alpha \in \{0,1\}^* : \alpha \text{ contains the string } 00 \} \). Find a regular expression which describes \( L \) and a regular expression which describes \( L^c = \{ \alpha : \alpha \text{ does not contain } 00 \} \).

(a) \( E = (0+1)^* \cdot 00 \cdot (0+1)^* \) is a regular expression which describes \( L \).

(b) First we convert \( E \) into an equivalent NFA, \( M \).

(c) Then we convert \( M \) into an equivalent DFA, \( M_D \).

\[ \begin{align*}
0(A) = \{ A \} & \quad \{ A, B, C \} \\
1(A) = \{ A \} & \quad \{ A, C \}
\end{align*} \]

Let \( D = \{ A \}, \quad E = \{ A, B \}, \quad F = \{ A, B, C \} \) and \( G = \{ A, C \} \).

Then \( M_D \) will be:

We can also minimize the DFA \( M_D \) to get \( (M_D)_{\min} \).

But we don't need to do this.

(d) Now switch the accepting & non-accepting states to get \( (M_D)^c \).

(e) Then find the regular expression which \( (M_D)_{\min} \) recognizes. Since \( F \) & \( G \) are non-accepting states, we only need to look at the NFA.

(f) Convert this NFA into an OAS-NFA.

Now get rid of \( E \) to obtain the GFA.

(g) Final Answer is: \( E^c = (1+01)^* \cdot (2+0) \).
Ex. 9. Let \( L = \{ \rho \in \{0,1\}^* : \rho \text{ contains the string } 101 \} \). Find regular expressions which describe \( L \) and \( L^c \).

(a) \((0+1)^* 101 (0+1)^*\) is a regular expression which describes \( L \).

(b) To find a regular expression which describes \( L^c \), we first find a DFA \( M \) which recognizes \( L \).

\[
M = \begin{array}{c}
A \quad \overset{1}{\rightarrow} \quad B \quad \overset{0}{\rightarrow} \quad C \quad \overset{1}{\rightarrow} \quad D
\end{array}
\]

We did this because it takes too many steps to go through an NFA.

(c) Now \( M^c \) = \[
\begin{array}{c}
A \quad \overset{1}{\rightarrow} \quad B \quad \overset{0}{\rightarrow} \quad C \quad \overset{1}{\rightarrow} \quad D
\end{array}
\]

So all we have to do now is to find the language which \( M^c \) recognizes (as a regular expression).

(d) We can ignore \( D \) and convert the rest of \( M^c \) into an OAS-NFA.

\[
M_1, \quad M_2, \quad M_3
\]

\[
E^c = (0+1)^* 00 (2+11)^* (0+0) = (0+11)^* 00 (2+11)^* 11^* 0
\]

Note that \( L^c = \{ \rho \in \{0,1\}^* : \rho \text{ does not contain } 101 \text{ as a substring} \}. \]
(15) Decidability problems involving Regular Languages

**Def.** A decision problem is a problem with unknown parameters which can take denumerably many values, such that for all values of the parameters, we have a YES or NO answer.

**Ex. 10 (Primality Decision Problem).** The problem is: Is \( n \) a prime number? Here \( n \) is the unknown parameter and for each value of \( n \), the answer is either YES or NO. The values the parameter \( n \) can take are \( \{0, 1, 2, 3, \ldots \} = \mathbb{N} \).

**Def.** A decision problem is algorithmically decidable if there is a fixed algorithm which takes as input the possible values of the unknown parameters and produces the correct answer.

**Ex. 11** The Primality Decision Problem is algorithmically decidable because we can find an algorithm which can decide whether or not \( n \) is prime. Just take \( n \) as input and try to see if any integer between 1 & \( \sqrt{n} \) divides \( n \). If none of the integers from 2 to \( \lfloor \sqrt{n} \rfloor \) divides \( n \), then \( n \) is prime. Otherwise \( n \) is not prime.

**Theorem 9 (Decidability Theorem for Reg. Lang.)**

Let \( L_1 \) & \( L_2 \) be regular languages. Then it is algorithmically decidable whether or not

(a) \( L_1 = \emptyset \)  
(b) \( L_1 \subseteq L_2 \)  
(c) \( L_1 = L_2 \)  
(d) \( L_1 \) is infinite.
Before we prove Theorem 9, let us first point out that the parameters are a pair of regular languages, \( L_1 \) and \( L_2 \). There are only denumerably many values of these two parameters because the number of regular languages is denumerable. We need two lemmas to help us in Theorem 9.

**Def.** An NFA is said to be \( \lambda \)-free if there are no \( \lambda \)-transitions that can take you from one state to a different state.

**Lemma 10:** Let \( M \) be a \( \lambda \)-free NFA with \( N \) states. Then \( L(M) \neq \emptyset \iff M \) accepts a string \( \gamma_0 \) of length \( \leq N-1 \).

**Proof:** 

\( \iff \): Suppose \( M \) accepts a string \( \gamma_0 \) of length \( \leq N-1 \). Then \( L(M) \neq \emptyset \) because \( \gamma_0 \in L(M) \).

\( \implies \) Now suppose \( L(M) \neq \emptyset \). Then we can find a string \( \gamma_1 \) such that \( M \) accepts \( \gamma_1 \). Consider any acceptance track of \( \gamma_1 \). If we remove all the loops in this acceptance track of \( \gamma_1 \), we will end up with an acceptance path of a string \( \gamma_0 \).

Since the length of the longest possible path in a graph with \( N \) states is \( N-1 \), we must have \( |\gamma_0| \leq N-1 \). So \( M \) accepts a string \( \gamma \) of length \( \leq N-1 \).
Lemma 11: Let $M$ be a $\lambda$-free NFA with $N$ states. Then $L(M)$ is infinite $\iff$ $M$ accepts a string $q_0$ with $N \leq |q_0| \leq 2N-1$.

Proof: ($\Leftarrow$) Suppose $M$ accepts a string $q_0$ with $N \leq |q_0| \leq 2N-1$. Now consider any acceptance track of $q_0$ in $M$. Since it takes $(q_0+1)$ states to process $q_0$, and $(q_0) \geq N$, this acceptance track must have a loop as shown below. Let $k = q_0 + 1$ and $q_0 = c_1 c_2 \cdots c_k$.

![Diagram showing a loop in an automaton accepting $q_0$.]

If we let $x = c_1 c_2 \cdots c_{i-1}$, $y = c_i+1 \cdots c_j$ and $z = c_{j+1} \cdots c_k$, then we can see that for each $r \geq 0$, $x y^r z$ will be accepted by $M$. Since $|y| = j-i \geq 1$, it follows that all these strings $x y^r z$ will be different from each other. So $L(M)$ will be infinite.

($\Rightarrow$) Suppose $L(M)$ is infinite. Then $M$ must accept a string $q_0$ with $|q_0| \geq N$ — because the total number of strings with length $\leq N-1$ is finite. Now if $|q_0| \leq 2N-1$, then we take $q_0$ to be $q_0$, and $M$ will accept a string $q_0$ with $N \leq |q_0| \leq 2N-1$. If $|q_0| > 2N-1$, then consider any acceptance track of $q_0$. If we delete the loops in this acceptance track of $q_0$, one at a time, we will eventually get a string $q_0$ which is accepted by $M$ and which satisfies $N \leq |q_0| \leq 2N-1$. So $M$ will accept a string $q_0$ with $N \leq |q_0| \leq 2N-1$. 
Proof of Theorem 9

(a) Since \( L_1 \) is a regular language, it follows from Theorem 5, that we can find a DFA (or \( \epsilon \)-free NFA) \( M \), such that \( L(M) = L_1 \). Now from Lemma 10, we know that \( L(M) \neq \emptyset \iff M \) accepts a string \( q_0 \) of length \( \leq N-1 \). So check all paths of length \( \leq N-1 \) from \( q_0 \) in \( M \). If one of these paths leads to an accepting state, then \( L(M) = L_1 \neq \emptyset \). If none of these paths lead to an accepting state, then \( L_1 = \emptyset \). So we have an algorithm which can decide whether or not \( L_1 = \emptyset \).

(b) First observe that \( L_1 \subseteq L_2 \iff L_1 - L_2 = \emptyset \). Since \( L_1 - L_2 \) is a regular language by Theorem 6(f), it follows that we can use the algorithm in part (a) to check whether or not \( L_1 - L_2 = \emptyset \). So we again have an algorithm to decide whether or not \( L_1 \subseteq L_2 \).

(c) Observe that \( L_1 = L_2 \iff L_1 \subseteq L_2 \) & \( L_2 \subseteq L_1 \). So use the algorithm in part (b) twice to check if both \( L_1 \subseteq L_2 \) & \( L_2 \subseteq L_1 \). So this gives us an algorithm to check whether or not \( L_1 = L_2 \).

(d) First find a \( \lambda \)-free NFA \( M \) such that \( L(M) = L_1 \). Now \( L(M) \) is infinite \( \iff M \) accepts a string \( q_0 \) with \( N \leq |q_0| \leq 2N-1 \). So check all possible acceptance tracks in \( M \) with lengths between \( N \) and \( 2N-1 \). If one track works, then \( L(M) = L_1 \) will be infinite. If none of the tracks works, then \( L(M) = L_1 \) will not be infinite.
§5. Non-regular languages & their properties.

Prop. 12: The set of all regular languages on \( \{a, b\} \) is countable and consequently non-regular languages exist.

Proof: We know that a regular language on \( \{a,b\} \) is one that can be described by a regular expression on \( \{a,b\} \). Now a reg. expr. on \( \{a,b\} \) is just a string based on the alphabet \( \{a,b,\lambda,0,+,\cdot,*,(,\})\} = T \). Since the set of all strings based on \( T \) is countable, it follows that \( REX \), the set of all regular expressions on \( \{a,b\} \) is also countable - because \( REX \subseteq T^* \).

Since we only have a countable number of reg. expr., the total no. of regular languages must also be countable.

Finally, the set of all languages on \( \{a,b\} \) is uncountable, so there must exist languages that are not regular. These languages are naturally called non-regular.

We will now give several concrete examples of non-regular languages.

Ex. 1: \( L_1 = \{a^kb^k : k \geq 0\} \) is a non-regular language.

Proof: Suppose \( L_1 \) is regular. Then we can find a \( \lambda \)-free NFA such that \( L(M) = L_1 \), by Theorem 5.

Let \( N = \) number of states in \( M \), and consider the string \( a^N b^N \). Since \( a^N b^N \in L_1 \), \( M \) will accept
Also since it takes \( N+1 \) states to process \( a^N \), any acceptance track of \( a^N b^N \) must have a loop as shown below.

Now if we skip the loop, we will see that \( M \) accepts the string \( a^i a^{N-j} b^N = a^{N-(j-i)} b^N \). Since \( i < j \), \( a^{N-(j-i)} b^N \notin L \). So we have a contradiction because \( L(M) = L \) and \( M \) accepted \( a^{N-(j-i)} b^N \). Hence \( L \) cannot be regular. So \( L \) is non-regular.

**Ex. 2** \( L_2 = \{ a^k b^m : k \leq m^2 \} \) is a non-regular language.

**Proof:** Suppose \( L_2 \) is regular. Then we can find a \( \lambda \)-free NFA \( M_2 \) such that \( L(M_2) = L_2 \). Let \( N \) be the number of states in \( M_2 \) and consider the string \( a^N b^N \). Since \( a^N b^N \in L_2 \), \( M_2 \) will accept \( a^N b^N \). Also since it takes \( N+1 \) states to process \( a^N \), any acceptance track of \( a^N b^N \) must contain a loop as shown below.
Now if we ride the loop twice, we will see that $M_2$ accepts the string $a^i \ a^{N-j} \ a^{j-i} \ a^{N-i} \ y^j \ b^N$.

But $a^{N+i} \ a^j \ b^N \in L_2$ because $N+(j-1) \neq N$ since $i < j$. This contradicts the fact that $L(M_2) = L_2$.

Hence $L_2$ cannot be regular. So $L_2$ is non-regular.

**Ex. 3** $L_3 = \{a^{k^2} : k \geq 0\}$ is a non-regular language.

**Proof:** Suppose $L_3$ is regular. Then we can find a $\lambda$-free

NFA $M_3$ such that $L(M_3) = L_3$. Let $N$ be the number of states in $M_3$ and consider the string $a^{(NH)^2} = a^{N^2+2N+1}$. Since $a^{N^2+2N+1} \in L_3$, it will be accepted by $M_3$. Also, since it takes $2N+2$ states to process the last $(2N+1)$th $a$'s, any acceptance track of $a^{N^2+2N+1}$ must have a loop as shown below.

Now if we skip the loop, we will see that $M_3$ accepts the string $a^{N^2} \cdot a^i \cdot a^{2NH-j} = a^{N^2+2N+1-(j-i)}$. But

$N^2 < N^2 + 2N+1-(j-i) < N^2 + 2N+1 = (NH)^2$, so it follows that $N^2+2NH-(j-i)$ cannot be a perfect square, because it is strictly between two consecutive perfect squares. Hence $a^{N^2+2NH-(j-i)} \notin L_3$. But this contradicts the fact that $L(M_3) = L_3$. Hence

$L_3$ cannot be regular. So $L_3$ is a non-reg. lang.
We can summarize the idea in the last 3 examples in the following result.

**Prop. 12 (Rumping Lemma for Regular Languages)**
Let $L$ be any infinite regular language. Then we can find a positive integer $N$ such that any $w \in L$ can be decomposed as $w = xyz$ with $|xy| \leq N$ and $|y| \geq 1$ such that $xy^rz \in L$ for each $r \in \mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

**Proof:** Since $L$ is regular, we can find a $Q$-free NFA $M$ such that $L(M) = L$. Put $N$ the number of states in $M$. Now if $w$ is any string in $L$ with $|w| \geq N$, put $w_N$ the string of the first $N$ characters of $w$. Since $w \in L$, $M$ will accept $w_N$. Also since $M$ has only $N$ states, and we need $N+1$ states to process $w_M$, any acceptance track of $w$ must contain a loop as shown below.

![Diagram of NFA](image)

Now $|xy| \leq N$ because the loop will appear somewhere between $q_0$ & $q_N$. Also $|y| = j-i \geq 1$. If we ride the loop $r$ times, we will see that $M$ accepts $xy^rz$. So $xy^rz \in L$ for each $r \in \mathbb{N}$. 
Ex. 4. Using the Pumping Lemma for Regular languages, prove that \( L_4 = \{ w \in \{a,b\}^* : 2^n(a) = n(b) \} \) is non-regular.

Proof: Suppose \( L_4 \) is regular. Then by the Pumping Lemma, we can find an \( N \geq 1 \) such that any \( w \in L_4 \) with \( |w| \geq N \) can be decomposed as \( w = xyz \) with \( |xy| \leq N \) and \( |y| \geq 1 \) such that \( xy^iz \in L_4 \) for all \( i \in \mathbb{N} \).

Now consider the string \( w = a^N b^2N \in L_4 \). Since the first \( N \) characters of \( w \) are all \( a \)'s, we must have \( x = a^p \), \( y = a^q \) and \( z = a^{N-p-q} b^2N \) for some \( p, q \) with \( 0 \leq p \leq N-1 \) and \( q \geq 1 \). But by the Pumping Lemma, \( xy^0z \in L_4 \). So

\[
a^p a^{N-p-q} b^2N = a^{N-q} b^2N \in L_4.
\]

But this contradicts the fact that strings in \( L_4 \) have twice as many \( b \)'s as \( a \)'s. Hence \( L_4 \) must be non-regular.

We can also prove that certain languages are non-regular by using the Closure Theorem & previous results.

Ex. 5. Show that \( L_5 = \{a^k b^m : k \neq m \} \) is non-regular.

Proof: Suppose \( L_5 \) is regular. Then \( a^* b^* - L_5 \) will also be regular by Theorem 6(6). But

\[
a^* b^* - L_5 = \{a^k b^m : k, m \geq 0 \} - \{a^k b^m : k + m \} = \{a^k b^m : k = m \} = \{a^k : k \geq 0 \} = L_1 \), which is non-regular.

So this is a contradiction. Hence \( L_5 \) is non-regular.
We will now explore some of the properties of non-regular languages.

**Prop. 13**: If \( L \) is a non-regular language, then
1. \( L^c \) is non-regular
2. \( L^R \) is non-regular

**Proof**: (a) Suppose \( L^c \) is regular. Then by the Closure Theorem (Theorem 6(e)), it follows that \((L^c)^c\) would also be regular. But \((L^c)^c = L\), so this contradicts the fact that \( L \) was non-regular. Hence \( L^c \) must also be non-regular.

(b) Suppose \( L^R \) is regular. Then by the Closure Theorem part (a), \((L^R)^R = L\) would also be regular. But this contradicts the fact that \( L \) is non-regular. Hence \( L^R \) must also be regular.

**Ex 6**: If \( L_1 \) & \( L_2 \) are non-regular languages, it is possible for
(a) \( L_1 \cup L_2 \) to be regular,
(b) \( L_1 \cdot L_2 \) to be regular,
and (c) \( L_1^* \) to be regular.

(a) Take \( L_1 = \{a^k b^k : k \geq 0\} \) and \( L_2 = \{a^k b^m : k \neq m\} \). Then \( L_1 \) & \( L_2 \) are both non-regular but \( L_1 \cup L_2 = a^* b^* \) which is regular.

(b) Take \( L_1 = \{a^k : k \geq 0\} \) and \( L_2 = \{a^m : m \text{ is not a square}\} \). Then \( L_1 \cdot L_2 = \{a^k a^m : k \geq 0, m \text{ is not a square}\} \). Take \( L_1 \cdot L_2 = L_1^c \). Then \( L_1 \cdot L_2 = \{a^2, a^3, a^4, a^5, \ldots \} \). \( L_1 \cdot L_2 = \{a^2, a^3, a^4, a^5, \ldots \} = \{a^k : k \geq 2\} = a^* a^* \).

(c) Take \( L_1 = \{a^k : k \geq 0\} \). Then \( L_1^* = a^* \) which is regular bec. \( a^* = \{a^0, a^1 a^2, a^4 a^5, \ldots \} \).