Date: 11-5-21

CS211 - Discrete Structures
Assignment # 5, Spring 2021
20K-1052 (S.M. Hassam Ali)

1- Number theory.

Number theory being a pure mathematics branch deals with the study of the natural numbers and the integers. It helps in finding the relation between different type of numbers, and to verify it. It consist of theoretical and experimental part.

Applications:

1- Generating Pseudorandom Numbers.

Pseudo Random Number Generator (PRNG) is an algorithm that uses number theory (in the form of mathematical formulas) to produce sequence of random numbers. Linear congruential Generator is the most popular algorithm for generating randomized numbers. The recurrence relation is defined as:

$$x_{n+1} = (a x_n + c) \bmod m$$

Where x is the sequence of random values.
m is the modulus greater than 0.
a is the multiplier, c is the increment.
x_0 is the seed or the starting value.

Lets take some values for implementing the function:

$a = 5 \quad x_0 = 3 \quad c = 9 \quad m = 5$

$x_1 = (5 \times 3 + 9) \bmod 5 = 24 \bmod 5 = 4$

$x_2 = (5 \times 4 + 9) \bmod 5 = 28 \bmod 5 = 3$

$x_3 = (5 \times 3 + 9) \bmod 5 = 24 \bmod 5 = 4$

K20-1052

Date:

Even the SRAND function in C, C++ language uses the same algorithm of generating pseudo random number.

2- Cryptography Algorithms.

A technique through which we secure information and communications through use of codes so that to whom the information is intended can understand the process. The concepts are derived ~~for~~ from mathematical theory that uses certain algorithms to convert messages in a specific code and then decode it.

~~Applications:~~

Caesar Cipher, a way of encryption of the messages in which each letter moves three letters forward.
The function we have is $f(p) = (p+K) \bmod 26$
Here K is the public key which is 3. The alphabets start ~~for~~ from (A(0) to Z(25)).
Take an example of word HELLO.
H(7), E(4), L(11), O(14)

$f(H) = (7+3) \bmod 26 = 10 \bmod 26 = 10\ (K)$
$f(E) = (4+3) \bmod 26 = 7 \bmod 26 = 7\ (H)$
$f(L) = (11+3) \bmod 26 = 14 \bmod 26 = 14\ (O)$
$f(O) = (14+3) \bmod 26 = 17 \bmod 26 = 17\ (R)$

The encrypted word is: KHOOR

Inorder to decrypt the key is taken as -3 and same method of working.
We also have shift cipher function $f(p) = (p+11) \bmod 26$ where the key is 11.

K20-1052

Date:

There is another RSA algorithm for encryption and decryption. It uses p and q two distinct prime numbers. for encryption we have $c \equiv m^e \bmod n$ and decryption $m \equiv c^d \bmod n$.
$n = pq$, $k = (p-1)(q-1)$, $1 < e < k$, $gcd(e,k) = 1$
d is the multiplicative inverse of e modulo k.

2. Proofs

A proof is a valid argument that establishes the truth of a mathematical statement. It uses the ingredients of hypotheses of the theorem, axioms assumed to be true; previously proven theorems and rules of inference.

Applications:

1- Verifying computer programs

So the programs we create using the algorithm or a particular language uses proofs in order to check what has been written is valid or false. For proving conditional statements we have direct and indirect proofs. For non-conditional statements we have indirect, direct, if-and-only-if, existence and uniqueness proofs, disproofs. Then comes mathematical induction. Take an example of a conditional statement in a C language that `if(x > 0){ x = x+1 }`. So here it would validate the statement using proof. Like direct proof would be used by the compiler for the condition $x > 0$ since it will take a value input by the user through console, hence would easily verify the condition.

2- Artificial Intelligence inferences.

AI has been performing its task very well. Ever wondered why is that so? It has been using the help of proof that has been written into its memory. For both the conditional and the non-conditional statements. AI has been put into many of the softwares integrated with electric components. Let's take an example of an automotive temperature sensor that measures the temperature based on the inferences. These inferences use the proofs. Like if the particular temperature has been set off by the system so it would validate the values using proofs. Suppose temperature has to be increased if lesser than 25°C by 2 or more degree. So it would use a direct proof method for comparing values.

3- Trees.

A general tree graph has no cycle that is known as acyclic graph. A tree is defined as non-empty finite set of elements called vertices or nodes having a property that each node can have maximum degree 1 and maximum degree n. It can be partitioned into n+1 disjoint subsets. such that the first subset contains the root of ~~three~~ tree.

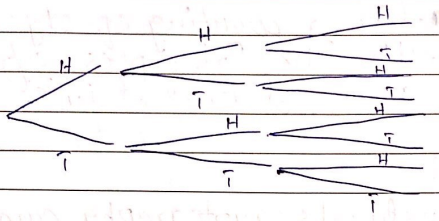
Applications:

1- Used in probability

Finding probabilities using the help of tree diagram has made it so easy. We can solve the bigger problems of probability using a rooted tree diagram where we can have all the possible

Date: _____

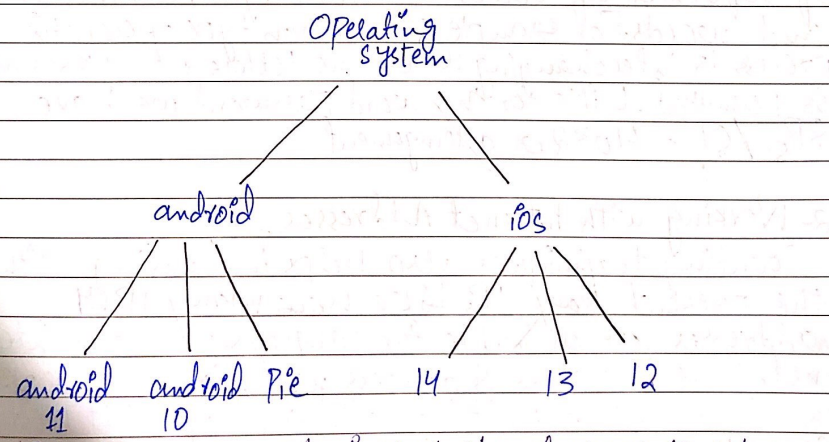
Outcomes in our diagram. For example if we want to find the probabity of three H/T in a row so we can do it like:



The probability of HHH/TTT would be $= \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$.

2- Forming a hierarchy.

Trees not just help us in finding the outcomes or the desired results to the problem but it also help in forming a hierarchy to simplify the situation or a problem so that it can be drawn into simpler way.



This is one of most simplest structure of the tree, we can design it to our needs.

K20-1052

Date:

4- Counting (combinatorics)

It is the branch of mathematics dealing with the study of finite or countable discrete structures. It includes numeration or counting of objects having certain properties. The Principles of counting includes Sum and product rule.

Applications:

1- Communication networks, cryptography and network security.

Permutations are frequently used in communication networks, parallel and distributed systems. Routing different permutations on a network for performance evaluation is a common problem in these fields. We also need to prevent our data from potential threats such as virus and hackers so here comes encryption. It envolves manipulation of sequences of codes such as digits, characters and words. For example one common type of encryption process is interchanging. Where the letters of a password is permuted. Like for the word password we have $8P_8 = 8! = 40320$ allowgement.

2- Working with Internet Addresses.

Counting techniques also helps in dealing with the present day IPs. Like how many IPv4 addresses are available for computers on the internet. There is a class A address used for large networks, a 0, followed by a 7 bit netid and a 24 bit hostid. Class B address used for the medium sized networks, a 10, followed by a 14 bit netid and a 16 bit hostid. Class C address used for the small networks, a 110, follo-

wed by a 21 bit netid and a 8-bit hostid. After multiplying the netid and hostid and then combining them all we have about 3,737,091,842 IPv4 addresses which combinatorics has helped to find.

5-) Sequence and Series.

It is a set of numbers in a definite order according to some defined rules. Each numb-er of set is called a term and its length is defined by n number of terms. A series is simply the sum of various terms of a sequence. If the sequence is $x_1, x_2, x \cdots x_n$ then series would be $x_1 + x_2 + x_3 - \cdots x_n$.

Applications:

1- Sequence in computer programming.

An important data type in computer programming consist of finite sequences. Known as one-dimensional arrays; a single variable in which a sequence of variables may be stored. For example, we have an array of size 10 of student name of type string. Then it would save the name stdn[0], stdn[1]... -- stdn[9]. So here the common difference between each term (name)/(value of index) is 1. This sequ-ence become arithmetic progression because of common difference. In certain loop conditions we increment the value of i either by 1, 2, 3... n depending on our need so each time same value is incremented with, makes the common difference or a common multiplier known as common ratio for the G.P.

2- Helps to understand and work with different type of series.
Whenever we need to work with different type of series in order to identify them, then we do use it. For example identifying the sequence that maybe either finite or infinite (3, 6, 9 ... n). Or for finding the particular value or some sum of particular values. One of the most famous sequence is the Fibonacci sequence. In which each term is the sum of the two preceding term. This series will help in finding the compound interest since the previous amount in compound interest is added to the new amount for a total value.

6- Graph theory
A graph is a non-linear data structure consisting of nodes and edges. The nodes are sometimes also refered to as vertices and edges are lines or arcs that connect any two nodes in the graph.

Applications:
1- Representing Networks.
Graphs are used to represent networks. The networks may include paths in a city or telephone network or circuit network. Graphs are also used in social media networks like Instagram, Facebook, Whatsapp and many more. For example in Instagram, each person is represented by a vertex. Each node is a structure and contains ~~if~~ information like person's user name that is id, name, gender and other profile features. Some

social networks graph include friendship graphs, collaboration graphs and influence graphs.

2- Information Networks.

Graphs can be used to model different types of networks that link different types of information. In a web graph, web pages are represented by vertices and links are represented by directed edges. A web graph models the web at a particular time. In citation network, research papers in a particular discipline are represented by vertices. When a paper cites a second paper as a reference, there is an edge from vertex representing this paper to the vertex representing the second paper.