What is TOC?
In theoretical computer science, the **theory of computation** is the branch that deals with whether and how efficiently problems can be solved on a model of computation, using an algorithm. The field is divided into three major branches: automata theory, computability theory and computational complexity theory.

In order to perform a rigorous study of computation, computer scientists work with a mathematical abstraction of computers called a model of computation. There are several models in use, but the most commonly examined is the Turing machine. Automata theory

In theoretical computer science, **automata theory** is the study of abstract machines (or more appropriately, abstract 'mathematical' machines or systems) and the computational problems that can be solved using these machines. These abstract machines are called automata. This automaton consists of

- **states** (represented in the figure by circles),
- and **transitions** (represented by arrows).

As the automaton sees a symbol of input, it makes a **transition** (or jump) to another state, according to its **transition function** (which takes the current state and the recent symbol as its inputs).

**Uses of Automata:** compiler design and parsing.

![Finite Automaton](image)

**Figure 1.2: A finite automaton modeling recognition of `then`**

**Introduction to formal proof:**
**Basic Symbols used:**
- **U** – Union
- **∩** – Conjunction
- **ϵ** – Empty String
- **Φ** – NULL set
- **¬** – Negation
- **′** – compliment
- **=>** – implies
Additive inverse: \( a + (-a) = 0 \)

Multiplicative inverse: \( a \cdot 1/a = 1 \)

Universal set \( U = \{1, 2, 3, 4, 5\} \)

Subset \( A = \{1, 3\} \)

\( A' = \{2, 4, 5\} \)

Absorption law: \( A \cup (A \cap B) = A, \ A \cap (A \cup B) = A \)

De Morgan’s Law:

\( (A \cup B)' = A' \cap B' \)

\( (A \cap B)' = A' \cup B' \)

Double compliment

\( (A')' = A \)

\( A \cap A' = \emptyset \)

Logic relations:

\( a \land b \Rightarrow 7a \cup b \)

\( 7(a \land b) = 7a \cup 7b \)

Relations:

Let \( a \) and \( b \) be two sets a relation \( R \) contains \( a \times b \).

Relations used in TOC:

Reflexive: \( a = a \)

Symmetric: \( aRb \Rightarrow bRa \)

Transition: \( aRb, bRc \Rightarrow a Rc \)

If a given relation is reflexive, symmetric and transitive then the relation is called equivalence relation.

Deductive proof: Consists of sequence of statements whose truth lead us from some initial statement called the hypothesis or the given statement to a conclusion statement.

The theorem that is proved when we go from a hypothesis \( H \) to a conclusion \( C \) is the statement “if \( H \) then \( C \).” We say that \( C \) is deduced from \( H \).

Additional forms of proof:

Proof of sets

Proof by contradiction

Proof by counter example

Direct proof (AKA) Constructive proof:

If \( p \) is true then \( q \) is true

Eg: if \( a \) and \( b \) are odd numbers then product is also an odd number.

Odd number can be represented as \( 2n+1 \)

\( a = 2x+1, \ b = 2y+1 \)

Product of \( a \times b = (2x+1) \times (2y+1) = 2(2xy+x+y)+1 = 2z+1 \) (odd number)
Proof by contrapositive:

1. \( H \) and \( C \) both true.
2. \( H \) true and \( C \) false.
3. \( C \) true and \( H \) false.
4. \( H \) and \( C \) both false.

That is, start by assuming both the hypothesis \( H \) and the negation of the conclusion \( C \). Complete the proof by showing that something known to be false follows logically from \( H \) and not \( C \). This form of proof is called proof by contradiction.

It often is easier to prove that a statement is not a theorem than to prove it is a theorem. As we mentioned, if \( S \) is any statement, then the statement “\( S \) is not a theorem” is itself a statement without parameters, and thus can

**Alleged Theorem 1.13:** All primes are odd. (More formally, we might say: if integer \( x \) is a prime, then \( x \) is odd.)

**DISPROOF:** The integer 2 is a prime, but 2 is even. \( \square \)
Suppose we are given a statement $S(n)$, about an integer $n$, to prove. One common approach is to prove two things:

1. The basis, where we show $S(i)$ for a particular integer $i$. Usually, $i = 0$ or $i = 1$, but there are examples where we want to start at some higher $i$, perhaps because the statement $S$ is false for a few small integers.

2. The inductive step, where we assume $n \geq i$, where $i$ is the basis integer, and we show that "if $S(n)$ then $S(n + 1)$.”

- The Induction Principle: If we prove $S(i)$ and we prove that for all $n \geq i$, $S(n)$ implies $S(n + 1)$, then we may conclude $S(n)$ for all $n \geq i$.

Be regarded as an observation than a theorem.

For any sets $a, b, c$ if $a \cap b = \emptyset$ and $c$ is a subset of $b$ the prove that $a \cap c = \emptyset$

Given : $a \cap b = \emptyset$ and $c$ subset $b$

Assume: $a \cap c = \emptyset$

Then

$\Rightarrow a \cap b \neq \emptyset \Rightarrow a \cap c = \emptyset$ (i.e., the assumption is wrong)

$\Sigma = \{0, 1\}$

$\Sigma = \{a, b, c\}$

$\Sigma = \{a, b, c, \&, \}$

$\Sigma = \{\#, \&, \symbol{101}, \}$

$\Sigma$ $\Sigma$
Languages:

The languages we consider for our discussion is an abstraction of natural languages. That is, our focus here is on formal languages that need precise and formal definitions. Programming languages belong to this category.

Symbols:

Symbols are indivisible objects or entity that cannot be defined. That is, symbols are the atoms of the world of languages. A symbol is any single object such as , a, 0, 1, #, begin, or do.

Alphabets:

An alphabet is a finite, nonempty set of symbols. The alphabet of a language is normally denoted by . When more than one alphabets are considered for discussion, then subscripts may be used (e.g. etc) or sometimes other symbol like G may also be introduced.

Example:

Strings or Words over Alphabet:

A string or word over an alphabet is a finite sequence of concatenated symbols of .

Example: 0110, 11, 001 are three strings over the binary alphabet \{ 0, 1 \} .
aab, abcb, b, cc are four strings over the alphabet \{ a, b, c \}.

It is not the case that a string over some alphabet should contain all the symbols from the alphabet. For example, the string cc over the alphabet \{ a, b, c \} does not contain the symbols a and b. Hence, it is true that a string over an alphabet is also a string over any superset of that alphabet.

**Length of a string:**
The number of symbols in a string \( w \) is called its length, denoted by \(| w |\).

**Example:** \(| 011 | = 4, |11| = 2, |b| = 1\)

**Convention:** We will use small case letters towards the beginning of the English alphabet to denote symbols of an alphabet and small case letters towards the end to denote strings over an alphabet. That is, (symbols) and (strings).

\[ \Sigma^0 = \{ \epsilon \} \]
\[ \Sigma^2 = \{ 00, 01, 10, 11 \} \]

**Some String Operations**
Let \( x \) and \( y \) be two strings. The concatenation of \( x \) and \( y \) denoted by \( xy \), is the string. That is, the concatenation of \( x \) and \( y \) denoted by \( xy \) is the string that has a copy of \( x \) followed by a copy of \( y \) without any intervening space between them.

**Example:** Consider the string 011 over the binary alphabet. All the prefixes, suffixes and substrings of this string are listed below.

- Prefixes: \( \langle 0, 01, 011 \rangle \)
- Suffixes: \( \langle 1, 11, 011 \rangle \)
- Substrings: \( \langle 0, 1, 01, 11, 011 \rangle \)

Note that \( x \) is a prefix (suffix or substring) to \( x \), for any string \( x \) and \( \epsilon \) is a prefix (suffix or substring) to any string.

A string \( x \) is a proper prefix (suffix) of string \( y \) if \( x \) is a prefix (suffix) of \( y \) and \( x \subseteq y \).

In the above example, all prefixes except 011 are proper prefixes.

**Powers of Strings:** For any string \( x \) and integer, we use to denote the string formed by sequentially concatenating \( n \) copies of \( x \). We can also give an inductive definition of as follows:

\[ x^0 = \epsilon, \text{ if } n = 0; \text{ otherwise } \]

\[ x^n = x_1 x_2 \cdots x_n \]

**Example:** If \( x = 011 \), then \( x^1 = 011\), \( x^2 = 011011\), \( x^3 = 011011011\), \( x^4 = 011011011011\)

**Powers of Alphabets**
We write \( (\text{for some integer } k) \) to denote the set of strings of length \( k \) with symbols from \( \Sigma \). In other words, 
\[
\Sigma^k = \{ w \mid w \text{ is a string over } \Sigma \text{ and } |w| = k \}.
\]
Hence, for any alphabet, \( \emptyset \) denotes the set of all strings of length zero. That is, 
\[
\emptyset = \{ \epsilon \}. \quad \text{For the binary alphabet } \{0, 1\}, \text{ we have the following.}
\]

The set of all strings over an alphabet \( \Sigma \) is denoted by \( \Sigma^* \). That is, 
\[
\Sigma^* = \{ w \mid w \text{ is a string over } \Sigma \text{ and } |w| \geq 0 \}.
\]

The set contains all the strings that can be generated by iteratively concatenating symbols from any number of times. 
\[
\alpha, \beta, \gamma \in \Sigma, \quad u, v, w, x, y, z
\]

**Example:** If \( \Sigma = \{a, b\} \), then 
\[
\Sigma^* = \{\epsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, \ldots\}.
\]

Please note that \( \emptyset^* = \{\epsilon\} \), that is, \(\emptyset^* \neq \emptyset\) and that one can proceed from the empty set to a non-empty set by iterated concatenation. But there is a reason for this and we accept this convention.

The set of all nonempty strings over an alphabet \( \Sigma \) is denoted by \( \Sigma^* \). That is, 
\[
\Sigma^* = \{ w \mid w \text{ is a string over } \Sigma \text{ and } |w| > 0 \}.
\]

Note that \( \Sigma^* \) is infinite. It contains no infinite strings but strings of arbitrary lengths.

**Reversal:**

For any string \( x \) the reversal of the string is \( \bar{x} \).

An inductive definition of reversal can be given as follows:

\[
\bar{x}^n = \begin{cases} 
\bar{x} & \text{if } n = 0 \\
\bar{x}^{n-1}x & \text{if } n > 0
\end{cases}
\]

**Languages:**

A language over an alphabet is a set of strings over that alphabet. Therefore, a language \( L \) is any subset of \( \Sigma^* \). That is, any subset of \( \Sigma^* \) is a language.
1. \( F \) is the empty language. 2. is a language for any.

3. \( \{e\} \) is a language for any. Note that, contains any string but \( \{e\} \) contains one string of length zero.

4. The set of all strings over \( \{0, 1\} \) containing equal number of 0's and 1's.

5. The set of all strings over \( \{a, b, c\} \) that starts with \( a \).

**Convention**: Capital letters \( A, B, C, L, \) etc. with or without subscripts are normally used to denote languages.

**Set operations on languages**: Since languages are set of strings we can apply set operations to languages. Here are some simple examples (though there is nothing new in it).

**Union**: A string iff or

**Example**: \( \{0, 1, 01, 011\} \sqcup \{1, 01, 110\} = \{0, 11, 011, 111\} \)

**Intersection**: A string, \( x \in L_1 \cap L_2 \) iff \( x \in L_1 \) and \( x \in L_2 \).

**Example**: \( \{0, 1, 01, 011\} \cap \{1, 01, 110\} = \{01\} \)

**Complement**: Usually, is the universe that a complement is taken with respect to. Thus for a language \( L \), the complement is \( L(\bar{\text{bar}}) = \{\}\). 

**Example**: Let \( L = \{x \mid \text{|x| is even}\} \). Then its complement is the language \( \{x \mid \text{|x| is odd}\} \). Similarly we can define other usual set operations on languages like relative complement, symmetric difference, etc.

**Reversal of a language**:

The reversal of a language \( L \), denoted as \( \bar{L} \), is defined as:

**Example**:

1. Let \( L = \{0, 11, 01, 011\} \). Then \( \bar{L} = \{0, 11, 10, 110\} \).

2. Let \( L = \{n \mid \text{n is an integer}\} \). Then \( \bar{L} = \{\bar{n} \mid \text{n is an integer}\} \).

**Language concatenation**: The concatenation of languages and is defined as.
Example: \( \{ a, ab \} \{ b, ba \} = \{ ab, aba, abb, abba \} \).

Note that,

1. in general. 
   \[ L^* \quad 2 \cdot LL^* \]

3. 

**Iterated concatenation of languages**:

Since we can concatenate two languages, we also repeat this to concatenate any number of languages. Or we can concatenate a language with itself any number of times. The operation denotes the concatenation of \( L \) with itself \( n \) times. This is defined formally as follows:

\[
L^* = L^0 \cup L^1 \cup L^2 \cup \cdots
\]

**Example**: Let \( L = \{ a, ab \} \). Then according to the definition, we have

\[
L^* = L^0 \cup L^1 \cup L^2 \cup \cdots
\]

and so on.

**Kleene's Star operation**: The Kleene star operation on a language \( L \), denoted as \( L^* \), is defined as follows:

\[
L^* = \{ x \mid x \text{ is the concatenation of zero or more strings from } L \}
\]

Thus is the set of all strings derivable by any number of concatenations of strings in \( L \). It is also useful to define

\[
= \{ x \mid x \text{ is the concatenation of one or more concatenations of strings in } L \}
\]
Example: Let \( L = \{ a, \text{ab} \} \). Then we have,

\[
\{e\} \quad \{a, \text{ab}\} \quad \{\text{aa, aab, aba, abab}\} \quad \ldots
\]

Note: \( \{ \text{is in } L \} \), for every language \( L \), including .

The previously introduced definition of \( \{ \) is an instance of Kleene star.

Grammar

Language

Automata: A algorithm or program that automatically recognizes if a particular string belongs to the language or not, by checking the grammar of the string.

An automata is an abstract computing device (or machine). There are different varities of such abstract machines (also called models of computation) which can be defined mathematically.

Every Automaton fulfills the three basic requirements.

Every automaton consists of some essential features as in real computers. It has a mechanism for reading input. The input is assumed to be a sequence of symbols over a given alphabet and is placed on an input tape (or written on an input file). The simpler automata can only read the input one symbol at a time from left to right but not change. Powerful versions can both read (from left to right or right to left) and change the input.

Getmynotes.com

CS6503 THEORY OF COMPUTATION

The automaton can produce output of some form. If the output in response to an input string is binary (say, accept or reject), then it is called an accepter. If it produces an output sequence in response to an input sequence, then it is called a transducer (or automaton with output).

The automaton may have a temporary storage, consisting of an unlimited number of cells, each capable of holding a symbol from an alphabet (which...
Infinite Automata

Automata (singular: automation) are a particularly simple, but useful, model of computation. They were initially proposed as a simple model for the behavior of neurons.
States, Transitions and Finite-State Transition System:

Let us first give some intuitive idea about a state of a system and state transitions before describing finite automata.

Informally, a state of a system is an instantaneous description of that system which gives all relevant information necessary to determine how the system can evolve from that point on.

Transitions are changes of states that can occur spontaneously or in response to inputs to the states. Though transitions usually take time, we assume that state transitions are instantaneous (which is an abstraction).

Some examples of state transition systems are: digital systems, vending machines, etc.

A system containing only a finite number of states and transitions among them is called a finite-state transition system.

Finite-state transition systems can be modeled abstractly by a mathematical model called finite automation.

**Deterministic Finite (-state) Automata**

Informally, a DFA (Deterministic Finite State Automaton) is a simple machine that reads an input string -- one symbol at a time -- and then, after the input has been completely read, decides whether to accept or reject the input. As the symbols are read from the tape, the automaton can change its state, to reflect how it reacts to what it has seen so far. A machine for which a deterministic code can be formulated, and if there is only one unique way to formulate the code, then the machine is called deterministic finite automata.

Thus, a DFA conceptually consists of 3 parts:

1. A **tape** to hold the input string. The tape is divided into a finite number of cells. Each cell holds a symbol from $\Sigma$.
2. A **tape head** for reading symbols from the tape
3. A **control**, which itself consists of 3 things:
   - finite number of states that the machine is allowed to be in (zero or more states are designated as accept or final states),
   - a current state, initially set to a start state,
   - a state transition function for changing the current state.

An automaton processes a string on the tape by repeating the following actions until the tape head has traversed the entire string:

1. The tape head reads the current tape cell and sends the symbol $s$ found there to the control. Then the tape head moves to the next cell.
2. The control takes $s$ and the current state and consults the state transition function to get the next state, which becomes the new current state.

Once the entire string has been processed, the state in which the automation enters is examined. If it is an accept state, the input string is accepted; otherwise, the string is rejected. Summarizing all the above we can formulate the following formal definition:

\[ \delta : Q \times \Sigma^* \rightarrow Q \]

**Deterministic Finite State Automaton**: A Deterministic Finite State Automaton (DFA) is a 5-tuple: $\delta \left( q, \psi \right)$

- $Q$ is a finite set of states.
- $\Sigma$ is a finite set of input symbols or alphabet.
- $\delta$ is the next state transition function (which is total). Intuitively, $\delta$ is a function that tells which state to move to in response to an input, i.e., if $M$ is in state $q$ and sees input $a$, it moves to state $\delta(q, a)$.
- $q_0$ is the start state.
- $F$ is the set of accept or final states.

**Acceptance of Strings**:

A DFA $\langle Q, \Sigma, \delta, q_0, F \rangle$ accepts a string $\psi$ if there is a sequence of states $q_i$ in $Q$ such that:

1. $q_0$ is the start state.
2. $q_i$ for all $i$.
3. $F = \{ q_f \}$

**Language Accepted or Recognized by a DFA**:

The language accepted or recognized by a DFA $M$ is the set of all strings accepted by $M$, and is denoted by $L(M)$. The notion of acceptance can also be made more precise by extending the transition function.

**Extended transition function**:

Getmynotes.com

<table>
<thead>
<tr>
<th>$q_0$</th>
<th>$q_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rightarrow q_0$</td>
<td>$\delta(q_0, \psi)$</td>
</tr>
</tbody>
</table>

(which is function on symbols) to a function on strings, i.e.

That is, the state the automation reaches when it starts from the state $q$ and finish processing the string $w$. Formally, we can give an inductive definition as follows:
The language of the DFA $M$ is the set of strings that can take the start state to one of the accepting states i.e.

$$L(M) = \{ \omega \mid M \text{ accepts } \omega \}$$

Example 1:

![Transition Diagram]

is the start state

$$q_0, q_1$$

It is a formal description of a DFA. But it is hard to comprehend. For ex. The language of the DFA is any string over \{0, 1\} having at least one 1.

We can describe the same DFA by transition table or state transition diagram as following:

**Transition Table:**

<table>
<thead>
<tr>
<th></th>
<th>$q_0$</th>
<th>$q_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$q_0$</td>
<td>$q_1$</td>
</tr>
<tr>
<td>1</td>
<td>$q_1$</td>
<td>$q_1$</td>
</tr>
</tbody>
</table>

$$\delta(q, a) = p$$

It is easy to comprehend the transition diagram.
Explanation: We cannot reach the final state w/o or in the input string. There can be any no. of 0's at the beginning. (The self-loop at on label 0 indicates it). Similarly, there can be any no. of 0's & 1's in any order at the end of the string.

Transition table:

It is basically a tabular representation of the transition function that takes two arguments (a state and a symbol) and returns a value (the next state).

Rows correspond to states, columns correspond to input symbols, entries correspond to next states. The start state is marked with an arrow. The accept states are marked with a star (*).

(State) Transition diagram:

A state transition diagram or simply a transition diagram is a directed graph which can be constructed as follows:

1. For each state in Q there is a node.
2. There is a directed edge from node q to node p labeled a iff. (If there are several input symbols that cause a transition, the edge is labeled by the list of these symbols.)
3. There is an arrow with no source into the start state.
4. Accepting states are indicated by double circle.

∀ a ∈ Σ

5.

6. Here is an informal description how a DFA operates. An input to a DFA can be any string. Put a pointer to the start state q. Read the input string w from

\[ r_1 \rightarrow r_2 \]

\[ r_1 + r_2 \]

\[ r \rightarrow r_2 \]

CS6503 THEORY OF COMPUTATION
left to right, one symbol at a time, moving the pointer according to the transition function. If the next symbol of \( w \) is \( a \) and the pointer is on state \( p \), move the pointer to state \( p' \). When the end of the input string \( w \) is encountered, the pointer is on some state, \( r \). The string is said to be accepted by the DFA if and only if \( r \). Note that there is no formal mechanism for moving the pointer.

7. A language is said to be regular if \( L = L(M) \) for some DFA \( M \).

**Regular Expressions: Formal Definition**

We construct REs from primitive constituents (basic elements) by repeatedly applying certain recursive rules as given below. (In the definition)

**Definition**: Let \( S \) be an alphabet. The regular expressions are defined recursively as follows.

**Basis**:

i) \( \phi \) is a RE

ii) \( \epsilon \) is a RE

iii) \( \forall a \in S \), \( a \) is RE.

These are called primitive regular expression i.e. Primitive Constituents

**Recursive Step**:

If \( r_1 \) and \( r_2 \) are REs over \( S \), then so are

i) \( \phi \) is a RE

ii) \( \epsilon \) is a RE

iii) \( \forall a \in S \), \( a \) is a RE.

iv) \( r_1 + r_2 \) is a RE

v) \( r_1^* \) is a RE

**Closure**: \( r \) is RE over only if it can be obtained from the basis elements (Primitive REs) by a finite no of applications of the recursive step (given in 2).
Example: Let \( \{ 0,1,2 \} \). Then \((0+21)^*(1+F)\) is a RE, because we can construct this expression by applying the above rules as given in the following step.

<table>
<thead>
<tr>
<th>Steps</th>
<th>RE Constructed</th>
<th>Rule Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( r_1 r_2 )</td>
<td>1(iii)</td>
</tr>
<tr>
<td>2</td>
<td>( r_1 r_2 )</td>
<td>2(1(i))</td>
</tr>
<tr>
<td>3</td>
<td>( r_1^* )</td>
<td>3(i)</td>
</tr>
<tr>
<td>4</td>
<td>( (1+ ) )</td>
<td>4(iii)</td>
</tr>
<tr>
<td>5</td>
<td>( 52(1(iii)) )</td>
<td>5(i)</td>
</tr>
<tr>
<td>6</td>
<td>( 61(1(iii)) )</td>
<td>6(i)</td>
</tr>
<tr>
<td>7</td>
<td>( 72(1(ii)), 5, 6 )</td>
<td>7(ii)</td>
</tr>
<tr>
<td>8</td>
<td>( 801(3(iii)) )</td>
<td>8(iii)</td>
</tr>
<tr>
<td>9</td>
<td>( 90+212(1(i)), 7, 8 )</td>
<td>9(i)</td>
</tr>
<tr>
<td>10</td>
<td>( 10(0+212(1(i)), 9 )</td>
<td>10(i)</td>
</tr>
<tr>
<td>11</td>
<td>( 11(0+212(1(i)), 10 )</td>
<td>11(i)</td>
</tr>
<tr>
<td>12</td>
<td>( 12(0+212(1(i)), 4, 11 )</td>
<td>12(i)</td>
</tr>
</tbody>
</table>

Language described by REs: Each describes a language (or a language is associated with every RE). We will see later that REs are used to attribute regular languages.

Notation: If \( r \) is a RE over some alphabet then \( L(r) \) is the language associate with \( r \).

We can define the language \( L(r) \) associated with (or described by) a REs as follows.

1. \( r \) is the RE denoting the empty language i.e. \( L( ) = \emptyset \).
2. \( r \) is a RE denoting the language \( \{ \} \) i.e. \( L( ) = \{ \} \).
3. \( r \), \( a \) is a RE denoting the language \( \{a\} \) i.e. \( L(a) = \{a\} \).

4. If \( r \) and \( s \) are REs denoting language \( L( ) \) and \( L( ) \) respectively, then
   i) \( r+s \) is a regular expression denoting the language \( L( ) = L( ) + L( ) \)
   ii) \( rs \) is a regular expression denoting the language \( L( ) = L( ) L( ) \)
   iii) \( r^* \) is a regular expression denoting the language \( L( ) = L( )^* \)
   iv) \( (r) \) is a regular expression denoting the language \( L( ) = L( ) \)

Example: Consider the RE \((0^*(0+1))\). Thus the language denoted by the RE is
\[
L(0^*(0+1)) = L(0^*) L(0+1) \quad \text{by 4(ii)}
\]

\[
= L(0)^* L(0) L(1)
\]

\[
= \{0, 00, 000, \ldots\} \{0\} \quad \{1\}
\]

\[
= \{0, 00, 000, \ldots\} \{0,1\}
\]

\[
= \{0, 00, 000, \ldots, 1, 01, 001, 0001, \ldots\}
\]

**Precedence Rule**

Consider the RE \(ab + c\). The language described by the RE can be thought of either \(L(a)L(b+c)\) or \(L(ab)L(c)\) as provided by the rules (of languages described by REs) given already. But these two represents two different languages lending to ambiguity. To remove this ambiguity we can either

1) Use fully parenthesized expression- (cumbersome) or

2) Use a set of precedence rules to evaluate the options of REs in some order. Like other algebras mod in mathematics.

For REs, the order of precedence for the operators is as follows:

i) The star operator precedes concatenation and concatenation precedes union (+) operator.

ii) It is also important to note that concatenation & union (+) operators are associative and union operation is commutative.

Using these precedence rule, we find that the RE \(ab+c\) represents the language \(L(ab)L(c)\) i.e. it should be grouped as \(((ab)+c)\).

We can, of course change the order of precedence by using parentheses. For example, the language represented by the RE \(a(b+c)\) is \(L(a)L(b+c)\).
Example: The RE $ab^*+b$ is grouped as $((a(b^*))b)$ which describes the language $L(a)(L(b))^* L(b)$

Example: The RE $(ab)^*+b$ represents the language $(L(a)L(b))^* L(b)$.

Example: It is easy to see that the RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The regular expression $r=(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: It is easy to see that the RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The regular expression $r=(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.

Example: The RE $(0+1)^*(0+1)$ represents the language of all strings over $\{0,1\}$ which are either ended with $0$ or $11$.
CS6503 THEORY OF COMPUTATION

\[ L(r) = \{ \text{has no pair of consecutive 1's} \} \]

**Solution**: Though it looks similar to ex ........, it is harder to construct to construct. We observer that, whenever a 1 occurs, it must be immediately followed by a 0. This substring may be preceded & followed by any no of 0's. So the final RE must be a repetition of strings of the form: 00...0100...0 i.e. 0*100*. So it looks like the RE is (0*100*)*. But in this case the strings ending in 1 or consisting of all 0's are not accounted for. Taking these observations into consideration, the final RE is

\[ r = (0*100*)(1+) + 0*(1+) = \phi \]

**Alternative Solution**:

The language can be viewed as repetitions of the strings 0 and 01. Hence get the RE as \( r = (0+10)^*(1+) \). This is a shorter expression but represents the same language.

**Regular Expression and Regular Language**:

**Equivalence (of REs) with FA**:

Recall that, language that is accepted by some FAs are known as Regular language. The two concepts : REs and Regular language are essentially same i.e. (for) every regular language can be developed by (there is) a RE, and for every RE there is a Regular Language. This fact is rather suprising, because RE approach to describing language is fundamentally diffferent from the FA approach. But REs and FA are equivalent in their descriptive power. We can put this fact in the focus of the following

**Theorem**: A language is regular iff some RE describes it.

This Theorem has two directions, and are stated & proved below as a separate lemma

\[ \varepsilon \]

**RE to FA**:

\[ a \in \Sigma \]

**REs denote regular languages**:

**Lemma**: If \( L(r) \) is a language described by the RE \( r \), then it is regular i.e. there is a FA such that \( L(M) = L(r) \).

**Proof**: To prove the lemma, we apply structured index on the expression \( r \). First, we show how to construct FA for the basis elements: , and for any. Then we show how to combine these Finite Automata into Complex Automata that accept the Union, Concatenation, Kleen Closure of the languages accepted by the original smaller automata.

\[ N = \{ (p,q), \Sigma, \delta, \omega, (q) \} \]

\[ \delta(p,a,q) = \delta(q,a,q) = (q) \]

\[ s \neq p \quad b \neq a \]
Use of NFAs is helpful in the case i.e. we construct NFAs for every REs which are represented by transition diagram only.

**Basis:**

Case (i): Then and the following NFA $N$ recognizes $L(r)$. Formally where $Q = \{q\}$ and

Case (ii): and the following NFA $N$ accepts $L(r)$. Formally where

Since the start state is also the accept step, and there is no any transition defined, it will accept the only string and nothing else.

Case (iii): $r = a$ for some . Then $L(r) = \{a\}$, and the following NFA $N$ accepts $L(r)$.

Formally, where for or

**Induction:**
Assume that the start of the theorem is true for REs and . Hence we can assume that we have automata and that accepts languages denoted by REs and , and respectively i.e. . The FAs are represented schematically as shown below.

Each has an initial state and a final state. There are four cases to consider.

**Case (i):** Consider the RE denoting the language . We construct FA , from and to accept the language denoted by RE as follows:

Create a new (initial) start state and give -transition to the initial state of and . This is the initial state of .

Create a final state and give -transition from the two final state of and . is the only final state of and final state of and will be ordinary states in .

All the state of and are also state of .
All the moves of $M_1$ and $M_2$ are also moves of $M_3$. [Formal Construction]

It is easy to prove that

$$L(M_1) = L(M_2) = L(M_3)$$

Proof: To show that $L(M_2)$ we must show that

$$L(M_2) = L(M_3)$$

by following transition of

Starts at initial state and enters the start state of either following the transition of $M_1$, $M_2$, or $M_3$ consuming any input. WLOG, assume that, it enters the start state of $M_1$. From this point onward it has to follow only the transition of $M_1$, $M_2$, or $M_3$ to enter the final state of $M$, because this is the only way to enter the final state of $M$ by following the e-transition. (Which is the last transition & no input is taken at the transition). Hence the whole input $w$ is considered while traversing from the start state of $M_1$ to the final state of $M$. Therefore $M_1$ must accept.

Say $M_1$ or $M_2$. WLOG, say $M_1$. Therefore when $M_1$ process the string $w$, it starts at the initial state and enters the final state when $w$ consumed totally, by following its transition. Then $M_2$ also accepts $w$, by starting at state $M_1$ and taking $-transition$ enters the start state of $M_2$, -follows the moves to enter the final state of $M_2$ consuming input $w$ thus takes $-transition$ to $M_2$. Hence proved

$M_1$ Case(ii): Consider the RE $M_1$ denoting the language $L(r_1)$. We construct FA from $M_1$ & to accept as follows:

$$r_3 = r_1 r_2$$

$L(r_1) L(r_2)$
Create a new start state and a new final state

1. Add transition from
   - to the start state of
   - to
   - final state of to the start state of

2. All the states of are also the states of has 2 more states than that of namely and .

3. All the moves of are also included in.

By the transition of type (b), can accept .

By the transition of type (a), can enter the initial state of w/o any input and then follow all kinds moves of to enter the final state of and then following -transition can enter . Hence if any is accepted by then w is also accepted by . By the transition of type (b), strings accepted by can be repeated by any no of times & thus accepted by . Hence accepts and any string accepted by repeated (i.e. concatenated) any no of times. Hence

Case(iv) : Let =(). Then the FAis also the FA for (), since the use of parentheses does not change the language denoted by the expression

**Non-Deterministic Finite Automata**

Nondeterminism is an important abstraction in computer science. Importance of nondeterminism is found in the design of algorithms. For examples, there are many problems with efficient nondeterministic solutions but no known efficient deterministic solutions. (Travelling salesman, Hamiltonian cycle, clique, etc). Behaviour of a process is in a distributed system is also a good example of nondeterministic situation. Because
the behaviour of a process might depend on some messages from other processes that might arrive at arbitrary times with arbitrary contents.

It is easy to construct and comprehend an NFA than DFA for a given regular language. The concept of NFA can also be used in proving many theorems and results. Hence, it plays an important role in this subject.

In the context of FA nondeterminism can be incorporated naturally. That is, an NFA is defined in the same way as the DFA but with the following two exceptions:

- multiple next state.
- transitions.

**Multiple Next State :**

In contrast to a DFA, the next state is not necessarily uniquely determined by the current state and input symbol in case of an NFA. (Recall that, in a DFA there is exactly one start state and exactly one transition out of every state for each symbol in ).

This means that - in a state q and with input symbol a - there could be one, more than one or zero next state to go, i.e. the value of $\delta_q^a$ is a subset of Q. Thus $\omega$ which means that any one of $q_1$, $q_4$ could be the next state.

The zero next state case is a special one giving $\omega = \emptyset$, which means that there is no next state to input symbol when the automata is in state q. In such a case, we may think that the automata "hangs" and the input will be rejected.

**- transitions:**

In an -transition, the tape head doesn't do anything; it does not read and it does not move. However, the state of the automata can be changed. That is, it can go to zero, one or more states. This is written formally as $\delta : Q \times (\Sigma \cup \{\epsilon\}) \rightarrow \mathcal{P}(Q)$ implying that the next state could by any one of $q_0$ w/o consuming the next input symbol.

**Acceptance :**

Informally, an NFA is said to accept its input if it is possible to start in some start state and process , moving according to the transition rules and making choices along the way whenever the next state is not uniquely defined, such that when is completely processed (i.e. end of is reached), the automata is in an accept state. There may be several possible paths through the automation in response to an input since the start state is not determined and there are choices along the way because of multiple next states. Some of these paths may lead to accept states while others may not. The

$$L(M) = \{ \omega | \delta(q_0, \omega) \cap F = \emptyset \}$$

$$\sum^* \delta(q_0, \omega)$$
automation is said to accept if at least one computation path on input starting from at least one start state leads to an accept state- otherwise, the automation rejects input. Alternatively, we can say that, is accepted iff there exists a path with label from some start state to some accept state. Since there is no mechanism for determining which state to start in or which of the possible next moves to take (including the \( - \) transitions) in response to an input symbol we can think that the automation is having some "guessing" power to chose the correct one in case the input is accepted.

Example 1:
Consider the language \( L = \{0, 1\}^* | \text{The 3rd symbol from the right is 1}\}. The following four-state automation accepts \( L \).

The m/c is not deterministic since there \( \delta(q_1, 1) \) transitions from state \( q_1 \) on input 1 and no transition (zero transition) from \( q \) on both 0 & 1. For any string whose 3rd symbol from the right is a 1, there exists a sequence of legal \( \epsilon \) transitions leading from the start state \( q \) to the accept state \( \epsilon \). But for any string where 3rd symbol from the right is 0, there is no possible sequence of legal transitions leading from \( \epsilon \) and \( \epsilon \). Hence m/c accepts \( L \). How does it accept any string \( \epsilon \)?

Formal definition of NFA:

Formally, an NFA is a quintuple \( N = (Q, \Sigma, \delta, q_0, F) \) where \( Q \), \( \Sigma \), \( \delta \), \( q_0 \), and \( F \) bear the same meaning as for a DFA, but the transition function is redefined as follows:

\[ \delta'(q, a) = \{ p | p \in \delta(q, a) \} \quad q \in Q, \quad a \in \Sigma, \]

where \( P(Q) \) is the power set of \( Q \) i.e. \( P(Q) = \{ \{ q \} | q \in Q \} \] \( \cup \) \( \{ \} \). Otherwise.

The Language of an NFA:

From the discussion of the acceptance by an NFA, we can give the formal definition of a language accepted by an NFA as follows:

If \( N \) is an NFA, then the language accepted by \( N \) is written as \( L(N) \) is given by

\[ \forall w \in \Sigma^* \quad w \in L(N) \iff \exists \hat{\delta} \left( q_0, w \right) \in F \]

That is, \( L(N) \) contains at least one accepting state.

\[ \forall w \in \Sigma^* \quad \hat{\delta}' \left( q_0, w \right) = \hat{\delta} \left( q_0, w \right) \]
- transitions do not increase the power of an NFA. That is, any - NFA (NFA with transition), we can always construct an equivalent NFA without -transitions. The equivalent NFA must keep track where the NFA goes at every step during computation. This can be done by adding extra transitions for removal of every -transitions from the - NFA as follows.

\[ |\varphi| \]

If we removed the - transition from the - NFA, then we need to moves from state \( p \) to all the state on input symbol which are reachable from state \( q \) (in the - NFA) on same input symbol \( q \). This will allow the modified NFA to move from state \( p \) to all states on some input symbols which were possible in case of -NFA on the same input symbol. This process is stated formally in the following theories.

Theorem if \( L \) is accepted by an - NFA \( N \), then there is some equivalent without -transitions accepting the same language \( L \)

\[ \hat{\delta}'(q_0, \alpha) = \hat{\delta}'(q_0, x\alpha) \]

\[ = \hat{\delta}'(q_0, x, \alpha) \]

be the given with

\[ \hat{\delta}'(q_0, x, \alpha) \]

We construct

\[ \hat{\delta}'(p, \alpha) \]

Where, \( \hat{\delta}'(p, \alpha) \)

\[ = \hat{\delta}'(q_0, x) \]

\[ = \hat{\delta}'(q_0, x\alpha) \]

Other elements of \( N' \) and \( N \)

We can show that i.e. \( N' \) and \( N \) are equivalent.

\[ |\varphi| = 0 \]

We need to prove that i.e.

We will show something more, that is,
Basis: \( \ldots \), then

But by definition of \( M_3 \).

Induction hypothesis: Let the statement hold for all \( M_1 \) with \( \ldots \).

By definition of extension of \( M_2 \).

By induction hypothesis.

Assuming that

\[
q' \\
\in \quad M_1 \\
q' \quad f' \\
M_1
\]

Since

To complete the proof we consider the case

When \( M_1 \) i.e. \( q' \) then \( f' \)

\[
M_3 \\
M_3 \\
M_3 \\
M_1 \\
M_1 \\
M_1 \\
M_1 \\
M_1 \\
M_1
\]

\[
M_3 \\
M_3 \\
M_3 \\
M_1 \\
M_1 \\
M_1 \\
M_1 \\
M_1 \\
M_1
\]

\[
L(M_3) = [L(M_1)]' = (L(r_1))' = r_1'
\]

\[
r_3 \quad r_1 \quad M_1 \quad r_1
\]
and by the construction of wherever constrains a state in $F$.

(and thus is not in $F$), then with leads to an accepting state in $N'$ iff it leads to an accepting state in $N$ (by the construction of $N'$ and $N$).

Also, if (thus $w$ is accepted by $N'$ iff $w$ is accepted by $N$ (iff

If (and, thus in $M$ we load in $F$), thus is accepted by both $N'$ and $N$.

Let . If $w$ cannot lead to in $N$, then . (Since can add transitions to get an accept state). So there is no harm in making an accept state in $N'$.

Ex: Consider the following NFA with

<table>
<thead>
<tr>
<th>NFA $N'$</th>
<th>$q_0$</th>
<th>$q_0, q_1, q_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q_1$</td>
<td>$q_1$</td>
<td>$q_2$</td>
</tr>
<tr>
<td>$F$</td>
<td>$q_2$</td>
<td>$q_2$</td>
</tr>
</tbody>
</table>

$\delta(q_0, \epsilon) = q_2$  $\epsilon$-NFA

$\delta(q_0, \epsilon) = q_2$  $\delta(q_2, 0) = q_2$  $\delta(q_2, 1) = q_2$  $\delta(q_0, 0) = q_2$

Transition Diagram

$\delta(q_3, 1) = q_2$

$\epsilon$  0  1

$\epsilon$  $\epsilon$  $a \in \Sigma$

Transition diagram for the equivalent NFA without $\epsilon$-moves

$R \subseteq Q$

$\delta'(q, a) = \epsilon$-closure $\delta(q, a)$
Since the start state \( q_0 \) must be final state in the equivalent NFA.

Since and and we add moves and in the equivalent NFA. Other moves are also constructed accordingly.

\[ \delta \times \Sigma \to \mathcal{P}(\Sigma) \]

\( N \to (Q', \Sigma, \delta', q_0', F) \)

\( \epsilon \)

- closures:

The concept used in the above construction can be made more formal by defining the \( \epsilon \)-closure for a state (or a set of states). The idea of \( \epsilon \)-closure is that, when moving from a state \( p \) to a state \( q \) (or from a set of states \( S_i \) to a set of states \( S_j \)) an input we need to take account of all \( \epsilon \)-moves that could be made after the transition. Formally, for a given state \( q \),

\[ \delta(q) = q, \quad \delta'(\{p\}, \epsilon) = \{q\} \]

Similarly, for a given set

- closures:

\( \omega = a_1 a_2 \cdots a_n \in L(D) \)

\( q_0, q_1, q_2, \cdots, q_n \)

So, the construction of an equivalent NFA \( N' \) without \( \epsilon \)-transition from any NFA with moves, the first rule can now be written as

\[ \delta'(\{q_{i+1}\}, \epsilon) = \{q_{i+1}\} \quad \delta'(q_n) = q_n \in F \]

\[ \omega \in L(N) \]

\( L(N') = L(L) \)

CS6503 THEORY OF COMPUTATION

Equivalence of NFA and DFA

It is worth noting that a DFA is a special type of NFA and hence the class of languages accepted by DFAs is a subset of the class of languages accepted by NFAs.

Surprisingly, these two classes are in fact equal. NFAs appeared to have more power than DFAs because of generality enjoyed in terms of \( \epsilon \)-transition and multiple next
states. But they are no more powerful than DFAs in terms of the languages they accept.

Converting DFA to NFA

Theorem: Every DFA has an equivalent NFA

Proof: A DFA is just a special type of an NFA. In a DFA, the transition functions is defined from whereas in case of an NFA it is defined from and be a DFA. We construct an equivalent NFA as follows.

\[Q_i \rightarrow Q_j \] i.e.

If and

All other elements of \(N\) are as in \(D\).

If then there is a sequence of states such that

Then it is clear from the above construction of \(N\) that there is a sequence of states (in \(N\)) such that and and hence

Similarly we can show the converse.

Hence,

Given any NFA we need to construct as equivalent DFA i.e. the DFA need to simulate the behaviour of the NFA. For this, the DFA have to keep track of all the states where the NFA could be in at every step during processing a given input string.

There are possible subsets of states for any NFA with \(n\) states. Every subset corresponds to one of the possibilities that the equivalent DFA must keep track of. Thus, the equivalent DFA will have states.

The formal constructions of an equivalent DFA for any NFA is given below. We first consider an NFA without transitions and then we incorporate the affects of
Formal construction of an equivalent DFA for a given NFA without transitions.

Given an NFA without - moves, we construct an equivalent DFA as follows

i.e.

(i.e. every subset of Q which as an element in F is considered as a final state in DFA D)

for all and

where

That is,

To show that this construction works we need to show that \( L(D) = L(N) \) i.e.

Or,

We will prove the following which is a stranger statement thus required.
Basis If \(n = 0\), then \(w = \epsilon\).

So, by definition.

Inductions hypothesis: Assume inductively that the statement holds for length less than or equal to \(n\).

Inductive step

\[
\delta(q, a) \in (\delta(q, a)) = \delta^D(q^n, a)
\]

Let \(\delta^D(q^n, a) = \{q \in Q | q \in \epsilon - \text{ closure}(\delta(q^n, a))\}\) with

Now,

\[
q_0^D \in q_0^D
\]

\[
\epsilon \in 2^n
\]

Now, given any NFA with \(-\)-transition, we can first construct an equivalent NFA without \(-\)-transition and then use the above construction process to construct an equivalent DFA, thus, proving the equivalence of NFAs and DFAs.

It is also possible to construct an equivalent DFA directly from any given NFA with \(-\)-transition by integrating the concept of \(-\)-closure in the above construction.

Recall that, for any \(-\)-closure:

\[
\rightarrow q_0 \quad \{q_0, q_1\} \quad \phi \quad \phi \quad 33
\]

CS6503 THEORY OF COMPUTATION

In the equivalent DFA, at every step, we need to modify the transition function to keep track of all the states where the NFA can go on \(-\)-transitions. This is done by replacing \(-\)-closure, i.e. we now compute at every step as follows:
Besides this the initial state of the DFA D has to be modified to keep track of all the states that can be reached from the initial state of NFA on zero or more transitions.

This can be done by changing the initial state to -closure (\( q_0 \)).

It is clear that, at any step in the processing of an input string by the DFA D, it enters a state that corresponds to the subset of states that the NFA N could be in at that particular point. This has been proved in the constructions of an equivalent NFA for any -NFA.

If the number of states in the NFA is \( n \), then there are states in the DFA. That is, each state in the DFA is a subset of state of the NFA.

But, it is important to note that most of these states are inaccessible from the start state and hence can be removed from the DFA without changing the accepted language.

Thus, in fact, the number of states in the equivalent DFA would be much less than \( 2^n \).

Example: Consider the NFA given below.

<table>
<thead>
<tr>
<th>E</th>
<th>( q_0 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q_0 ), ( q_1 )</td>
<td>( { q_0 } )</td>
</tr>
<tr>
<td>( q_0 ), ( q_2 )</td>
<td>( { q_0 } )</td>
</tr>
<tr>
<td>( q_0 ), ( q_1, q_2 )</td>
<td>( { q_0 } )</td>
</tr>
<tr>
<td>( q_0 ), ( q_1, q_3 )</td>
<td>( { q_0 } )</td>
</tr>
<tr>
<td>( q_0 ), ( q_1, q_2 )</td>
<td>( { q_0 } )</td>
</tr>
<tr>
<td>( q_0 ), ( q_1, q_3 )</td>
<td>( { q_0 } )</td>
</tr>
<tr>
<td>( q_0 ), ( q_1, q_2 )</td>
<td>( { q_0 } )</td>
</tr>
</tbody>
</table>

Since there are \( 2^n \) states in the NFA, the number of states in the equivalent DFA will be \( 2^n \) states (representing all possible subset of states) in the equivalent DFA. The transition table of the DFA constructed by using the subset constructions process is produced here.

There will be states (representing all possible subset of states) in the equivalent DFA. The transition table of the DFA constructed by using the subset constructions process is produced here.
The final states are all those subsets that contain \( \{q_0\} \) (since in the NFA).

Let us compute one entry:

\[
\begin{array}{c}
0 \\
1 \\
1 \\
\end{array}
\]

Similarly, all other transitions can be computed.

\[
\forall a \in \Sigma \quad \delta^D(\mathcal{S}, a)
\]

Note that states are not accessible and hence can be removed. This gives us the following simplified DFA with only 3 states.

Corresponding Transition fig. for DFA.
It is interesting to note that we can avoid encountering all those inaccessible or unnecessary states in the equivalent DFA by performing the following two steps inductively.

1. If \( q_1 \) is the start state of the NFA, then make \(-\) closure \((\cdot)\) the start state of the equivalent DFA. This is definitely the only accessible state.
2. If we have already computed a set of states which are accessible. Then compute because these set of states will also be accessible.

Following these steps in the above example, we get the transition table given below

\[
\begin{array}{ccc}
\emptyset & \in & \forall \ a \in \mathcal{S} \\
\end{array}
\]

\[
\begin{array}{ccc}
r_1 & r_2 & \emptyset \\
q_1 & r_2 & q_1 \\
q_1 & r_2 & r_1 \\
q_1 & r_2 & \emptyset \\
(\emptyset) & r_1 & \emptyset \\
\end{array}
\]

Regular Expressions: Formal Definition

We construct REs from primitive constituents (basic elements) by repeatedly applying certain recursive rules as given below. (In the definition)
Definition: Let \( S \) be an alphabet. The regular expressions are defined recursively as follows.

**Basis:**

1. \( \epsilon \) is a RE.
2. \( \delta^R \) is a RE.
3. \( a \) is RE.

These are called primitive regular expression i.e. Primitive Constituents.

**Recursive Step:**

If \( R \) and \( S \) are REs over \( \Sigma \), then so are:

1. \( R \cup S \)
2. \( R \cdot S \)
3. \( R^* \)
4. \( R^+ \)

**Closure:** \( r \) is RE over \( \Sigma \) if and only if it can be obtained from the basis elements (primitive REs) by a finite number of applications of the recursive step.

**Example:** Let \( \Sigma = \{0, 1, 2\} \). Then \((0+21)*(1+2)\) is a RE, because we can construct this expression by applying the above rules as given in the following step:

<table>
<thead>
<tr>
<th>Steps</th>
<th>RE Constructed</th>
<th>Rule Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( 1 )</td>
<td>Rule 1(iii)</td>
</tr>
<tr>
<td>2</td>
<td>( R \cup S )</td>
<td>Rule 1(i)</td>
</tr>
<tr>
<td>3</td>
<td>( 1+)</td>
<td>Rule 2(iv) &amp; Step 3</td>
</tr>
<tr>
<td>4</td>
<td>( 0+21)</td>
<td>Rule 1(iii)</td>
</tr>
<tr>
<td>5</td>
<td>( 1+2 )</td>
<td>Rule 2(iv) &amp; Step 3</td>
</tr>
<tr>
<td>6</td>
<td>( (0+21)^* )</td>
<td>Rule 2(iv) &amp; Step 3</td>
</tr>
</tbody>
</table>

\( (0+21)^* \) is a RE because it can be constructed from the basis elements (primitive REs) by applying the recursive step a finite number of times.

---

Rule 2(iv) & Step 3
Language described by REs: Each describes a language (or a language is associated with every RE). We will see later that REs are used to attribute regular languages.

Notation: If $r$ is a RE over some alphabet, then $L(r)$ is the language associate with $r$. We can define the language $L(r)$ associated with (or described by) a REs as follows.

1. $\varepsilon$ is the RE describing the empty language i.e. $L(\varepsilon) = \{\}$. 
2. $\{\} = \{\}$ is a RE describing the language $\{\}$. 
3. $a$ is a RE denoting the language $\{a\}$ i.e. $L(a) = \{a\}$. 
4. If $L(r)$ and $L(s)$ are REs denoting language $L(r)$ and $L(s)$ respectively, then
   i) $r + s$ is a regular expression denoting the language $L(r) + L(s)$
   ii) $rs$ is a regular expression denoting the language $L(rs)$
   iii) $(r)$ is a regular expression denoting the language $L((r))$

Example: Consider the RE $0^*(0^*+1)$. Thus the language denoted by the RE is $L(0^*(0^*+1)) = L(0^*) L(0^*+1)$. By induction hypothesis

Consider the RE $ab + c$. The language described by the RE can be thought of either $L(a)L(b+c)$ or $L(ab) L(c)$ as provided by the rules (of languages described by REs) given already. But these two represents two different languages lending to ambiguity. To remove this ambiguity we can either

1) Use fully parenthesized expression- (cumbersome) or
2) Use a set of precedence rules to evaluate the options of REs in some order. Like other algebras mod in mathematics.

For REs, the order of precedence for the operators is as follows:

declare
- The star operator precedes concatenation and concatenation precedes union (+) operator.
- It is also important to note that concatenation & union (+) operators are associative and union operation is commutative.

Using these precedence rule, we find that the RE \(ab+c\) represents the language \(L(ab)\) \(L(c)\) i.e. it should be grouped as \((ab)+c\).

We can, of course change the order of precedence by using parentheses. For example, the language represented by the RE \(a(b+c)\) is \(L(a)L(b+c)\).

**Example:** The RE \(ab^*+b\) is grouped as \(((a(b^*))+b)\) which describes the language \(L(a)(L(b))^*\) \(L(b)\)

**Example:** The RE \((ab)^*+b\) represents the language \((L(a)L(b))^*\) \(L(b)\).

**Example:** It is easy to see that the RE \(0^*(1+1)^*\) represents the language of all strings over \(\{0,1\}\) which are either ended with 0 or 11.

**Example:** The regular expression \(r=(00)^*(11)^*1\) denotes the set of all strings with an even number of 0's followed by an odd number of 1's i.e.

**Note:** The notation is used to represent the RE \(rr^*\). Similarly, represents the RE \(rr\), denotes \(r\), and so on.

An arbitrary string over \(\{0,1\}\) is denoted as \((0+1)^*\).

**Exercise:** Give a RE \(r\) over \(\{0,1\}\) s.t. \(L(r)\) has at least one pair of consecutive 1's.

**Solution:** Every string in \(L(r)\) must contain 00 somewhere, but what comes before and what goes before is completely arbitrary. Considering these observations we can write the REs as \((0+1)^*11(0+1)^*\).

**Example:** Considering the above example it becomes clean that the RE \((0+1)^*11(0+1)^*+(0+1)^*00(0+1)^*\) represents the set of string over \(\{0,1\}\) that contains the substring 11 or 00.

**Example:** Consider the RE \(0^*10^*10^*\). It is not difficult to see that this RE describes the set of strings over \(\{0,1\}\) that contains exactly two 1's. The presence of two 1's in the RE and any no of 0's before, between and after the 1's ensure it.

**Example:** Consider the language of strings over \(\{0,1\}\) containing two or more 1's.

**Solution:** There must be at least two 1's in the RE somewhere and what comes before, between, and after is completely arbitrary. Hence we can write the RE as \((0+1)^*1(0+1)^*1(0+1)^*\). But following two REs also represent the same language, each ensuring presence of at least two 1's somewhere in the string.
Consider a RE $r$ over $\{0,1\}$ such that $L(r) = \{ \text{has no pair of consecutive 1's} \}$

**Solution:** Though it looks similar to ex. ..., it is harder to construct. We observer that, whenever a 1 occurs, it must be immediately followed by a 0. This substring may be preceded & followed by any no of 0's. So the final RE must be a repetition of strings of the form: 00...0100...0 i.e. $0^*100^*$. So it looks like the RE is $(0^*100^*)^*$. But in $(0^*)^*$ case the strings ending in 1 or consisting of all 0's are not accounted for. Taking these observations into consideration, the final RE is $r = (0^*100^*)(1+)^*0^*(1+)$. This is a shorter expression but represents the same language.

**Alternative Solution:**
The language can be viewed as repetitions of the strings 0 and 01. Hence get the RE as $r = (0+10)^*(1+)^*$. This is a shorter expression but represents the same language.

### Regular Expression:

FA to regular expressions:

FA to RE (REs for Regular Languages):

**Lemma:** If a language is regular, then there is a RE to describe it. i.e. if $L = L(M)$ for some DFA $M$, then there is a RE $r$ such that $L = L(r)$. 

**Proof:** We need to construct a RE $r$ such that. Since $M$ is a DFA, it has a finite no of states. Let the set of states of $M$ is $Q = \{1, 2, 3, ..., n\}$ for some integer $n$. [Note: if the $n$ states of $M$ were denoted by some other symbols, we can always rename those to indicate as 1, 2, 3, ..., $n$]. The required RE is constructed inductively.

**Notations:** $r_i^j(k)$ is a RE denoting the language which is the set of all strings $w$ such that $w$ is the label of a path from state $i$ to state $j$ in $M$, and that path has no intermediate state whose number is greater than $k$. (i & j (begining and end pts) are not considered to be "intermediate" so i and/or j can be greater than k)

We now construct inductively, for all $i, j \in Q$ starting at $k = 0$ and finally reaching $k = n$.

**Basis:** $k = 0$, i.e. the paths must not have any intermediate state (since all states are numbered 1 or above). There are only two possible paths meeting the above condition:

1. A direct transition from state $i$ to state $j$.  

---

Getmynotes.com
\( o = a \) if there is a transition from state \( i \) to state \( j \) on symbol the single symbol \( a \).

\( o = \) if there are multiple transitions from state \( i \) to state \( j \) on symbols.

\( o = f \) if there is no transition at all from state \( i \) to state \( j \).

2. All paths consisting of only one node i.e. when \( i = j \). This gives the path of length 0 (i.e. the RE denoting the string ) and all self loops. By simply adding \( I \) to various cases above we get the corresponding REs i.e.

\( o = + a \) if there is a self loop on symbol \( a \) in state \( i \).

\( o = + \) if there are self loops in state \( i \) as multiple symbols.

\( o = \) if there is no self loop on state \( i \).

**Induction:**

Assume that there exists a path from state \( i \) to state \( j \) such that there is no intermediate state whose number is greater than \( k \). The corresponding RE for the label of the path is

There are only two possible cases:

1. The path dose not go through the state \( k \) at all i.e. number of all the intermediate states are less than \( k \). So, the label of the path from state \( i \) to state \( j \) is the language described by the RE.

2. The path goes through the state \( k \) at least once. The path may go from \( i \) to \( j \) and \( k \) may appear more than once. We can break the into pieces as shown in the figure 7.
1. The first part from the state \(i\) to the state \(k\) which is the first recurrence. In this path, all intermediate states are less than \(k\) and it starts at \(i\) and ends at \(k\). So the \(R\) denotes the language of the label of path.

2. The last part from the last occurrence of the state \(k\) in the path to state \(j\). In this path also, no intermediate state is numbered greater than \(k\). Hence the \(R\) denoting the language of the label of the path.

3. In the middle, for the first occurrence of \(k\) to the last occurrence of \(k\), represents a loop which may be taken zero times, once or any no of times. And all states between two consecutive \(k\)’s are numbered less than \(k\).

Hence the label of the path of the part is denoted by the \(R\). The label of the path from state \(j\) to \(j\) is the concatenation of these 3 parts which is

Since either case 1 or case 2 may happen the labels of all paths from state \(i\) to \(j\) is denoted by the following \(R\):

We can construct for all \(i, j \in \{1, 2, \ldots, n\}\) in increasing order of \(k\) starting with the basis \(k = 0\) upto \(k = n\) since \(\epsilon\) depends only on expressions with a small superscript (and hence will be available). WLOG, assume that state 1 is the start state and are the \(m\) final states where \(j\) are the \(m\) final states where \(j\) and . According to the convention used, the language of the automata can be denoted by the \(R\):

Regular Grammar:

A grammar is right-linear if each production has one of the following three forms:
A, B, A

A, A

A

\( \delta(q_0, a_1) = q_1 \)

\( \delta(q_{k-1}, a_k) = q_k \)

A right or left-linear grammar is called a regular grammar.

Regular grammar and Finite Automata are equivalent as stated in the following theorem.

**Theorem:** A language \( L \) is regular iff it has a regular grammar. We use the following two lemmas to prove the above theorem.

**Lemma 1:** If \( L \) is a regular language, then \( L \) is generated by some right-linear grammar.

**Proof:** Let \( M \) be a DFA that accepts \( L \).

Let \( N = \{ N \text{, } \Sigma, P, S \} \)

\[ N = Q, \quad g = (N, \Sigma, P, S) \]

[ Note: If \( \), then \( \) ]

\[ \text{For} \ M \text{ to accept } w, \text{ there must be a sequence of states } \]

\[ \text{such that } \]

\[ w = a_1a_2...a_k \in L(G) \]

We construct the right-linear grammar by letting

\( q_k \in F \)

By construction, the grammar \( G \) will have one production for each of the above transitions. Therefore, we have the corresponding derivation.
Hence \( w \in L(G) \).

\[ S \overset{\alpha}{\rightarrow} a_1 a_2 \cdots a_k (= w) \]

Conversely, if, then the derivation of \( w \) in \( G \) must have the form as given above. But, then the construction of \( G \) from \( M \) implies that

\[
\delta(q_1, a_1) = q_2 \quad \text{where} \quad \delta(q_1, a_2) = q_3
\]

**Lemnà 2**: Let \( M \) be a right-linear grammar. Then \( L(G) \) is a regular language.

Proof: To prove it, we construct a FA \( M \) from \( G \) to accept the same language.

\[ w = a_1 a_2 \cdots a_k \in L(M) \]

is constructed as follows:

\[ w = a_1 a_2 \cdots a_k \quad (i.e. \ is \ a \ special \ symbol \ not \ in \ N) \]

For any \( \delta(q_i, a) \) is defined as

\[ A \rightarrow cB \quad A \rightarrow Be \]

We now show that this construction works.

Let \( G \) be a right-linear grammar with \( L(G) \) is a regular language.

Then there is a derivation of \( w \) in \( G \) of the form

\[ G: S \rightarrow 0A \sim 0 \]

\[ A \rightarrow BS \]

By contradiction of \( M \), there must be a sequence of transitions
implying that $w$ is accepted by $M$, then because the only accepting state of $M$, the transitions causing $w$ to be accepted by $M$ will be of the form given above. These transitions corresponds to a derivation of $w$ in the grammar $G$. Hence, completing the proof of the lemma.

Given any left-linear grammar $G$ with production of the form, we can construct from it a right-linear grammar by replacing every production of $G$ of the form with

It is easy to prove that. Since is right-linear, is regular. But then so are

i.e. because regular languages are closed under reversal.

Putting the two lemmas and the discussions in the above paragraph together we get the proof of the theorem-

A language $L$ is regular iff it has a regular grammar

**Example** : Consider the grammar

It is easy to see that $G$ generates the language denoted by the regular expression $(01)^*0$. The construction of lemma 2 for this grammar produces the following FA. This FA accepts exactly $(01)^*1$.

**Decisions Algorithms for CFL**

In this section, we examine some questions about CFLs we can answer. A CFL may be represented using a CFG or PDA. But an algorithm that uses one representation can be made to work for the others, since we can construct one from the other.

Given any CFL $L$, there is a CFG $G$ to generate it. We can determine, using the construction described in the context of elimination of useless symbols, whether the start symbol is useless. If so, then otherwise not.

**Testing Emptiness** :

**Theorem** : There are algorithms to test emptiness of a CFL.

**Proof** : Given any CFL $L$, there is a CFG $G$ to generate it. We can determine, using the construction described in the context of elimination of useless symbols, whether the start symbol is useless. If so, then otherwise not.

**Testing Membership** :

Given a CFL $L$ and a string $x$, the membership problem is to determine whether
Given a PDA $P$ for $L$, simulating the PDA on input string $x$ does not quite work, because the PDA can grow its stack indefinitely on input, and the process may never terminate, even if the PDA is deterministic.

So, we assume that a CFG is given such that $L = L(G)$. Let us first present a simple but inefficient algorithm.

Convert $G$ to in CNF generating. If the input string, then we need to determine whether and it can easily be done using the technique given in the context of elimination of -production. If, then iff. Consider a derivation under a grammar in CNF. At every step, a production in CNF is used, and hence it adds exactly one terminal symbol to the sentential form. Hence, if the length of the input string $x$ is $n$, then it takes exactly $n$ steps to derive $x$ (provided $x$ is in $L(G)$).

Let the maximum number of productions for any nonterminal in $G$ is $K$. So at every step in derivation, there are at most $K$ choices. We may try out all these choices, systematically, to derive the string $x$ in $L(G)$. Since there are at most $i.e.$ choices. This algorithm is of exponential time complexity. We now present an efficient (polynomial time) membership algorithm.

Let $\omega \in \{0, 1\}^* \setminus \emptyset$.

**Pumping Lemma:**

**Limitations of Finite Automata and Non-regular Languages:**

The class of languages recognized by FA's is strictly the regular set. There are certain languages which are non-regular i.e. cannot be recognized by any FA.

Consider the language $L(r) = \{ w \mid w \in L(\{a^n b^n\}) \}$.

But the number of $a$'s is not limited and may be much larger than the number of states since the string may be arbitrarily long. Since the amount of information the automaton need to remember is unbounded.

A finite automaton cannot remember this many $a$'s with finite memory (i.e. finite number of states). The fact that FAs have finite memory imposes some limitations on the structure of the languages recognized. Inductively, we can say that a language is regular only if in processing any string in this language, the information that has to be remembered at any point is strictly limited. The argument given above to show that is non regular is informal. We now present a formal method for showing that certain languages such as are non regular.

**Properties of CFL's**

**Closure properties of CFL:**
We consider some important closure properties of CFLs.

**Theorem:** If \( L_1 \) and \( L_2 \) are CFLs then so is \( L_3 = L_1 \cup L_2 \).

**Proof:** Let \( G_1 \) and \( G_2 \) be CFGs generating. Without loss of generality, assume that \( w \in L(G_1) \) or \( w \in L(G_2) \). Let \( S \) be a nonterminal not in \( N_1 \) or \( N_2 \). We construct the grammar \( G_3 \) from \( G_1 \) and \( G_2 \), where

\[
\begin{align*}
N_1 & \cup N_2 & \quad S_1 \rightarrow w \\
S_1 \rightarrow & \quad w \\
S_1 \rightarrow & \quad w \\
G_1 & \quad G_2 \\
G_2 & \quad G_1 \\
S_3 & \rightarrow \quad w \\
S_1 \rightarrow & \quad w \\
S_1 \rightarrow & \quad w \\
S_1 \rightarrow & \quad w \\
\end{align*}
\]

We now show that

\[ L(G_3) = L_1 \cup L_2 \]

Thus proving the theorem.

Let \( L_3 = L_1 \cup L_2 \). All productions applied in their derivation are also in \( L_3 \). Hence

\[ L_1 \quad L_2 \]

Similarly, if

\[ N_1 \quad N_2 \]

Then \( \Sigma_2 = \Sigma_1 \cup \Sigma_2 \)

Thus

\[ P_3 = P_1 \cup P_2 \cup \{ S_3 \rightarrow S_1 S_2 \} \]

Conversely, let \( G_3 \) and the first step in this derivation must be either

\[ S \rightarrow \quad w \]

Considering the former case, we have

\[ P_1 \subseteq P \quad P_2 \subseteq P \quad L_1 L_2 \subseteq L(G_3) \]

Since \( S \) is the start symbol of \( G_3 \). Hence, giving
So, as claimed.

**Theorem:** If $L_1$ and $L_2$ are CFLs, then so is $L_1 \cup L_2$.

Proof: Let $G_1$ and $G_2$ be the CFGs generating $L_1$ and $L_2$ respectively. Again, we assume that $M_1$ and $M_2$ are disjoint, and $S$ is a nonterminal not in $M_1$ or $M_2$. we construct the CFG $G_3$ from $G_1$ and $G_2$, where

$$
G_3 = (N, \Sigma, P, S)
$$

We claim that $L(G_3) = L_1 \cup L_2$. To prove it, we first assume that $w \in L_1$ and $w = \gamma_1 \gamma_2 \cdots \gamma_k$. Then $S \rightarrow \epsilon$ and $P \subseteq P'$ such that $w \in L^{+}$.

We can derive the string $xy$ in $G'$ as shown below.

$$
S \rightarrow \gamma_1 \gamma_2 \cdots \gamma_k
$$

since and . Hence .

$$
L(G') - (L(G'))^* = L
$$

We will prove the converse, let . Then the derivation of $w$ in $L$ will be of the form $C_i C_j$, where $i, j \geq 0$.

i.e. the first step in the derivation must see the rule and . Again, since and are disjoint and and , some string $x$ will be generated from also in ) and such that .

Thus

Hence and .
This means that $W$ can be divided into two parts $X, Y$ such that $X = \sum_{i=1}^{n} \sum_{j=2}^{m} r_{ij}$ and $Y = \sum_{j=2}^{m} r_{1j}$. Thus this completes the proof.

**Theorem:** If $L$ is a CFL, then so is $L^*$.

**Proof:** Let $G = (N, \Sigma, S, P)$ be the CFG generating $L$. Let us construct the CFG $G'$ from $G$ where

$$r_{ij} = \sum_{x \in \sum} \sum_{y \in \sum} r_{ij}$$

We now prove that $G'$ can generate $W$ in one step by using the productions since $W$ can generate any string in $L$.

For any $n > 1$ we can write

$$w = a_1 a_2 \ldots a_k \in L(M)$$

The nonterminal $X$ generates strings of the form $a_1 a_2 \ldots a_k \in L(M)$ and $C$ generates strings of the form $a_1 a_2 \ldots a_k \in L(M)$. Hence, $S$ generates

Using similar reasoning, it can be shown that the following grammar also a CFL.

**Theorem:** CFLs are not closed under intersection.

**Proof:** We prove it by giving a counter example. Consider the language $L_1$ and hence a CFL $L_2$.

$$G = (N, \Sigma, S, P, S')$$

First $(n-1)$-steps uses the production $S \rightarrow SS$ producing the sentential form of $n$ numbers of $S$'s. The nonterminal $S$ in the $l$-th position then generates using production in $P$ (which are also in $P'$) for $l > 1$ and none other.

$$\Rightarrow \Rightarrow \Rightarrow \in \Sigma$$

It is also easy to see that $G$ can generate the empty string, any string in $L$ and any string.

Hence

**Theorem:** CFLs are not closed under intersection.
But, and is already shown to be not context-free.

Hence proof.

**Theorem:** A CFL's are not closed under complementations

**Proof:** Assume, for contradiction, that CFL's are closed under complementation. Since, CFL's are also closed under union, the language \( L \) where \( L \) and \( L' \) are CFL's must be CFL. But by DeMorgan's law

This contradicts the already proved fact that CFL's are not closed under intersection.

But it can be shown that the CFL's are closed under intersection with a regular set.

**Theorem:** If \( L \) is a CFL and \( R \) is a regular language, then \( L \cap R \) is a CFL.

**Proof:** Let \( P \) be a PDA for \( L \) and let \( D \) be a DFA for \( R \).

We construct a PDA \( M \) from \( P \) and \( D \) as follows

where \( M \) is defined as

contains \( w \) iff

The idea is that \( M \) simulates the moves of \( P \) and \( D \) parallely on input \( w \), and accepts \( w \) iff both \( P \) and \( D \) accepts. That means, we want to show that

We apply induction on \( n \), the number of moves, to show that
Basic Case is $n=0$. Hence $\vdash_{\Sigma}$. For this case it is trivially true.

Inductive hypothesis: Assume that the statement is true for $n-1$.

Inductive Step: Let $w=xa$ and $G=(N,\Sigma, P, S')$

Let $G=(N,\Sigma, P, S')$

By inductive hypothesis, and $A \vdash a$

From the definition of $G'$ and considering the $n$-th move of the PDA $M$ above, we have

$A \vdash_{a} a$

Hence $A \vdash_{G} a$

If $A \rightarrow BC$, then $A \vdash_{G} a$ and we got that if $M$ accepts $w$, then both $P$ and $D$ accepts it.

We can show the converse, in a similar way. Hence $L$ is a CFL (since it is accepted by a PDA $M$).

Example: Consider the language $L$ which is already known to be not context-free. Hence

Theorem: CFL's are closed under reversal. That is if $L$ is a CFL, then so is $L^R$.

Proof: Let the CFG $G$ generates $L$. We construct a CFG $G'$ which is in CNF. We now show that $L(G') = L^R$, thus proving the theorem.

We need to prove that

iff.

The proof is by induction on $n$, the number of steps taken by the derivation. We assume, for simplicity (and of course without loss of generality), that $G$ and hence $G'$ are in CNF.

The basis is $n=1$ in which case it is trivial. Because must be either or BC with
The converse case is exactly similar

**Substitution:**

Let be a language (over any alphabet). This defines a function \( S \), called substitution, on denoted as- for all

This definition of substitution can be extended further to apply strings and language as well.

If , where , is a string in , then

Similarly, for any language \( L \),

The following theorem shows that CFLs are closed under substitution.

**Theorem:** Let \( L \) is a CFL, and \( S \) is a substitution on such that is a CFL for all , thus \( S(L) \) is a CFL

**Proof:** Let \( L = L(G) \) for a CFG and for every , for some

Without loss of generality, assume that the sets of nonterminals \( N \) and 's are disjoint.

52
consists of

1. and
2. The production of \( P \) but with each terminal \( a \) in the right hand side of a production replaced by everywhere.

We now want to prove that this construction works i.e. iff

If Part: Let then according to the definition there is some string and

for such that

We will show that

From the construction of we find that, there is a derivation corresponding to the string (since contains all productions of \( G \) but every \( a_i \) replaced with in the RHS of any production).

Every is the start symbol of and all productions of also included in Hence

\[
\begin{align*}
S' & \Rightarrow \varepsilon \\
& \in \\
\in \\
& \in L(G') & x \in L(G)
\end{align*}
\]

Therefore,

(Only-if Part) Let . Then there must be a derivative as follows:

(using the production of \( G \) include in as modified by (step 2) of the construction of ).

Each can only generate a string , since each 's and \( N \) are disjoin. Therefore,

since

\[
L = \{ a^n b^n | n \geq 0 \}
\]

53
The string is formed by substituting strings for each and hence.

**Theorem:** CFL's are closed under homomorphism

**Proof:** Let be a CFL, and is a homomorphism on , i.e. for some alphabets consider the following substitution: Replace each symbol by the language consisting of the only string , i.e.

\[
\text{for all. Then, it is clear that, } h(L) = s(L). \text{ Hence, CFL's being closed under substitution must also be closed under homomorphism.}
\]

\[
L_1 \cup L_2 \subseteq L(G_3)
\]

\[
\begin{align*}
G_1 &= (N_1, \Sigma_1, P_1, S_1) \quad & G_2 &= (N_2, \Sigma_2, P_2, S_2) \\
N_1 \cap N_2 &= \emptyset \quad & S_3 &= N_1 \cup N_2 \\
G_3 &= (N_3, \Sigma_3, P_3, S_3) \\
N_3 &= N_1 \cup N_2 \cup \{S_3\} \\
\Sigma_3 &= \Sigma_1 \cup \Sigma_2 \\
P_3 &= P_1 \cup P_2 \cup \{S_3 \rightarrow S_1 \mid S_2\} \\
L(G_3) &= L(G_1) \cup L(G_2) = L_1 \cup L_2
\end{align*}
\]
Grammar

A grammar is a mechanism used for describing languages. This is one of the most simple but yet powerful mechanism. There are other notions to do the same, of course.

In everyday language, like English, we have a set of symbols (alphabet), a set of words constructed from these symbols, and a set of rules using which we can group the words to construct meaningful sentences. The grammar for English tells us what are the words in it and the rules to construct sentences. It also tells us whether a particular sentence is well-formed (as per the grammar) or not. But even if one following the rules of the English grammar it may lead to some sentences which are not meaningful at all, because of imprecision and ambiguities involved in the language. In English grammar we use many other higher level constructs like noun-phrase, verb-phrase, article, noun, predicate, verb etc. A typical rule can be defined as

\[
\alpha \rightarrow \beta \quad \alpha, \beta \in (N \cup \Sigma)^* \]

meaning that "a sentence can be constructed using a 'noun-phrase' followed by a predicate".

Some more rules are as follows:

\[
\alpha \rightarrow \beta \quad \alpha \in (N \cup \Sigma)^* \\
\beta \in (N \cup \Sigma)^* \\
\delta \alpha \gamma \rightarrow \delta \beta \gamma \\
\delta \alpha \gamma \rightarrow \epsilon \beta \gamma
\]

with similar kind of interpretation given above.

If we take \{a, an, the\} to be <article>; cow, bird, boy, Ram, pen to be examples of <noun>; and eats, runs, swims, walks, are associated with <verb>, then we can construct the sentence- a cow runs, the boy eats, an pen walks- using the above rules. Even though all sentences are well-formed, the last one is not meaningful. We observe that we start with the higher level construct <sentence> and then reduce it to <noun-phrase>, <article>, <noun>, <verb> successively, eventually leading to a group of words associated with these constructs.

These concepts are generalized in formal language leading to formal grammars. The word 'formal' here refers to the fact that the specified rules for the language are explicitly stated in terms of what strings or symbols can occur. There can be no ambiguity in it.

Formal definitions of a Grammar

\[ G = (N, \Sigma, P, S) \]

\[ L(G) = \{ \gamma \in \Sigma^* \mid S \Rightarrow^* \gamma \} \]

A grammar \( G \) is defined as a quadruple.

\( N \) is a non-empty finite set of non-terminals or variables,

is a non-empty finite set of terminal symbols such that

\( \varphi \in L(G) \) is a special non-terminal (or variable) called the start symbol, and

finite set of production rules.
In other words, $P$ is a finite set of production rules of the form

The production rules specify how the grammar transforms one string to another. Given a string, we say that the production rule is applicable to this string, since it is possible to use the rule to rewrite the (in ) to obtaining a new string. We say that derives and is denoted as

By applying the production rules in arbitrary order, any given grammar can generate many strings of terminal symbols starting with the special start symbol, $S$, of the grammar. The set of all such terminal strings is called the language generated (or defined) by the grammar.

Formally, for a given grammar, the language generated by $G$ is

That is iff .
If \( \frac{a}{b} \), we must have for some \( \frac{a}{b} \), denoted as a derivation sequence of \( w \), the strings are denoted as sentential forms of the derivation.

**Example:** Consider the grammar, where \( N = \{ S \} \), \( \Sigma = \{ a, b \} \) and \( P \) is the set of the following production rules

\[
\{ S \rightarrow ab, S \rightarrow aSb \}
\]

Some terminal strings generated by this grammar together with their derivation is given below.

\[
\begin{align*}
S & \rightarrow ab \\
S & \rightarrow aSb \quad aabb \\
S & \rightarrow aSb \quad aaSbb \quad aaabbb
\end{align*}
\]

It is easy to prove that the language generated by this grammar is

By using the first production, it generates the string \( ab \) (for \( i = 1 \)).

To generate any other string, it needs to start with the production \( S \rightarrow ab \) and then the non-terminal \( S \) in the RHS can be replaced either by \( ab \) (in which we get the string \( aabb \)) or the same production \( S \rightarrow aSb \) can be used one or more times. Every time it adds an 'a' to the left and a 'b' to the right of \( S \), thus giving the sentential form.

When the non-terminal is replaced by \( ab \) (which is then only possibility for generating a terminal string) we get a terminal string of the form.

There is no general rule for finding a grammar for a given language. For many languages we can devise grammars and there are many languages for which we cannot find any grammar.

**Example:** Find a grammar for the language

It is possible to find a grammar for \( L \) by modifying the previous grammar since we need to generate an extra \( b \) at the end of the string. We can do this by adding a production \( S \rightarrow Bb \) where the non-terminal \( B \) generates as given in the previous example.

Using the above concept we devise the following grammar for \( L \).

\[
\text{where, } N = \{ S, B \}, \quad P = \{ S \rightarrow Bb, B \rightarrow ab, B \rightarrow aBb \}
\]

Parse Trees:
Construction of a Parse tree:

```
       P
      /|
     P 0
    /|
   1  P
  /|
 ε 1
```

Figure 5.5: A parse tree showing the derivation $P \Rightarrow 0110$

If we look at the leaves of any parse tree and concatenate them from the left, we get a string, called the yield of the tree, which is always a string that is derived from the root variable. The fact that the yield is derived from the root will be proved shortly. Of special importance are those parse trees such that:

1. The yield is a terminal string. That is, all leaves are labeled either with a terminal or with $\epsilon$.
2. The root is labeled by the start symbol.
When a grammar fails to provide unique structures, it is sometimes possible to redesign the grammar to make the structure unique for each string in the language. Unfortunately, sometimes we cannot do so. That is, there are some CFL’s that are “inherently ambiguous”; every grammar for the language puts more than one structure on some strings in the language. Grammar lets us generate expressions with any sequence of * and + operators, and the productions $E \rightarrow E + E \mid E * E$ allow us to generate these expressions in any order we choose.

**Example 5.25:** For instance, consider the sentential form $E + E * E$. It has two derivations from $E$:

1. $E \Rightarrow E + E \Rightarrow E + E * E$

2. $E \Rightarrow E * E \Rightarrow E + E * E$

Notice that in derivation (1), the second $E$ is replaced by $E * E$, while in derivation (2), the first $E$ is replaced by $E + E$. Figure 5.17 shows the two parse trees, which we should note are distinct trees.

![Yield of a Parse tree](image)

(a) (b)

Figure 5.17: Two parse trees with the same yield we say a CFG $G = (V, T, P, S)$ is ambiguous if there is at least one string $w$ in $T^*$ for which we can find two different parse trees, each with root labeled $S$ and yield $w$. If each string has at most one parse tree in the grammar, then the grammar is unambiguous.
UNIT 3  PUSH DOWN AUTOMATA

Regular language can be characterized as the language accepted by finite automata. Similarly, we can characterize the context-free language as the language accepted by a class of machines called "Pushdown Automata" (PDA). A pushdown automation is an extension of the NFA.

It is observed that FA have limited capability. (in the sense that the class of languages accepted or characterized by them is small). This is due to the "finite memory" (number of states) and "no external memory" involved with them. A PDA is simply an NFA augmented with an "external stack memory". The addition of a stack provides the PDA with a last-in, first-out memory management capability. This "Stack" or "pushdown" be used to record a potentially unbounded information. It is due to this memory management capability with the help of the stack that a PDA can overcome the memory limitations that prevents a FA to accept many interesting languages like. Although, a PDA can store an unbounded amount of information on the stack, its access to the information on the stack is limited. It can push an element onto the top of the stack and pop off an element from the top of the stack. To read down into the stack the top elements must be popped off and are lost. Due to this limited access to the information on the stack, a PDA still has some limitations and cannot accept some other interesting languages.

As shown in figure, a PDA has three components: an input tape with read only head, a finite control and a pushdown store.

The input head is read-only and may only move from left to right, one symbol (or cell) at a time. In each step, the PDA pops the top symbol off the stack; based on this symbol, the input symbol it is currently reading, and
its present state, it can push a sequence of symbols onto the stack, move its read-only head one cell (or symbol) to the right, and enter a new state, as defined by the transition rules of the PDA.

PDA are nondeterministic, by default. That is, transitions are also allowed in which the PDA can pop and push, and change state without reading the next input symbol or moving its read-only head. Besides this, there may be multiple options for possible next moves.

**Formal Definitions:** Formally, a PDA \( M \) is a 7-tuple \( M = (Q, \Sigma, \Gamma, \delta, q_0, Z_0, F) \) where,

- \( Q \) is a finite set of states,
- \( \Sigma \) is a finite set of input symbols (input alphabets),
- \( \Gamma \) is a finite set of stack symbols (stack alphabets),
- \( Q \) is a transition function from \( \Sigma \) to subset of \( \Gamma \),
- \( q_0 \) is the start state,
- \( Z_0 \) is the initial stack symbol, and
- \( F \subseteq Q \) is the final or accept states.

**Explanation of the transition function,**

\( \delta(q, a, Z) = \{(p_1, \beta_1), (p_2, \beta_2), \ldots, (p_k, \beta_k)\} \)

If, for any, This means intuitively that whenever the PDA is in state \( q \) reading input symbol \( a \) and \( Z \) on top of the stack, it can nondeterministically for any \( i \),

- go to state \( 1 \leq i \leq k \)
- pop \( Z \) off the stack
- push onto the stack (where (The usual convention is that if \( p_i \) will be at the top and at the bottom.)
- move read head right one cell past the current symbol \( a \).
- \( \beta \) \( \beta \) \( \beta \) \( \beta \)
- \( X_1 \) \( X_2 \) \( X_3 \) \( X_4 \) \( X_5 \)
- means intuitively that whenever the PDA is in state \( q \) with \( Z \) on the top of the stack regardless of the current input symbol, it can nondeterministically for any \( i \),

\( \delta(q, \varepsilon, Z) = \{(p_1, \beta_1), (p_2, \beta_2), \ldots, (p_k, \beta_k)\} \)

If \( a = \varepsilon \), then

\( \beta \) \( \beta \) \( \beta \) \( \beta \) \( \beta \)
State transition diagram: A PDA can also be depicted by a state transition diagram. The labels on the arcs indicate both the input and the stack operation. The transition for and is depicted by

Final states are indicated by double circles and the start state is indicated by an arrow to it from nowhere.

**Configuration or Instantaneous Description (ID):**

A configuration or an instantaneous description (ID) of PDA at any moment during its computation is an element describing the current state, the portion of the input remaining to be read (i.e. under and to the right of the read head), and the current stack contents. Only these three elements can affect the computation from that point on and, hence, are parts of the ID.

The start or initial configuration (or ID) on input is . That is, the PDA always starts in its start state, with its read head pointing to the leftmost input symbol and the stack containing only the start/initial stack symbol.

The "next move relation" one figure describes how the PDA can move from one configuration to another in one step.

Formally,

iff

'a' may be or an input symbol.

Let I, J, K be IDs of a PDA. We define we write I \(\rightarrow\) K, if ID I can become K after exactly i moves. The relations and define as follows

I \(\rightarrow\) K

I \(\leftarrow\) J if \ such that I \(\rightarrow\) K and K \(\rightarrow\) J

I \(\leftarrow\) J if \ such that I \(\rightarrow\) J.
That is, is the reflexive, transitive closure of $I$. We say that $I$ follows from the ID $J$ if the ID $J$ follows from the ID $I$ in

\[
\begin{align*}
\frac{\vdash \beta_1 \beta_2 \ldots \beta_n \beta_2 \vdash \beta_2 & \vdash \alpha_1 \beta_2}{\vdash \beta_1 \beta_2 \ldots \beta_n \beta_2 \vdash \alpha_1 \beta_2} \\
\vdash \gamma \beta_2 & \vdash \gamma \\
= & w \\
& w = \gamma \beta_2 \gamma \\
L \subseteq & \Sigma^* \\
\Sigma & h : \Sigma \rightarrow \Delta^* \\
\Delta & a \in \Sigma \\
\sigma(a) & = \{h(a)\} \\
& a \in \Sigma
\end{align*}
\]
Language accepted by a PDA $M$

There are two alternative definitions of acceptance as given below.

1. Acceptance by final state:

Consider the PDA. Informally, the PDA $M$ is said to accept its input by final state if it enters any final state in zero or more moves after reading its entire input, starting in the start configuration on input.

Formally, we define $L(M)$, the language accepted by final state to be

$$
\{ \_ \mid \text{ for some } \_ \text{ and } \_
\}
$$

2. Acceptance by empty stack (or Null stack):

The PDA $M$ accepts its input by empty stack if starting in the start configuration on input, it ever empties the stack w/o pushing anything back on after reading the entire input. Formally, we define $N(M)$, the language accepted by empty stack, to be

$$
\{ \_ \mid \text{ for some } \_
\}
$$

Note that the set of final states, $F$ is irrelevant in this case and we usually let the $F$ to be the empty set i.e. $F = Q$.

**Example 1**: Here is a PDA that accepts the language $L(M)$.

, and consists of the following transitions
The PDA can also be described by the adjacent transition diagram.

\[ (q_1, aabab, z) \xrightarrow{(q_2, aba\delta, az)} \]
\[ (q_2, bab, aaz) \]

Informally, whenever the PDA \( M \) sees an input \( a \) in the start state with the start symbol \( z \) on the top of the stack it pushes \( a \) onto the stack and changes state to \( q_1 \). (to remember that it has seen the first 'a'). On state \( q_2 \) if it sees anymore \( a \), it simply pushes it onto the stack. Note that when \( M \) is on state \( q_2 \), the symbol on the top of the stack can only be \( a \). On state \( q_3 \) if it sees the first \( b \) with \( a \) on the top of the stack, then it needs to pop off the \( a \) from the top of the stack and enters in state \( q_3 \) (to remember that the comparison process has begun). On state \( q_3 \) it expects only \( b \)'s in the input (if it sees any more \( a \) in the input then the input will not be in the proper form of \( a^n b^n \)). Hence there is no more on input \( a \) when it is in state \( q_3 \). On state \( q_3 \) it pops off an \( a \) from the top of the stack for every \( b \) in the input. When it sees the last \( b \) on state \( q_3 \) (i.e. when the input is exhausted), then the last \( a \) from the stack will be popped off and the start symbol \( z \) is exposed. This is the only possible case when the input (i.e. on -input ) the PDA \( M \) will move to state \( q_4 \) which is an accept state.

We will now show the computation of the PDA on a given input using the IDs and next move relations. For example, following are the computation on two input strings.

Let the input be \( aabb \). We start with the start configuration and proceed to the subsequent IDs using the transition function defined

\[ \delta(q_1, [a], z) = (q_2, [a], x) \]
\[ \delta(q_2, [a], x) = (q_2, [], x) \]
\[ \delta(q_2, [b], x) = (q_3, [b], x) \]

( using transition 1 )

\[ \delta(q_3, [b], x) = (q_4, [b], x) \]

( using transition 3 )

\[ \delta(q_4, [b], x) = (q_5, [b], x) \]

( using transition 5 )
(using transition 4), (using transition 5), is final state. Hence, accept. So the string $aabb$ is rightly accepted by $M$.

We can show the computation of the PDA on a given input using the IDs and next move relations. For example, following are the computation on two input strings.

i) Let the input be $aabab$.

No further move is defined at this point. Hence the PDA gets stuck and the string $aabab$ is not accepted.

**Example 2:** We give an example of a PDA $M$ that accepts the set of balanced strings of parentheses $[]$ by empty stack. The PDA $M$ is given below.

where $z$ is defined as

Informally, whenever it sees a $[$, it will push the $]$ onto the stack. (first two transitions), and whenever it sees a $]$ and the top of the stack symbol is $[$, it will pop the symbol $[$ off the stack. (The third transition). The fourth transition is used when the input is exhausted in order to pop $z$ off the stack (to empty the stack) and accept. Note that there is only one state and no final state. The following is a sequence of configurations leading to the acceptance of the string $[ [ ] ] ] ] ]$.

Equivalence of acceptance by final state and empty stack.

It turns out that the two definitions of acceptance of a language by a PDA - acceptance by final state and empty stack - are equivalent in the sense that if a language can be accepted by empty stack by some PDA, it can also be accepted by final state by some other PDA and vice versa. Hence it doesn't matter which one we use, since
each kind of machine can simulate the other. Given any arbitrary PDA $M$ that accepts the language $L$ by final state or empty stack, we can always construct an equivalent PDA $M'$ with a single final state that accepts exactly the same language $L$. The construction process of $M'$ from $M$ and the proof of equivalence of $M \& M'$ are given below.

There are two cases to be considered.

**CASE I:** PDA $M$ accepts by final state, Let $q_f$ be a new state not in $Q$.

Consider the PDA $M = \left( Q, \Sigma, \Gamma, \delta, q_0, F \right)$ as the following transition.

$L(M) = L(\delta'((q, \epsilon, X)))$ for some $X \in \Gamma^*$

Let $L(M')$. Then $M'$ accepts a string $w$ if and only if $M$ accepts $w$.

Thus, $\delta'(q_0, \epsilon, X) \vdash^* M' (q_f, \epsilon, \gamma)$ and

Conversely, let $M'$ accepts $w$ if and only if $M$ accepts $w$. Informsally, $M'$ enters one of its final states if and only if $M$ enters its final states in $F$.

**CASE II:** PDA $M$ accepts by empty stack.

We will construct $M'$ from $M$ in such a way that $M'$ simulates $M$ and detects when $M$ empties its stack.

Thus, $M'$ accepts a string $w$ if and only if $M$ accepts $w$. Let $M'$ have the same initial state as $M$ and contains all the transition of $M$, as well as the following two transitions.

1. $\delta'(q_0, \epsilon, X) = \{(q_0, X)\}$
2. $\delta'(q, \epsilon, X) = \{(q_f, \epsilon)\}$, $\forall q \in Q$
Transitions 1 causes to enter the initial configuration of $M$ except that marker $X$ which is below the symbols of $M$'s stack. From this point onward will have its own bottom-of-stack will simulate every move of $M$ since all the transitions of $M$ are also in

There is a tree representation for derivations that has proved extremely useful. This tree shows us clearly how the symbols of a terminal string are grouped into substrings, each of which belongs to the language of one of the variables of the grammar. But perhaps more importantly, the tree, known as a “parse tree”

Let $M$ accepts . Then

Let us fix on a grammar $G = (V, T, P, S)$. The parse trees for $G$ are trees with the following conditions:

1. Each interior node is labeled by a variable in $V$.
2. Each leaf is labeled by either a variable, a terminal, or $\epsilon$. However, if the leaf is labeled $\epsilon$, then it must be the only child of its parent.
3. If an interior node is labeled $A$, and its children are labeled $X_1, X_2, \ldots, X_k$.

Hence, also accepts . Conversely, let $X_1; X_2; \ldots; X_k$.

Then, respectively, from the left, then $A \rightarrow X_1X_2\cdotsX_k$ is a production in $P$. Note that the only time one of the $X$’s can be $\epsilon$ is if that is the label of the only child, and $A \rightarrow \epsilon$ is a production of $G$.

Hence, also accepts . Conversely, let $X_1; X_2; \ldots; X_k$.

Example 5.10: Figure 5.8 shows a parse tree for the palindrome grammar of Fig. 5.1. The production used at the root is $P \rightarrow 0P0$, and at the middle child of the root it is $P \rightarrow 1P1$. Note that at the bottom is a use of the production $P \rightarrow \epsilon$. That use, where the node labeled by the head has one child, labeled $\epsilon$, is the only time that a node labeled $\epsilon$ can appear in a parse tree.

Equivalence of PDAs and CFG’s:
We will now prove that pushdown automata and context-free grammars are equivalent in expressive power, that is, the language accepted by PDAs are exactly the context-free languages. To show this, we have to prove each of the following:

i) Given any arbitrary CFG $G$ there exists some PDA $M$ that accepts exactly the same language generated by $G$.

ii) Given any arbitrary PDA $M$ there exists a CFG $G$ that generates exactly the same language accepted by $M$.

(i) CFA to PDA
We will first prove that the first part i.e. we want to show to convert a given CFG to an equivalent PDA.
Let the given CFG is. Without loss of generality we can assume that $G$ is in Greibach Normal Form i.e. all productions of $G$ are of the form.

$$A \xrightarrow{0} xy \quad A = xy \quad \text{where} \quad x = \epsilon \quad y = \lambda$$

From the given CFG $G$ we now construct an equivalent PDA $M$ that accepts by empty stack. Note that there is only

$$M = \left( \begin{array}{l}
(q, \epsilon, \lambda) \rightarrow^0 (q, \epsilon, \epsilon) \\
(q, \epsilon, A) \rightarrow^0 (q, \epsilon, \epsilon)
\end{array} \right)$$

where

$q$ is the only state

$\Sigma$ is the input alphabet,

$N$ is the stack alphabet,

$q_0$ is the start state,

$S$ is the start/initial stack symbol, and

the transition relation is defined as follows

For each production $A \rightarrow \alpha \beta$. We now want to show that $M$ and $G$ are equivalent i.e. $L(G) = L(M)$. i.e. for any

$$A \rightarrow \alpha \beta \xrightarrow{0} \alpha \beta$$

If $\alpha = \epsilon$ then by definition of $L(G)$, there must be a leftmost derivation starting with $S$ and deriving $w$.

$$\alpha = \epsilon \quad \gamma = \beta$$

i.e.

$$\left( q, \epsilon, A \right) \rightarrow_\delta^0 (q, \epsilon, \epsilon)$$

But we will prove a more general result as given in the following lemma. Replacing $A$ by $S$ (the start symbol)

and $\epsilon$ by a terminal symbol. Therefore we need to show that for any

$$\left( q, \beta \right) \in \delta(q, \epsilon, B)$$

iff

$$\left( q, \beta \right) \in \delta(q, \epsilon, B)$$

Lemma: For any

$$\left( q, \alpha \epsilon, A \right) \rightarrow_\delta^n \left( q, \alpha \epsilon, B \alpha \right) \rightarrow_\delta^1 \left( q, \beta, \beta \alpha \right)$$

via a leftmost derivative iff

$$\alpha = \epsilon \quad \gamma = \beta \alpha$$

Proof: The proof is by induction on $n$.

Basis: $n = 0$

$$A \xrightarrow{0} \epsilon \quad \left( q, \epsilon, A \right) \rightarrow_\delta^0 (q, \epsilon, \epsilon)$$

$$\left( q, \epsilon, A \right) \rightarrow_\delta^0 (q, \epsilon, \epsilon)$$
iff i.e. and

\[ i(\ell(q,c,B)) = (q, \beta) \]
\[ \alpha \in \Gamma^* \]

iff

\[ (q, \alpha \gamma, A) \xrightarrow{\gamma} (q, \alpha \gamma, B \gamma) \xrightarrow{\gamma} \]
\[ (q, \gamma, \beta \alpha) \quad \gamma = \alpha \gamma \quad \gamma = \beta \alpha \]

**Induction Step:**

First assume that via a leftmost derivation. Let the last production applied in their derivation is

\[ A \xrightarrow{\delta} \omega B \alpha \]

for some and

Then, for some

\[ B \xrightarrow{\beta} \gamma \beta \alpha \]

\[ (q, \beta) \in \delta(q, c, B) \]

\[ \omega B \alpha \]

where and

\[ \frac{\gamma}{\gamma} \]

Now by the induction hypothesis, we get,

\[ \text{..........................(1)} \]

Again by the construction of \( M \), we get

\[ \]

\[ \]

\[ \]

so, from (1), we get

\[ \]

since \( \) and \( \), we get

\[ \]

\[ \]

That is, \( \) , then

\[ \]

Conversely, assume that

\[ \]

and let

\[ M = (\{q\}, \{a, b\}, \{S, A, B\}, \delta, q, S, \Sigma) \]
be the transition used in the last move. Then for some \\
and \\
and \\
where \\

Now, by the induction hypothesis, we get \\
via a leftmost derivation.

Again, by the construction of \( M \), \\
must be a production of \( G \). [ Since \\
Applying the production to the sentential form \\
we get \\

\[
(1) \quad S \rightarrow aAB \\
(2) \quad A \rightarrow a \\
(3) \quad A \rightarrow aA \\
(4) \quad B \rightarrow a \\
(5) \quad B \rightarrow bB
\]

i.e.

\[
(1) \quad (2) \quad (5) \quad (4)
\]

via a leftmost derivation:

\[
\Rightarrow \quad \Rightarrow \quad \Rightarrow \quad \Rightarrow
\]

Hence the proof.

**Example**: Consider the CFG \( G \) in GNF

\[
S \rightarrow aAB \\
A \rightarrow a/aA \\
B \rightarrow a/bB
\]

The one state PDA \( M \) equivalent to \( G \) is shown below. For convenience, a production of \( G \) and the corresponding transition in \( M \) are marked by the same encircled number.

\[
\begin{align*}
(1) & \quad S \rightarrow aAB \\
(2) & \quad A \rightarrow a \\
(3) & \quad A \rightarrow aA \\
(4) & \quad B \rightarrow a \\
(5) & \quad B \rightarrow bB
\end{align*}
\]

\[
(q, x, S) \rightarrow^* (q, \epsilon, \alpha) \quad S \Rightarrow^* x\alpha
\]

\[
(q, x, S) \rightarrow^* (q, \epsilon, \epsilon) \quad S \Rightarrow\alpha \quad x \in M(M) \quad x \in L(G)
\]

We have used the same construction discussed earlier

**Some Useful Explanations**:

Consider the moves of \( M \) on input \( \text{aaaba} \) leading to acceptance of the string.

**Steps**
1. \((q, aaaba, s) \rightarrow (q, aaba, AB)\)

2. \((q, aba, AB) \in \delta(q, c, A)\)
   \(A \rightarrow cB_1B_2\ldots B_k\)

3. \((q, ba, B) \in \mathcal{P}(\Sigma, \delta, \mathcal{P}, S)\)
   \(S = \varepsilon_0\)

4. \((q, a, B) \rightarrow (q, s, \varepsilon)\)

5. \((q, , ) \rightarrow (q, \varepsilon, \varepsilon)\) Accept by empty stack.

Note: encircled numbers here shows the transitions rule applied at every step.

Now consider the derivation of the same string under grammar \(G\). Once again, the production used at every step is shown with encircled number.

\(S \rightarrow aAB \rightarrow aaAB \rightarrow aaaB \rightarrow aaabB \rightarrow aaaba\)

Steps
\(N \rightarrow \{\varepsilon_0, A\}, S \rightarrow \varepsilon_0\)

Observations:
- There is an one-to-one correspondence of the sequence of moves of the PDA \(M\) and the derivation sequence under the CFG \(G\) for the same input string in the sense that - number of steps in both the cases are same and transition rule corresponding to the same production is used at every step (as shown by encircled number).
- Considering the moves of the PDA and derivation under \(G\) together, it is also observed that at every step the input read so far and the stack content together is exactly identical to the corresponding sentential form i.e.
  \(<\text{what is Read}> <\text{stack}> = <\text{sentential form}>\)

  Say, at step 2, Read so far = \(a\)
  stack = \(AB\)
  Sentential form = \(aAB\)

From this property we claim that \(\text{iff} \quad \text{or} \quad \text{iff} (\text{by definition})\)

Thus \(N(M) = L(G)\) as desired. Note that we have already proved a more general version of the claim

PDA and CFG:

We now want to prove: For every PDA \(M\) that accepts \(L(M)\) by empty stack, there is a CFG \(G\) such that \(L(G) = N(M)\)

we first see whether the "reverse of the construction" that was used in part (i) can be used here to construct an equivalent CFG from any PDA \(M\).

\(M' \quad N(M) = N(M')\)

It can be show that this reverse construction works only for single state PDAs.
That is, for every one-state PDA $M$ there is CFG $G$ such that $L(G) = N(M)$. For every move of the PDA $M$ we introduce a production in the grammar $G$ where $N = T$ and we can now apply the proof in part (i) in the reverse direction to show that $L(G) = N(M)$.

But the reverse construction does not work for PDAs with more than one state. For example, consider the PDA $M$ produced here to accept the language

Now let us construct CFG using the "reverse" construction.

( Note ).

Transition in $M$ Corresponding Production in $G$

$S \rightarrow \langle q_0 z_0 q \rangle \quad \forall q \in Q$

\[
\langle q_1, B_1 B_2 \cdots B_n \rangle \in \delta(q, a, A)
\]

\[
S \rightarrow \langle q_0 z_0 q \rangle \quad \forall q \in Q
\]

\[
(p, q) \in \Sigma \quad A \in \Gamma
\]

We can drive strings like these which are in the language.

The above grammar produces some strings which are not in the language. e.g

\[
\langle q_A q_1 \rangle \rightarrow a
\]

and

\[
\langle q_A q_{n+1} \rangle \Rightarrow \emptyset
\]

Therefore, to complete the proof of part (ii) we need to prove the following claim also.

Claim: For every PDA $M$ there is some one-state PDA $N$ such that

It is quite possible to prove the above claim. But we will adopt a different approach. We start with any arbitrary PDA $M$ that accepts by empty stack and directly construct an equivalent CFG $G$. 

\[
p = q_0, A = z_0 \quad \langle q_0, \ v, q \rangle \Rightarrow \emptyset \quad \langle q_0, \ v, z_0 \rangle \rightarrow (q, \ v, \ e)
\]

\[
q \in Q \quad q \in Q \quad S \rightarrow \langle q_0 z_0 q \rangle
\]
We want to construct a CFG \( G \) to simulate any arbitrary PDA \( M \) with one or more states. Without loss of generality we can assume that the PDA \( M \) accepts by empty stack.

The idea is to use nonterminal of the form \(<PAq>\) whenever PDA \( M \) in state \( P \) with \( A \) on top of the stack goes.

That is, for example, for a given transition of the PDA corresponding production in the grammar asto state shown below,

\[
S \rightarrow \langle q_0z_0q \rangle \quad \langle q_3, a, z_q \rangle \rightarrow (q, \varepsilon, \varepsilon) \quad \rightarrow \quad \delta(q, a, z_q) \rightarrow w
\]

And, we would like to show, in general, that \( \text{iff} \) the PDA \( M \), when started from state \( P \) with \( A \) on the top of the stack will finish processing, arrive at state \( q \) and remove \( A \) from the stack.

we are now ready to give the construction of an equivalent CFG \( G \) from a given PDA \( M \), we need to introduce two kinds of productions in the grammar as given below. The reason for introduction of the first kind of production will be justified at a later point. Introduction of the second type of production has been justified in the above discussion.

\[
S \rightarrow \langle q_0z_0q \rangle
\]

Let \( M \) be a PDA. We construct from \( M \) a equivalent CFG \( G \).

Where

\[
N \text{ is the set of nonterminals of the form } <PAq> \text{ for and and } P \text{ contains the following two kind of production}
\]

1. \[
\langle P, w, A \rangle \rightarrow (q, \varepsilon, \varepsilon) \quad \Rightarrow \quad \langle PAq \rangle \rightarrow w
\]

Include the following production

\[
\langle P, w, A \rangle (q, \varepsilon, \varepsilon) \quad w \in \Sigma^* \quad A \in \Gamma \quad p, q \in \mathcal{Q}
\]

If \( n = 0 \), then the production is.

For the whole exercise to be meaningful we want means there is a sequence of transitions (for PDA \( M \)), starting in state \( q \), ending in during which the PDA \( M \) consumes the input \( w \) and removes \( A \) from the stack (and, of course, all other symbols pushed onto stack in \( A \)'s place, and so on.)

That is we want to claim \( \langle P, w, A \rangle \rightarrow (q, \varepsilon, \varepsilon) \)

\[
a \in \Sigma \cup \{\varepsilon\} \quad \Rightarrow \quad \bar{x} \in \mathcal{L}^*
\]

\[
(q_1, B_1, B_2, \ldots, B_n) \in \mathcal{L}(p, a, A)(p, w, A)
\]

If this claim is true, then let to get \( B_1B_2\ldots B_n \) for some

But for all we have as production in \( G \). Therefore,

\[
q_{x1} \ldots q_{xn} = \bar{p}
\]

Getmynotes.com
Now, to show that the above construction of CFG $G$ from any PDA $M$ works, we need to prove the proposed claim.

$$\iff \text{PDA } M \text{ accepts } w \text{ by empty stack or } L(G) = N(M)$$

Note: At this point, the justification for introduction of the first type of production (of the form $B_i$) in the CFG $G$ (and hence, the PDA $M$) is clear. This helps us in deriving a string from the start symbol of the grammar.

**Proof:** Of the claim. For some and

The proof is by induction on the number of steps in a derivation of $G$ (which of course is equal to the number of moves taken by $M$). Let the number of steps taken is $n$. The proof consists of two parts: 'if' part and 'only if' part. First, consider the 'if' part

If

Then

**Basis is $n = 1$**

$$\langle q_1, x, B \rangle \rightarrow^{*} \langle q_{i+1}, \epsilon \rangle$$

1 ≤ $i$ ≤ $n + 1$

Then

In this case, it is clear that

Hence, by construction $x$ is a production of $G$.

Then

**Inductive Hypothesis:**

$$\langle p, w, A \rangle \rightarrow^{*} \langle q_1, x, B \rangle \rightarrow^{*} \langle q_{i+1}, \epsilon \rangle$$

1 ≤ $i$ ≤ $n + 1$

**Inductive Step:**

For $n > 1$, let $w = ax$ for some general transition

$$\rightarrow^{*} \langle q_3, \epsilon, z \rangle \rightarrow^{*} \langle q_4, \epsilon, z \rangle$$

. Now $M$ must remove $x$ from stack while consuming $x$ in the remaining $n-1$ moves.

Let , where is the prefix of $x$ that $M$ has consumed when first appears at top of the stack. Then there must exist a sequence of states in $M$ (as per construction) (with ), such that

$$\rightarrow \langle q_2, aab, az \rangle$$

$$\rightarrow \langle q_3, bab, aaz \rangle$$
\[ \delta'(q, \varepsilon, z_0) \vdash^* (q_f, \varepsilon) \]

We can show the computation of the PDA on a given input using the IDs and next move relations. For example, following are the computation on two input strings.

i) Let the input be \text{aabb}. we start with the start configuration and proceed to the subsequent IDs using the transition function defined

\begin{align*}
( \text{using transition 1} ), & \quad ( \text{using transition 2} ) \\
( \text{using transition 3} ), & \quad ( \text{using transition 4} ) \\
( \text{using transition 5} ), & \quad ( \text{using transition 6} )
\end{align*}

we can show the computation of the PDA on a given input using the IDs and next move relations. For example, following are the computation on two input strings.

ii) Let the input be \text{aabab}. we start with the start configuration and proceed to the subsequent IDs using the transition function defined

\begin{align*}
( \text{using transition 1} ), & \quad ( \text{using transition 2} ) \\
( \text{using transition 3} ), & \quad ( \text{using transition 4} ) \\
( \text{using transition 5} ), & \quad ( \text{using transition 6} )
\end{align*}

No further move is defined at this point.
Hence the PDA gets stuck and the string \textit{aabab} is not accepted.

The following is a sequence of configurations leading to the acceptance of the string \([ []] [ ]\).

\[
\begin{align*}
M' & \quad \alpha \quad \alpha \in L(M') \quad (q_0, \alpha, z_0) \xrightarrow{}^{*} M' (q_f, \varepsilon, \gamma) \xrightarrow{1} M' (q_f, \varepsilon, \gamma) \\
q & \in F \\
q & \in F \\
\alpha & \quad M' \\
\alpha & \quad M'
\end{align*}
\]

Equivalence of acceptance by final state and empty stack.

It turns out that the two definitions of acceptance of a language by a PDA - acceptance by final state and empty stack - are equivalent in the sense that if a language can be accepted by empty stack by some PDA, it can also be accepted by final state by some other PDA and vice versa. Hence it doesn't matter which one we use, since each kind of machine can simulate the other. Given any arbitrary PDA \(M\) that accepts the language \(L\) by final state or empty stack, we can always construct an equivalent PDA \(M'\) with a single final state that accepts exactly the same language \(L\). The construction process of \(M'\) from \(M\) and the proof of equivalence of \(M\) and \(M'\) are given below.

There are two cases to be considered.

\textbf{CASE 1: PDA \(M\) accepts by final state. Let } \( q_f \) \text{ be a new state not in } Q. \text{ Let } \delta' = \{ (q_f, \varepsilon, X) \} \text{, where the only new state } q_f \text{ contains } q_0, q_f \notin Q \text{ and } X \in \Gamma \text{, } \beta'.

Consider the PDA 

\[
\begin{align*}
\delta' & = \{ (q_f, \varepsilon, X) \} \\
\delta & \quad \delta' \\
\delta & \quad \delta'
\end{align*}
\]

\[
\begin{align*}
M' & = \{ q, \alpha, X \} \cup \{ q_0, \varepsilon, X \} \\
& \quad \cup \{ (q_f, \varepsilon) \} \quad \forall q \in Q \\
& \quad \cup \{ (q_f, \varepsilon) \} \quad \forall X \in \Gamma \\
& \quad \cup \{ (q_f, \varepsilon) \} \quad \forall \beta'.
\end{align*}
\]

Let \( q_0, q_f \notin Q \text{ and } X \in \Gamma \text{, } \beta'. \text{ Let } q \text{ be a new state not in } Q. \text{ Let } \delta' = \{ (q_f, \varepsilon, X) \} \text{, where as well as the following transition.}

Consider the PDA 

\[
\begin{align*}
\delta' & = \{ (q_f, \varepsilon, X) \} \\
\delta & \quad \delta' \\
\delta & \quad \delta'
\end{align*}
\]

\[
\begin{align*}
M' & = \{ q, \alpha, X \} \cup \{ q_0, \varepsilon, X \} \\
& \quad \cup \{ (q_f, \varepsilon) \} \quad \forall q \in Q \\
& \quad \cup \{ (q_f, \varepsilon) \} \quad \forall X \in \Gamma \\
& \quad \cup \{ (q_f, \varepsilon) \} \quad \forall \beta'.
\end{align*}
\]

Let \( q \in Q \text{ and } \beta' \text{ for some } q \text{ and } X \text{ and } \beta'. \text{ Then } \delta' \text{ for some } q \text{ and } X \text{ and } \beta'.

Thus \( M' \text{ accepts } \omega \).

\[
\begin{align*}
(q_0, \alpha, z_0) & \xrightarrow{} (q, \varepsilon, \varepsilon) \\
(q_0, \alpha, X) & \xrightarrow{1} M' (q_0, \alpha, z_0 X) \\
\xrightarrow{*} M' (q, \varepsilon, X)
\end{align*}
\]

Conversely, let \( M' \) accepts i.e. for some inherit all other moves except the last one from \( M \). Hence for some
Thus $M$ accepts $w$. Informally, on any input $w$, simulate all the moves of $M$ and enters in its own final state whenever $M$ enters in any one of its final status in $F$. Thus accepts a string $w$ iff $M$ accepts it.

CASE 2 : PDA $M$ accepts by empty stack.

we will construct $M'$ from $M$ in such a way that $M'$ simulates $M$ and detects when $M$ empties its stack.

Let $M'$ be defined as follows:

where and and contains all the transition of $M$ as well as the following two transitions.

and

Transitions 1 cause $M'$ to enter the initial configuration of $M$ except that it will have its own bottom-of-stack marker $X$ which is below the symbols of $M$'s stack. From this point onward, $M'$ will simulate every move of $M$ since all the transitions of $M$ are also in $M'$.

If $M$ ever empties its stack, then when simulating $M$ will empty its stack except the symbol $X$ at the bottom. At this point, $M$ will enter its final state by using transition rule 2, thereby (correctly) accepting the input.

Therefore, we will prove that $M$ and $M'$ are equivalent.

Let $M$ accept $w$. Then for some $q_f$ and $z_0$, $w$ is in $F$, and we will prove $M'$ and are equivalent.

Let $M'$ accept $w$. Then for some . But then,

(by transition rule 1)

(since include all the moves of $M$)

Hence, also accepts . Conversely, let accepts .

Getmynotes.com

CS6503 THEORY OF COMPUTATION

(by transition rule 2)
Thm 6.17: If \( L \) is a regular language, then \( L = \mathcal{L}(P) \) for some DPDA \( P \).

Every move in the sequence were taken from \( M \).

Hence, \( M \) starting with its initial configuration will eventually empty its stack and accept the input i.e.

PROOF: Essentially, a DPDA can simulate a deterministic finite automation. The PDA keeps some stack symbol \( Z_0 \) on its stack, because a PDA has to have a stack, but really the PDA ignores its stack and just uses its state. Formally, let \( A = (Q, \Sigma, \delta_A, q_0, F) \) be a DFA. Construct DPDA

\[
P = (Q, \Sigma, \{Z_0\}, \delta_P, q_0, Z_0, F)
\]

by defining \( \delta_P(q, \alpha, Z_0) = \{(p, Z_0)\} \) for all states \( p \) and \( q \) in \( Q \), such that \( \delta_A(q, \alpha) = p \).

We claim that \( (q_0, w, Z_0) \overset{*}{\underset{P}{ightarrow}} (p, \varepsilon, Z_0) \) if and only if \( \hat{\delta_A}(q_0, w) = p \). That is, \( P \) simulates \( A \) using its state. The proofs in both directions are easy inductions on \(|w|\), and we leave them for the reader to complete. Since both \( A \) and \( P \) accept by entering one of the states of \( F \), we conclude that their languages are the same. \( \square \)

Regular Languages and DPDA’s The DPDA’s accepts a class of languages that is in between the regular languages and CFL’s.
Deterministic Pushdown Automata (DPDA) and Deterministic Context-free Languages (DCFLs)

Pushdown automata that we have already defined and discussed are nondeterministic by default, that is, there may be two or more moves involving the same combination of state, input symbol, and top of the stack, and again, for some state and top of the stack the machine may either read and input symbol or make an ε-transition (without consuming any input).

In deterministic PDA, there is never a choice of move in any situation. This is handled by preventing the above mentioned two cases as described in the definition below.

Definition: Let \( M \) be a PDA. Then \( M \) is deterministic if and only if both the following conditions are satisfied.

1. has at most one element for any combination of any of the form \( (q_0, \alpha, X) \to^* (q, \beta, \gamma) \) and \( q \in Q \) (this condition prevents multiple choice for any combination of any of the form \( (q_0, \alpha, X) \to^* (q, \beta, \gamma) \) and \( q \in Q \))
2. If \( (q_0, \alpha, z_0) \to^* (q, \epsilon, \epsilon) \) and \( z_0 \) for every \( q \in Q \) (this condition prevents the possibility of a choice between a move with or without an input symbol).

\( (q_0, \alpha, z_0) \to^* (q, \epsilon, \epsilon) \)
A variable $A$ is left-recursive if it occurs in a production of the form

$$A \rightarrow Ax$$

for any $x \in (V \cup T)^*$.

A grammar is left-recursive if it contains at least one left-recursive variable.

Every content-free language can be represented by a grammar that is not left-recursive.

$$A \rightarrow y_1 y_2 \ldots y_n, \quad m \geq 2.$$

If $y_1$ is a terminal, say ‘$a$’, then introduce a new variable $B_a$ and a production

$$B_a \rightarrow a$$

Repeat this for every terminal on RHS.

Let $P'$ be the set of productions in $P$ together with the new productions.
NORMAL FORMS

Two kinds of normal forms viz., Chomsky Normal Form and Greibach Normal Form (GNF) are considered here.

Chomsky Normal Form (CNF)
Any context-free language \( L \) without any useless terminals is generated by a grammar whose productions are of the form \( A \rightarrow BC \) or \( A \rightarrow a \), where \( A, B \in V_N \) and \( a \in \Sigma \).

Procedure to find Equivalent Grammar in CNF:
(i) Eliminate the unit productions, and useless terminals if any,
(ii) Eliminate the terminals on the right hand side of length two or more.
(iii) Restrict the number of variables on the right hand side of productions to two.

Proof:
For Step (i): Apply the following theorem: Every context-free language can be generated by a grammar with no useless symbols and no unit productions.
At the end of this step the RHS of any production has a single terminal or two or more symbols.
Let us assume the equivalent resulting grammar as \( G = (V_N, V_T, P, S) \).
For Step (ii): Consider a production of the form \( A \rightarrow B_1 B_2 \ldots B_m \) where \( B_i \)'s are variables and \( m \geq 3 \).
If \( m = 2 \), then \( A \rightarrow B_1 B_2 \) is in proper form.
The production \( A \rightarrow B_1 B_2 \ldots B_m \) is replaced by new productions
\( A \rightarrow B_1 B_2 \ldots B_{m-2} \) and \( B_{m-2} \rightarrow B_{m-1} B_m \).

For step (iii): Consider \( A \rightarrow B_1 B_2 \ldots \ldots B_m \)
where \( B_i \)'s are variables and \( m \geq 3 \).

The resulting grammar \( G_1 = (V'_N, V_T, P', S) \) is equivalent to \( G \) and every production in \( P' \) has either a single terminal or two or more variables.

Proof:

For Step (ii): Consider any production of the form \( A \rightarrow B_1 B_2 \ldots B_m \) where \( B_i \)'s are variables.
\( S \rightarrow aAzB \)
\( A \rightarrow aA \mid a \)
\( B \rightarrow bB \mid b \).
Example
Obtain a grammar in Chomsky Normal Form (CNF) equivalent to the grammar $G$ with productions $P$ given

Solution
A recursive variable $A$ can be either

(i) "Directly Recursive", i.e., there is a production

$$A \rightarrow x_1 Ax_2$$

for some strings $x_1, x_2 \in (T \cup \Sigma)^*$, or

(ii) "Indirectly Recursive", i.e., there are variables $X_i$ and productions

$$A \rightarrow X_1 \ldots$$
$$X_1 \rightarrow \ldots X_2 \ldots$$
$$X_2 \rightarrow \ldots X_3 \ldots$$
$$X_N \rightarrow \ldots A \ldots$$
Pumping Lemma for CFG

A Pumping Lemma is a theorem used to show that, if certain strings belong to a language, then certain other strings must also belong to the language. Let us discuss a Pumping Lemma for CFL. We will show that, if \( L \) is a context-free language, then strings of \( L \) that are at least \( m \) symbols long can be "pumped" to produce additional strings in \( L \). The value of \( m \) depends on the particular language. Let \( L \) be an infinite context-free language. Then there is some positive integer \( m \) such that, if \( S \) is a string of \( L \) of length at least \( m \), then

(i) \( S = uvwxy \) (for some \( u, v, w, x, y \))
(ii) \(| vwx | \leq m \)
(iii) \(| vx | \geq 1 \)
(iv) \( uv^iwx^iy \in L \) for all non-negative values of \( i \).

It should be understood that

(i) If \( S \) is sufficiently long string, then there are two substrings, \( v \) and \( x \), somewhere in \( S \). There is stuff \( u \) before \( v \), stuff \( w \) between \( v \) and \( x \), and stuff \( y \), after \( x \).
(ii) The stuff between \( v \) and \( x \) won't be too long, because \(| vwx | \) can't be larger than \( m \).
(iii) Substrings \( v \) and \( x \) won't both be empty, though either one could be.
(iv) If we duplicate substring \( v \), some number \( i \) of times, and duplicate \( x \) the same number of times, the resultant string will also be in \( L \).

Definitions

A variable is useful if it occurs in the derivation of some string. This requires that
(a) the variable occurs in some sentential form (you can get to the variable if you start from \( S \)) and
(b) a string of terminals can be derived from the sentential form (the variable is not a "dead end"). A variable is recursive if it can generate a string containing itself. For example, variable \( A \) is recursive if

\[
S \Rightarrow uAy \Rightarrow uvAx
\]

Finally the derivation must have eliminated all variables to reach a string \( X \) in the language.

\[
S \Rightarrow uAy \Rightarrow uvAx \Rightarrow uvwxy = X
\]

This shows that derivation steps

\[
A \Rightarrow vAx
\]

and

\[
A \Rightarrow w
\]

are possible. Hence the derivation

\[
A \Rightarrow vwx
\]

Proof of Pumping Lemma

(a) Suppose we have a CFL given by \( L \). Then there is some context-free Grammar \( G \) that generates \( L \). Suppose

(i) \( L \) is infinite, hence there is no proper upper bound on the length of strings belonging to \( L \).
(ii) \( L \) does not contain \( I \).
(iii) \( G \) has no productions or \( l \)-productions.

Getmynotes.com
variable have finite lengths. The only way that a grammar can generate arbitrarily long strings is if one or more variables is both useful and recursive. Suppose no variable is recursive. Since the start symbol is non recursive, it must be defined only in terms of terminals and other variables. Then since those variables are non recursive, they have to be defined in terms of terminals and still other variables and so on. After a while we run out of —other variables‖ while the generated string is still finite. Therefore there is an upper bond on the length of the string which can be generated from the start symbol. This contradicts our statement that the language is finite. Hence, our assumption that no variable is recursive must be incorrect.

(b) Let us consider a string X belonging to L. If X is sufficiently long, then the derivation of X must have involved recursive use of some variable A. Since A was used in the derivation, the derivation should have started as

Getmynotes.com
Proof: Suppose $L$ is a context-free language.

If string $X \in L$, where $|X| > m$, it follows that $X = uvwx$, where $|vwx| \leq m$.

Choose a value $i$ that is greater than $m$. Then, wherever $vwx$ occurs in the string $a^i b^i c^i$, it cannot contain more than two distinct letters it can be all $a$'s, all $b$'s, all $c$'s, or it can be $a$'s and $b$'s, or it can be $b$'s and $c$'s.

Therefore the string $vwx$ cannot contain more than two distinct letters, but by the “Pumping Lemma” it cannot be empty, either, so it must contain at least one letter.

Now we are ready to “pump”.

Since $uvwx$ is in $L$, $uv^2wx^2y$ must also be in $L$. Since $v$ and $x$ can’t both be empty,

$$|uv^3wx^2y| > |uvwx|,$$

Usage of Pumping Lemma.

so we have added letters.

Both since $vwx$ does not contain all three distinct letters, we cannot have added the same number of each letter.

Therefore, $uv^2wx^2y$ cannot be in $L$.

Thus we have arrived at a “contradiction”.

Let $s = a^n b^n c^{2n}$, $n$ being obtained from Pumping Lemma.

Then $s = uvwx$, where $1 \leq |vwx| \leq n$.

Therefore, $vwx$ cannot have all the three symbols $a$, $b$, $c$.

If you assume that $vwx$ has only $a$’s and $b$’s then we can choose $i$ such that $uv^iwx^iy$ has more than $2n$ occurrence of $a$ or $b$ and exactly $2n$ occurrences of $c$.

Hence $uv^iwx^i y \notin L$, which is a contradiction. Hence $L$ is not a CFL.
Let $\Sigma$ be an alphabet, and suppose that for every symbol $a$ in $\Sigma$, we choose a language $L_a$. These chosen languages can be over any alphabets, not necessarily $\Sigma$ and not necessarily the same. This choice of languages defines a function $s$ (a substitution) on $\Sigma$, and we shall refer to $L_a$ as $s(a)$ for each symbol $a$.

If $w = a_1a_2 \cdots a_n$ is a string in $\Sigma^*$, then $s(w)$ is the language of all strings $x_1x_2 \cdots x_n$ such that string $x_i$ is in the language $s(a_i)$, for $i = 1, 2, \ldots, n$. Put another way, $s(w)$ is the concatenation of the languages $s(a_1)s(a_2) \cdots s(a_n)$. We can further extend the definition of $s$ to apply to languages: $s(L)$ is the union of $s(w)$ for all strings $w$ in $L$.

**Theorem 7.23:** If $L$ is a context-free language over alphabet $\Sigma$, and $s$ is a substitution on $\Sigma$ such that $s(a)$ is a CFL for each $a$ in $\Sigma$, then $s(L)$ is a CFL.

**Proof:** The essential idea is that we may take a CFG for $L$ and replace each terminal $a$ by the start symbol of a CFG for language $s(a)$. The result is a single CFG that generates $s(L)$. However, there are a few details that must be gotten right to make this idea work.

Example

Check whether the language given by $L = \{ a^m b^m c^n : m, n \in \mathbb{N} \}$ is a CFL or not.

Solution

More formally, start with grammars for each of the relevant languages, say $G = (V, \Sigma, P, S)$ for $L$ and $G_a = (V_a, T_a, P_a, S_a)$ for each $a$ in $\Sigma$. Since we can choose any names we wish for variables, let us make sure that the sets of variables are disjoint; that is, there is no symbol $A$ that is in two or more of $V$ and any of the $V_a$’s. The purpose of this choice of names is to make sure that when we combine the productions of the various grammars into one set of productions, we cannot get accidental mixing of the productions from two grammars and thus have derivations that do not resemble the derivations in any of the given grammars.

We construct a new grammar $G' = (V', T', P', S)$ for $s(L)$, as follows:

Closure properties of CFL – Substitution

---

Getmynotes.com
**Theorem 7.24**: The context-free languages are closed under the following operations:

1. Union.
2. Concatenation.
3. Closure (*), and positive closure (+).

Applications of substitution theorem


**Proof**: Each requires only that we set up the proper substitution. The proofs below each involve substitution of context-free languages into other context-free languages, and therefore produce CFL’s by Theorem 7.23.

1. **Union**: Let $L_1$ and $L_2$ be CFL’s. Then $L_1 \cup L_2$ is the language $s(L)$, where $L$ is the language $\{1, 2\}$, and $s$ is the substitution defined by $s(1) = L_1$ and $s(2) = L_2$.

2. **Concatenation**: Again let $L_1$ and $L_2$ be CFL’s. Then $L_1 L_2$ is the language $s(L)$, where $L$ is the language $\{12\}$, and $s$ is the same substitution as in case (1).

3. **Closure and positive closure**: If $L_1$ is a CFL, $L$ is the language $\{1\}^*$, and $s$ is the substitution $s(1) = L_1$, then $L_1^* = s(L)$. Similarly, if $L$ is instead the language $\{1\}^+$, then $L_1^+ = s(L)$.

4. Suppose $L$ is a CFL over alphabet $\Sigma$, and $h$ is a homomorphism on $\Sigma$. Let $s$ be the substitution that replaces each symbol $a$ in $\Sigma$ by the language consisting of the one string that is $h(a)$. That is, $s(a) = \{h(a)\}$, for all $a$ in $\Sigma$. Then $h(L) = s(L)$.

**Theorem 7.25**: If $L$ is a CFL, then so is $L^R$.

**Proof**: Let $L = L(G)$ for some CFL $G = (V, T, P, S)$. Construct $G^R = (V, T, P^R, S)$, where $P^R$ is the “reverse” of each production in $P$. That is, if $A \rightarrow \alpha$ is a production of $G$, then $A \rightarrow \alpha^R$ is a production of $G^R$. It is an easy induction on the lengths of derivations in $G$ and $G^R$ to show that $L(G^R) = L^R$. Essentially, all the sentential forms of $G^R$ are reverses of sentential forms of $G$, and vice-versa. We leave the formal proof as an exercise.  

CS6503 THEORY OF COMPUTATION
Reversal

Inverse Homomorphism:
3. Note that, as defined in (7.1), the start state of \( P' \) is \((q_0, \epsilon)\); i.e., \( P' \) starts in the start state of \( P \) with an empty buffer.

4. Likewise, the accepting states of \( P' \), as per (7.1), are those states \((q, \epsilon)\) such that \( q \) is an accepting state of \( P \).

The following statement characterizes the relationship between \( P' \) and \( P \):

- \((q_0, h(w), Z_0) \xrightarrow{P'} (p, \epsilon, \gamma)\) if and only if \(((q_0, \epsilon), w, Z_0) \xrightarrow{P} ((p, \epsilon), \epsilon, \gamma)\).

\[ M = (Q, \Sigma, \Gamma, \delta, q_0, B, F) \]
UNIT 4 TURING MACHINE

Informal Definition:
We consider here a basic model of TM which is deterministic and have one-tape. There are many variations, all are equally powerful.

The basic model of TM has a finite set of states, a semi-infinite tape that has a leftmost cell but is infinite to the right and a tape head that can move left and right over the tape, reading and writing symbols.

For any input w with \(|w| = n\), initially it is written on the n leftmost (contiguous) tape cells. The infinitely many cells to the right of the input all contain a blank symbol, B which is a special tape symbol that is not an input symbol. The machine starts in its start state with its head scanning the leftmost symbol of the input w. Depending upon the symbol scanned by the tape head and the current state the machine makes a move which consists of the following:

\[
\delta(q, x) = (p, y, d)\in
\]
writes a new symbol on that tape cell,
moves its head one cell either to the left or to the right and (possibly) enters a new state.

The action it takes in each step is determined by a transition functions. The machine continues computing (i.e. making moves) until it decides to "accept" its input by entering a special state called accept or final state or halts without accepting i.e. rejecting the input when there is no move defined.

On some inputs the TM many keep on computing forever without ever accepting or rejecting the input, in which case it is said to "loop" on that input.

Formal Definition:

Formally, a deterministic turing machine (DTM) is a 7-tuple, where

- \(Q\) is a finite nonempty set of states.
- \(\Gamma\) is a finite non-empty set of tape symbols, called the tape alphabet of \(M\).
- \(\Sigma\) is a finite non-empty set of input symbols, called the input alphabet of \(M\).
- \(\delta\) is the transition function of \(M\),
- \(q_0\) is the initial or start state.
- \(\beta\) is the set of final state.
- \(\epsilon\) is the blank symbol.

So, given the current state and tape symbol being read, the transition function describes the next state, symbol to be written on the tape, and the direction in which to move the tape head (L and R denote left and right, respectively).
Transition function:

The heart of the TM is the transition function, because it tells us how the machine gets one step to the next. when the machine is in a certain state \( q \in Q \) and the head is currently scanning the tape symbol.

1. replaces the symbol \( X \) by \( Y \) on the tape.
2. goes to state \( p \), and
3. the tape head moves one cell (i.e., one tape symbol) to the left (or right) if \( D = L \) (or \( R \)).

The ID (instantaneous description) of a TM captures what is going on at any moment i.e., it contains all the information to exactly capture the "current state of the computations".

It contains the following:

- The current state, \( q \)
- The position of the tape head,
- The constants of the tape up to the rightmost nonblank symbol or the symbol to the left of the head, whichever is rightmost.

\[ \delta(q, X) = (p, Y, L) \]

An ID (or configuration) of a TM \( M \) is denoted by

\[ \text{ID} = (q, X, \beta) \]

where

\[ q \text{ is the current state.} \]
\[ \beta \text{ is the tape contents to the left of the head.} \]
\[ X \text{ is the tape contents at or to the right of the head.} \]

That is, the tape head is currently scanning the leftmost symbol of the tape (note that if the tape head is scanning a blank symbol).

\[ \delta(q, X) = (p, Y, R) \]

If \( q \) is the start state and \( w \) is the input to a TM, the start or initial configuration of \( M \) is obviously denoted by

\[ M = (Q, \Sigma, \Gamma, \delta, q_0, \beta, F) \]

where

\[ w \in \Sigma^* \]

\[ \in \Gamma^* \]

\[ q_0, \beta \in \Gamma \]

CS6503 THEORY OF COMPUTATION

Moves of Turing Machines

To indicate one move we use the symbol \( \rightarrow \). Similarly, zero, one, or more moves will be represented by

\[ \text{let } M \text{ be an ID of } M \text{ where} \]

\[ ID_1, ID_2, \ldots, ID_k \]
Then we write meaning that ID yields.

Alternatively, if is a transition of \( M \), then we write

\[
\text{means that the ID \( y \) yields } \]

In other words, when two IDs are related by the relation, we say that the first one yields the second (or the second is the result of the first) by one move.

If ID \( j \) results from ID \( i \) by zero, one or more (finite) moves then we write (If the TM \( M \) is understand, then the subscript \( M \) can be dropped from

\[
\]}

which

**Special Boundary Cases**

Let be an ID and be an ID allowed to fall off the left end of the tape. be an transition of \( M \). Then . That is, the head is not

Let be an ID and then figure (Note that is equivalent to )

Let be an ID and then figure

Let be an ID and then figure

The language accepted by a TM , denoted as \( L(M) \) is

\[
L(M) = \{ \text{w} \mid \text{and figure for some } F \text{ and } \}
\]

In other words the TM \( M \) accepts a string that cause \( M \) to enter a final or accepting state when started in its initial ID (i.e. ). That is a TM \( M \) accepts the string if a sequence of IDs,

exists such that

is the initial or starting ID of \( M \)

;
The set of strings that $M$ accepts is the language of $M$, denoted $L(M)$, as defined above.

More about configuration and acceptance

An ID of $M$ is called an accepting (or final) ID if is undefined i.e. the TM has no move at this point.

An ID is called a blocking (or halting) ID if.

is called reactable from if

is the initial (or starting) ID if

is the input to the TM and

is the initial (or start) state of $M$.

On any input string, either

$M$ halts on $w$ if there exists a blocking (configuration) ID, such that

There are two cases to be considered

$M$ accepts $w$ if $I$ is an accepting ID. The set of all accepted by $M$ is denoted as $L(M)$ as already defined

$M$ rejects $w$ if $I$ is a blocking configuration. Denote by reject ($M$), the set of all rejected by $M$.

or

$M$ loops on $w$ if it does not halt on $w$.

Let $\text{loop}(M)$ be the set of all on which $M$ loops for.

It is quite clear that

That is, we assume that a TM $M$ halts

When it enters an accepting or

When it enters a blocking i.e. when there is no next move.

However, on some input string, $w$, it is possible that the TM $M$ loops for ever i.e. it never halts.
The input to a Turing machine is a string. Turing machines themselves can be written as strings. Since these strings can be used as input to other Turing machines. A Universal Turing machine is one whose input consists of a description \( M \) of some arbitrary Turing machine, and some input \( w \) to which machine \( M \) is to be applied, we write this combined input as \( M + w \). This produces the same output that would be produced by \( M \). This is written as Universal Turing Machine \( (M + w) = M(w) \).

As a Turing machine can be represented as a string, it is fully possible to supply a Turing machine as input to itself, for example \( M(M) \). This is not even a particularly bizarre thing to do for example, suppose you have written a C pretty printer in C, then used the Pretty printer on itself. Another common usage is Bootstrapping—where some convenient languages used to write a minimal compiler for some new language \( L \), then used this minimal compiler for \( L \) to write a new, improved compiler for language \( L \). Each time a new feature is added to language \( L \), you can recompile and use this new feature in the next version of the compiler. Turing machines sometimes halt, and sometimes they enter an infinite loop.

A Turing machine might halt for one input string, but go into an infinite loop when given some other string. The halting problem asks: “Is it possible to tell, in general, whether a given machine will halt for some given input?” If it is possible, then there is an effective procedure to look at a Turing machine and its input and determine whether the machine will halt with that input. If there is an effective procedure, then you can build a Turing machine to implement it. Suppose we have a Turing machine \( \text{WillHalt}(M, w) \) which, given an input string \( M + w \), will halt and accept the string if Turing machine \( M \) halts on input \( w \) and will halt and reject the string if Turing machine \( M \) does not halt on input \( w \). When viewed as a Boolean function, \( \text{WillHalt}(M, w) \) halts and returns \( \text{TRUE} \) in the first case, and (halts and) returns \( \text{FALSE} \) in the second.

**Theorem**

Turing Machine \( \text{WillHalt}(M, w) \) does not exist.

**Proof:** This theorem is proved by contradiction. Suppose we could build a machine \( \text{WillHalt} \). Then we can certainly build a second machine \( \text{LoopIfHalts} \), that will go into an infinite loop if and only if \( \text{WillHalt} \) accepts its input:

```
Function LoopIfHalts (M, w):
if WillHalt (M, w) then
while true do { }
else
return false;
```

We will also define a machine \( \text{LoopIfHaltsOnItSelf} \) that, for any given input \( M \), representing a Turing machine, will determine what will happen if \( M \) is applied to itself, and loops if \( M \) will halt in this case:

```
Function LoopIfHaltsOnItself (M):
return LoopIfHalts (M, M);
```

Finally, we ask what happens if we try:

```
Function Impossible:
return LoopIfHaltsOnItself (LoopIfHaltsOnItself):
```

This machine, when applied to itself, goes into an infinite loop if and only if it halts when applied to itself. This is impossible. Hence the theorem is proved.
Implications of Halting Problem

Programming

The Theorem of the Halting Problem does not say that we can never determine whether or not a given program halts on a given input. Most of the times, for practical reasons, we could eliminate all infinite loops from programs. Most of the time, we could use a meta-program to check another program for potential infinite loops, and get this meta-program to work most of the time. The theorem says that we cannot ever write such a meta-program and have it work all of the time. This result is also used to demonstrate that certain other programs are also impossible. The basic outline is as follows:

(i) If we could solve a problem X, we could solve the Halting problem
(ii) We cannot solve the Halting problem
(iii) Therefore, we cannot solve problem X

The first component of T's state becomes q1.

2. a) δ([q1, 0], 1) = ([q1, 0], 1, R)
   b) δ([q1, 1], 0) = ([q1, 1], 0, R)

   (If T has a 0 stored and sees a 1, or vice versa, then T continues to move to the right.)

3. a) δ([q1, 0], B) = ([q1, B], 0, L)
   b) δ([q1, 1], B) = ([q1, B], 0, L)

   (T enters the final state [q1, B] if T reaches a blank symbol without having first encountered a second copy of the leftmost symbol.)

Example

If T reaches a blank in state [q1, 0] or [q1, 1], it accepts. For state [q1, 0] and symbol 0 or for state [q1, 1] and symbol 1, δ is not defined, so if T ever sees the symbol stored, it halts without accepting.

In general, we can allow the finite control to have k components, all but one of which store information.
2. Multiple Tracks
We can imagine that the tape of the Turing machine is divided into k tracks, for any finite k. This arrangement is shown in Fig., with k = 3. What is actually done is that the symbols on the tape are considered as k-tuples. One component for each track.

Example
The tape in Fig. can be imagined to be that of a Turing machine which takes a binary input greater than 2, written on the first track, and determines if it is a prime. The input is surrounded by $ and $ on the first track.
Thus, the allowable input symbols are [¢, B, B], [0, B, B], [1, B, B], and [$, B, B]. These symbols can be identified with ¢, 0, 1, and $, respectively, when viewed as input symbols. The blank symbol can be represented by [B, B, B].
To test if its input is a prime, the Tm first writes the number two in binary on the second track and copies the first track onto the third track. Then, the second track is subtracted, as many times as possible, from the third track, effectively dividing the third track by the second and leaving the remainder. If the remainder is zero, the number on the first track is not a prime. If the remainder is nonzero, increase the number on the second track by one.
If now the second track equals the first, the number on the first track is a prime, because it cannot be divided by any number between one and itself. If the second is less than the first, the whole operation is repeated for the new number on the second track. In Fig., the Tm is testing to determine if 47 is a prime. The Tm is dividing by 5; already 5 has been subtracted twice, so 37 appears on the third track.

3. Subroutines

(i) There are no unit productions in the given set of \( P \).

(ii) Amongst the given productions, we have

\[
A \rightarrow a, \\
B \rightarrow b
\]

which are in proper form.

Assume that \( m \) and \( n \) are positive integers. Let us represent the input as \( 0^m B 0^n \).

If the separating \( B \) is removed and 0’s come together we have the required output, \( m + n \) is unity.

(i) The separating \( B \) is replaced by a 0.

(ii) The rightmost 0 is erased i.e., replaced by \( B \).

Let us define \( M = (\{q_0, q_1, q_2, q_3, q_4\}, \{0, 1, B, \delta\}, \delta, q_0, \{q_4\}) \). \( \delta \) is defined by Table shown below.

<table>
<thead>
<tr>
<th>Tape Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>( S \rightarrow B ) ( A R B ) (( q_0, 0, R )) (( q_1, 0, R )) (( q_2, B, L ))</td>
</tr>
</tbody>
</table>

Hence we assume new variables \( D_1 \) and \( D_2 \) and the productions

\[
q_3 \rightarrow D_1 \\
q_3 \rightarrow D_2
\]

\( M \) starts from \( q_0 \), \( 0^m B 0^n \), moves right until seeking the blank \( B \). \( M \) changes state to \( q_1 \). On reaching the right end, it reverts, replaces the rightmost \( 0 \) by \( B \). It moves left until it reaches the beginning of the input string. It halts at the final state \( q_4 \).

Design a Turing machine to add two given integers.

Solution:

\[
S \rightarrow B_a D_1, \\
D_1 \rightarrow A D_2, \\
D_2 \rightarrow B_b B, \\
A \rightarrow B_a A, \\
B \rightarrow B_b B, \\
B_0 \rightarrow a, \\
B_1 \rightarrow b, \\
A \rightarrow a, \\
B \rightarrow b.
\]

CS6503 THEORY OF COMPUTATION
Some unsolvable Problems are as follows:

(i) Does a given Turing machine $M$ halts on all input?
(ii) Does Turing machine $M$ halt for any input?
(iii) Is the language $L(M)$ finite?
(iv) Does $L(M)$ contain a string of length $k$, for some given $k$?
(v) Do two Turing machines $M_1$ and $M_2$ accept the same language?

It is very obvious that if there is no algorithm that decides, for an arbitrary given Turing machine $M$ and input string $w$, whether or not $M$ accepts $w$. These problems for which no algorithms exist are called —UNDECIDABLE‖ or —UNSOLVABLE‖.

Code for Turing Machine:

Getmynotes.com
The language $L_d$, the \textit{diagonalization language}, is the set of strings $w_i$ such that $w_i$ is not in $L(M_i)$.

That is, $L_d$ consists of all strings $w$ such that the TM $M$ whose code is $w$ does not accept when given $w$ as input.

The reason $L_d$ is called a “diagonalization” language can be seen if we consider Fig. 9.1. This table tells for all $i$ and $j$, whether the TM $M_i$ accepts input string $w_j$; 1 means “yes it does” and 0 means “no it doesn’t.” We may think of the $i$th row as the \textit{characteristic vector} for the language $L(M_i)$; that is, the 1’s in this row indicate the strings that are members of this language.

\begin{table}[h]
\centering
\begin{tabular}{c|cccc}
  & 1 & 2 & 3 & 4 \\
\hline
1 & 0 & 1 & 1 & 0 \\
2 & 1 & 1 & 0 & 0 \\
3 & 0 & 0 & 1 & 1 \\
4 & 0 & 1 & 0 & 1 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\

\end{tabular}
\caption{Diagonal}
\end{table}

The diagonal values tell whether $M_i$ accepts $w_i$. To construct $L_d$, we complement the diagonal. For instance, if Fig. 9.1 were the correct table, then the complemented diagonal would begin $1,0,0,0,\ldots$. Thus, $L_d$ would contain $w_1 = \epsilon$, not contain $w_2$ through $w_4$, which are 0, 1, and 00, and so on.

The trick of complementing the diagonal to construct the characteristic vector of a language that cannot be the language that appears in any row, is called \textit{diagonalization}. It works because the complement of the diagonal is ...
Theorem 9.2: \( L_d \) is not a recursively enumerable language. That is, there is no Turing machine that accepts \( L_d \).

Proof: Suppose \( L_d \) were \( L(M) \) for some TM \( M \). Since \( L_d \) is a language over alphabet \( \{0, 1\} \), \( M \) would be in the list of Turing machines we have constructed, since it includes all TMs with input alphabet \( \{0, 1\} \). Thus, there is at least one code for \( M \), say \( i \); that is, \( M = M_i \).

Now, ask if \( w_i \) is in \( L_d \).

- If \( w_i \) is in \( L_d \), then \( M_i \) accepts \( w_i \). But then, by definition of \( L_d \), \( w_i \) is not in \( L_d \), because \( L_d \) contains only those \( w_j \) such that \( M_j \) does not accept \( w_j \).
- Similarly, if \( w_i \) is not in \( L_d \), then \( M_i \) does not accept \( w_i \). Thus, by definition of \( L_d \), \( w_i \) is in \( L_d \).

Since \( w_i \) can neither be in \( L_d \) nor fail to be in \( L_d \), we conclude that there is a contradiction of our assumption that \( M \) exists. That is, \( L_d \) is not a recursively enumerable language. \( \square \)

We call a language \( L \) recursive if \( L = L(M) \) for some Turing machine \( M \) such that:

1. If \( w \) is in \( L \), then \( M \) accepts (and therefore halts).

2. If \( w \) is not in \( L \), then \( M \) eventually halts, although it never enters an accepting state.

A TM of this type corresponds to our informal notion of an “algorithm,” a well-defined sequence of steps that always finishes and produces an answer. If we think of the language \( L \) as a “problem,” as will be the case frequently, then problem \( L \) is called decidable if it is a recursive language, and it is called 104 undecidable if it is not a recursive language.
It should be noted here that the above does not imply that a was used recursively only once. The * of $\Rightarrow$ could cover many uses of $A$, as well as other recursive variables.

There has to be some “last” recursive step. Consider the longest strings that can be derived for $v, w$ and $x$ without the use of recursion. Then there is a number ‘$m$’ such that $|vwx| < m$.

Since the grammar does not contain any $\lambda$-productions or unit productions, every derivation step either introduces a terminal or increases the length of the sentential form. Since $A \Rightarrow^* vAx$, it follows that $|v| > 0$.

Finally, since $uvAxv$ occurs in the derivation, and $A \Rightarrow^* vAx$ and $A \Rightarrow^* w$ are both possible, it follows that $uv^iwx^iy$ also belongs to $L$.

This completes the proof of all parts of Lemma.

The Pumping Lemma can be used to show that certain languages are not context-free.

Let us show that the language

$$L = \{a^ib^ic^i \mid i > 0\}$$

is not context-free.
Theorem 9.4: If both a language $L$ and its complement are RE, then $L$ is recursive. Note that then by Theorem 9.3, $\overline{L}$ is recursive as well.

**Proof:** The proof is suggested by Fig. 9.4. Let $L = L(M_1)$ and $\overline{L} = L(M_2)$. Both $M_1$ and $M_2$ are simulated in parallel by a TM $M$. We can make $M$ a two-tape TM, and then convert it to a one-tape TM, to make the simulation easy and obvious. One tape of $M$ simulates the tape of $M_1$, while the other tape of $M$ simulates the tape of $M_2$. The states of $M_1$ and $M_2$ are each components of the state of $M$.

![Diagram](image)

Figure 9.4: Simulation of two TM's accepting a language and its complement

If input $w$ to $M$ is in $L$, then $M_1$ will eventually accept. If so, $M$ accepts and halts. If $w$ is not in $L$, then it is in $\overline{L}$, so $M_2$ will eventually accept. When $M_2$ accepts, $M$ halts without accepting. Thus, on all inputs, $M$ halts, and $L(M)$ is exactly $L$. Since $M$ always halts, and $L(M) = L$, we conclude that $L$ is recursive. □

We define $L_u$, the *universal language*, to be the set of binary strings that encode, in the notation of Section 9.1, a pair $(M, w)$, where $M$ is a TM with the binary input alphabet, and $w$ is a string in $(0 + 1)^*$, such that $w$ is in $L(M)$. That is, $L_u$ is the set of strings representing a TM and an input accepted by that TM. We shall show that there is a TM $U$, often called the *universal Turing machine*, such that $L_u = L(U)$. Since the input to $U$ is a binary string, $U$ is in fact some $M_i$ in the list of binary-input Turing machines we developed in
Universal Language:

Undecidability of Universal Language:
**Theorem 9.6:** $L_u$ is RE but not recursive.

**Proof:** We just proved in Section 9.2.3 that $L_u$ is RE. Suppose $L_u$ were recursive. Then by Theorem 9.3, $\overline{L_u}$, the complement of $L_u$, would also be recursive. However, if we have a TM $M$ to accept $\overline{L_u}$, then we can construct a TM $M'$ to accept $L_d$ (by a method explained below). Since we already know that $L_d$ is not RE, we have a contradiction of our assumption that $L_u$ is recursive.

Given $w$ as input, $M'$ changes the input to $w111w$. You may, as an exercise, write a TM program to do this step on a single tape. However, an easy argument that it can be done is to use a second tape to copy $w$, and then convert the two-tape TM to a one-tape TM.

1. $M'$ simulates $M$ on the new input. If $w$ is $w_i$ in our enumeration, then $M'$ determines whether $M_i$ accepts $w_i$. Since $M$ accepts $\overline{L_u}$, it will accept if and only if $M_i$ does not accept $w_i$; i.e., $w_i$ is in $L_d$.

Thus, $M'$ accepts $w$ if and only if $w$ is in $L_d$. Since we know $M'$ cannot exist by Theorem 9.2, we conclude that $L_u$ is not recursive. \(\square\)
Post's Correspondence Problem (PCP)

A post correspondence system consists of a finite set of ordered pairs 
\[ (x_i, y_i) \]
where 
\[ \alpha \]
for some alphabet \( \Sigma \).

Any sequence of numbers 
\[ \ell \]
is called a solution to a Post Correspondence System.

The Post Correspondence Problem is the problem of determining whether a Post Correspondence system has a solution.

Example 1: Consider the post correspondence system

\[ (a^1, a^2), (a^2, a^1), \ldots, (a^n, a^n) \]

\[ \exists k \text{ such that } i_k = j_k \text{ or } \exists k \text{ and } i \text{ such that } i_k > j_k \text{ and } i_i < j_i \]

\[ \sum \left| \sum \right| \geq 1 \]

(A post correspondence system is also denoted as an instance of the PCP)

Example 2: The following PCP instance has no solution

\[ \Gamma = \{(0, 1)\} \]

\[ a_i \in \Sigma, 1 \leq i \leq k \]

\[ \sum \]

This can be proved as follows. cannot be chosen at the start, since than the LHS and RHS would differ in the first symbol ( in LHS and in RHS). So, we must start with . The next pair must be so that the 3rd symbol in the RHS becomes identical to that of the LHS, which is a . After this step, LHS and RHS are not matching. If is selected next, then would be mismatched in the 7th symbol.
Example 3 : The list 1, 3, 2, 3 is a solution to the following PCP instance.

\[(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\]

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>101</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>00</td>
</tr>
<tr>
<td>3</td>
<td>011</td>
<td>11</td>
</tr>
</tbody>
</table>

\[G_x = (N_x, \Sigma, P_x, S_x)\]
\[G_y = (N_y, \Sigma, P_y, S_y)\]

The following properties can easily be proved.

Proposition : The Post Correspondence System has solutions if and only if

Corollary : PCP over one-letter alphabet is decidable.

Proposition : Any PCP instance over an alphabet with \(|\Sigma| = m\) is equivalent to a PCP instance over an alphabet with \(|\Sigma'| = 2\).

Proof : Let \(G_x\) and \(G_y\) be a PCP instance over the alphabet \(\Sigma\) and \(\Sigma'\), respectively.

Consider \(G_y\) as an alphabet with only two symbols, 0 and 1, and hence, is equivalent to a PCP instance over

Theorem : PCP is undecidable. That is, there is no algorithm that determines whether an arbitrary
Post Correspondence System has a solution.

Proof: The halting problem of turning machine can be reduced to PCP to show the undecidability of PCP. Since halting problem of TM is undecidable (already proved), this reduction shows that PCP is also undecidable. The proof is little bit lengthy and left as an exercise.

Some undecidable problem in context-free languages.

We can use the undecidability of PCP to show that many problems concerning the context-free languages are undecidable. To prove this we reduce the PCP to each of these problems. The following discussion makes it clear how PCP can be used to serve this purpose.

Let be a Post Correspondence System over the alphabet two CFG's \(G_x\) and \(G_y\) from the ordered pairs \(x, y\) respectively as follows.
generates the strings that can appear in the LHS of a sequence while solving it is clear that the grammar the PCP followed by a sequence of numbers. The sequence of number at the end records the sequence of strings from the PCP instance (in reverse order) that generates the string. Similarly, generates the strings that can be obtained from the RHS of a sequence and the corresponding sequence of numbers (in reverse order).

Now, if the Post Correspondence System has a solution, then there must be a sequence

According to the construction of and

In this case
Hence, \( L(G_1) \subseteq L(G_2) \) implying

\[
L(G_1) = \sum^* \quad L(G_1) = \phi
\]

Conversely, let

\[
L(G_1) = \phi
\]

Hence, \( w \) must be in the form \( wkw \) where \( w \) is in a sequence (since, only that kind of strings can be generated by \( G_1 \) and \( G_2 \)).

\[
L = L(G_x) \cup L(G_y)
\]

\[
L = L(G_x) \cap L(G_y)
\]

Now, the string is a solution to the Post Correspondence System.

It is interesting to note that we have here reduced PCP to the language of pairs of CFG's whose intersection is nonempty. The following result is a direct conclusion of the above.

Theorem: Given any two CFG's \( G_1 \) and \( G_2 \) the question "Is \( L(G_1) = \phi \)" is undecidable.

Proof: Assume for contradiction that there exists an algorithm \( A \) to decide this question. This would imply that PCP is decidable as shown below.

For any Post Correspondence System, \( P \) construct grammars \( G_x \) and \( G_y \) by using the constructions elaborated already. We can now use the algorithm \( A \) to decide whether

\[
L_1 = L(G_x) \cup L(G_y)
\]

Thus, PCP is decidable, a contradiction. So, such an algorithm does not exist.

If \( G_1 \) and \( G_2 \) are CFG's constructed from any arbitrary Post Correspondence System, than it is not difficult to and are also context-free, even though the class of context-free languages are not show that closed under complementation. \( w \in L(G_x) \cap L(G_y) \) and their complements can be used in various ways to show that many other questions related to CFL's are undecidable. We prove here some of those.

\[
L(G_2) = (\sum \cup \{1, 2, \ldots, n\})^*
\]

Theorem: For any two arbitrary CFG's the following questions are undecidable

i. Is \( L(G_1) = L(G_2) \)

ii. Is \( L(G_1) \subseteq L(G_2) \)
iii. Is

Proof:

i. If then,

Hence, it suffice to show that the question —Is " is undecidable.

Since, and are CFL's and CFL's are closed under union, is also context-free. By DeMorgan's theorem,

If there is an algorithm to decide whether we can use it to decide whether

or not. But this problem has already been proved to be undecidable.

Hence there is no such algorithm to decide or not.

ii.

Let P be any arbitrary Post correspondence system and and are CFg's constructed from the pairs of strings.

must be a CFL and let G1 generates L1. That is,

by De Morgan's theorem, as shown already, any string, represents a solution to the PCP. Hence, contains all but those strings representing the solution to the PCP.

Let for same CFG G:

It is now obvious that if and only if the PCP has no solutions, which is already proved to be undecidable. Hence, the question —Is " be ?" is undecidable.

iii.
Let \( G \) be a CFG generating the language \( L \) and \( G' \) be a CFG generating \( L' \) where \( G \) and \( G' \) are CFGs constructed from same arbitrary instance of PCP.

\[
\text{iff}\]

i.e. iff the PCP instance has no solutions as discussed in part (ii).

Hence the proof.

Theorem: It is undecidable whether an arbitrary CFG is ambiguous.

Proof: Consider an arbitrary instance of PCP and construct the CFG's \( G \) and \( G' \) from the ordered pairs of strings.

We construct a new grammar \( G \) from \( G \) and \( G' \) as follows.

\[
\text{where}
\]

is same as that of \( G \) and \( G' \).

This constructions gives a reduction of PCP to the -------- of whether a CFG is ambiguous, thus leading to the undecidability of the given problem. That is, we will now show that the PCP has a solution if and only if \( G \) is ambiguous. (where \( G \) is constructed from an arbitrary instance of PCP).

Only if Assume that \( S \) is a solution sequence to this instance of PCP.

Consider the following two derivation in .
A Turing machine $M$ is said to be of *time complexity* $T(n)$ [or to have “running time $T(n)$”] if whenever $M$ is given an input $w$ of length $n$, $M$ halts after making at most $T(n)$ moves, regardless of whether or not $M$ accepts. This definition applies to any function $T(n)$, such as $T(n) = 50n^2$ or $T(n) = 3^n + 5n^4$; we shall be interested predominantly in the case where $T(n)$ is a polynomial in $n$. We say a language $L$ is in class $\mathcal{P}$ if there is some polynomial $T(n)$ such that $L = L(M)$ for some deterministic TM $M$ of time complexity $T(n)$.

If it is important to note that any string of terminals cannot have more than one derivation in and

Because, every terminal string which are derivable under these grammars ends with a sequence of integers

This sequence uniquely determines which productions must be used at every step of the derivation.

Hence, if a terminal string, has two leftmost derivations, then one of them must begin with the step.

then continues with derivations under

In both derivations the resulting string must end with a sequence for same

The reverse of this sequence must be a solution to the PCP, because the string that precede in one case is and in the other case. Since the string derived in both cases are identical, the sequence

must be a solution to the PCP.

Hence the proof
Class p-problem solvable in polynomial time:

Non deterministic polynomial time:
A nondeterministic TM that never makes more than \( p(n) \) moves in any sequence of choices for some polynomial \( p \) is said to be non polynomial time NTM.

NP is the set of languages that are accepted by polynomial time
NTM’s Many problems are in NP but appear not to be in \( p \).
One of the great mathematical questions of our age: is there anything in NP that is not in \( p \)?

NP-complete problems:
If we cannot resolve the \( \neg P=NP \) question, we can at least demonstrate that certain problems in NP are the hardest, in the sense that if any one of them were in \( P \), then \( P=NP \).
These are called NP-complete.

Intellectual leverage: Each NP-complete problem’s apparent difficulty reinforces the belief that they are all hard.

Methods for proving NP-Complete problems:
Polynomial time reduction (PTR): Take time that is some polynomial in the input size to convert instances of one problem to instances of another.
If \( P_1 \) PTR to \( P_2 \) and \( P_2 \) is in \( P \), then \( P_1 \) is in \( P \).
Start by showing every problem in NP has a PTR to Satisfiability of Boolean formula.
Then, more problems can be proven NP complete by showing that SAT PTRs to them directly or indirectly.
\begin{align*}
\alpha \gamma \beta & \quad q \in F \\
\alpha \omega x \beta & \quad \delta(q, x) \\
1D_j & \quad ID_i \vdash_{M} 1D_j \\
q_0 \omega & \quad w \in \Sigma^* \\
q_0 \in Q & \quad q_0 \in Q \\
\omega & \in \Sigma^* \\
I' & \quad q_0 \omega \vdash_{M} I' \\
\omega & \in \Sigma^* \\
I' & \quad w \in \Sigma^* \\
\omega & \in \Sigma^* \\
L(M) \cup \text{reject}(M) \cup \text{loop}(M) &= \Sigma^* \\
1D_1 & \\
1D_1 & \\
\omega \notin L(M) &
\end{align*}
Our next goal is to devise a binary code for Turing machines so that each TM with input alphabet \( \{0, 1\} \) may be thought of as a binary string. Since we just saw how to enumerate the binary strings, we shall then have an identification of the Turing machines with the integers, and we can talk about "the \( i \)th Turing machine, \( M_i \)." To represent a TM \( M = (Q, \{0, 1\}, \Gamma, \delta, q_1, B, F) \) as a binary string, we must first assign integers to the states, tape symbols, and directions \( L \) and \( R \).

- We shall assume the states are \( q_1, q_2, \ldots, q_r \) for some \( r \). The start state will always be \( q_1 \), and \( q_2 \) will be the only accepting state. Note that, since we may assume the TM halts whenever it enters an accepting state, there is never any need for more than one accepting state.

- We shall assume the tape symbols are \( X_1, X_2, \ldots, X_s \) for some \( s \). \( X_1 \) always will be the symbol 0, \( X_2 \) will be 1, and \( X_3 \) will be \( B \), the blank. However, other tape symbols can be assigned to the remaining integers arbitrarily.

- We shall refer to direction \( L \) as \( D_1 \) and direction \( R \) as \( D_2 \).

Since each TM \( M \) can have integers assigned to its states and tape symbols in many different orders, there will be more than one encoding of the typical TM. However, that fact is unimportant in what follows, since we shall show that no encoding can represent a TM \( M \) such that \( L(M) = L_a \).

Once we have established an integer to represent each state, symbol, and direction, we can encode the transition function \( \delta \). Suppose one transition rule is \( \delta(q_i, X_j) = (q_k, X_l, D_m) \), for some integers \( i, j, k, l, \) and \( m \). We shall encode this rule by the string \( 0^i10^j10^k10^l10^m \). Notice that, since all of \( i, j, k, l, \) and \( m \) are at least one, there are no occurrences of two or more consecutive 1's within the code for a single transition.

A code for the entire TM \( M \) consists of all the codes for the transitions, in some order, separated by pairs of 1’s:

\[
C_111C_211 \cdots C_{n-1}11C_n
\]

where each of the \( C \)'s is the code for one transition of \( M \).
**Theorem 9.3:** If $L$ is a recursive language, so is $\overline{L}$.

**Proof:** Let $L = L(M)$ for some TM $M$ that always halts. We construct a TM $\overline{M}$ such that $\overline{L} = L(\overline{M})$ by the construction suggested in Fig. 9.3. That is, $\overline{M}$ behaves just like $M$. However, $M$ is modified as follows to create $\overline{M}$:

1. The accepting states of $M$ are made nonaccepting states of $\overline{M}$ with no transitions; i.e., in these states $\overline{M}$ will halt without accepting.

2. $\overline{M}$ has a new accepting state $r$; there are no transitions from $r$.

3. For each combination of a nonaccepting state of $M$ and a tape symbol of $M$ such that $M$ has no transition (i.e., $M$ halts without accepting), add a transition to the accepting state $r$.

Since $M$ is guaranteed to halt, we know that $\overline{M}$ is also guaranteed to halt. Moreover, $\overline{M}$ accepts exactly those strings that $M$ does not accept. Thus $\overline{M}$ accepts $\overline{L}$. $\square$
\( x_i, y_i \in \Sigma^* \sum \)

\( x_1, x_2, \ldots, x_k = y_1, y_2, \ldots, y_k \)

\[ \{(aa, aab), (bb, ba), (abb, b)\} \]

\( x_1 x_2 x_3 = y_1 y_2 y_3 \)

\[ aabb aaabb - aabbaaabb b \]

\[ aabbaaabb = aabad \]

\[ (x_2, y_2), (x_2, y_2) \]

\( a, b \)

\( (x_1, y_1) \)
\[
\frac{G_1}{L(G_1) \cup L(G_p)} \quad G_x \quad G_p
\]

\[L(G_1) \subseteq L(G_2) \quad \overline{L(G_1) \cup L(G_p)} = [\Sigma U(1, 2, \ldots, n)]^*
\]

\[G = (N, \Sigma, P, S)
\]

\[N = \{S, S_x, S_p\},
\]

\[\Sigma \quad G_x \quad G_p
\]

\[P = \{P_x \cup P_p \cup \{S \rightarrow S_x | S_p\}\}
\]

\[i_1, i_2, \ldots, i_k
\]

\[\overrightarrow{S} \quad \overrightarrow{S_x} \quad \overrightarrow{\chi_x S_x} \quad \overrightarrow{\chi_x \chi_x S_x i_{21}}
\]

\[\overrightarrow{\chi_x \chi_x \chi_x \ldots \chi_x S_x i_{2k-1} \ldots i_{21}}
\]

\[\overrightarrow{\chi_x \chi_x \chi_x \ldots \chi_x \chi_x \chi_x i_{k} i_{k-1} \ldots i_{21}}
\]
\[
\begin{align*}
S & \Rightarrow S_y \Rightarrow x_1 \bar{S}_y \bar{a}_1 \Rightarrow x_1 \bar{S}_y \bar{b}_1 \\
& \Rightarrow \nu_{i_1} \nu_{i_2} \cdots \nu_{i_k} S_y i_{k-1} \cdots \bar{a}_1 \\
& \Rightarrow \nu_{i_1} \nu_{i_2} \cdots \nu_{i_k} \nu_{i_{k-1}} \bar{b}_1 \cdots \bar{a}_1 \\
\end{align*}
\]

\[x_1 x_2 \cdots x_k = \nu_{i_1} \nu_{i_2} \cdots \nu_{i_k}, \text{ since } i_{1,2,\ldots,i_k} \]

\[(x_1 x_2 \cdots x_k) \]

\[G_y \]

\[i_{i_{k-1}} \cdots \bar{i}_{2_1} \]

\[w \in L(G) \]

\[G_y \]

\[i_{j_{p-1}} \cdots \bar{i}_{2_1} \quad p \geq 1 \]

\[x_1 x_2 \cdots x_{i_p} x_{i_p} = \nu_{j_1} \nu_{j_2} \cdots \nu_{j_{i_p}} \nu_{i_{i_p}} \]

\[i_1, i_2, \ldots, i_{p-1}, i_p \]