Discrete Structures Report

Pratik Sahoo

July 24, 2023

1 Introduction

In this report, I will be covering the topics that I studied during this reading project of discrete structures. This is but a brief summary of what I covered, but I will try my best to refer to the relevant points.

2 Propositional Calculus & Quantifiers

This reading project began by studying logical propositions and their truth tables. It includes operators like $\neg$ (negation), $\wedge$ (conjunction), $\vee$ (disjunction), $\rightarrow$ (implication), and $\leftrightarrow$ (bi-implication). Quantifiers, namely $\forall$ (for all) and $\exists$ (there exists), are used to express statements on a set of objects rather than an object. First order logic uses quantifiers over variables/objects, while Second order logic uses quantifiers over predicates as well (for example, Well Ordering Theorem).

3 Proofs

Proofs in mathematics involve demonstrating the truth of a statement using logical reasoning. Common proof techniques include direct proof, proof by contradiction, and proof by induction.

4 Induction Hypothesis & Well Ordering Theorem

Induction is a powerful proof technique. The Induction Hypothesis states that if a statement is true for 0 (base case) and if it being true for one value implies it is true for the next value (inductive step), then it is true for all values. This is equivalent to the Well Ordering Theorem, which states that for every predicate P, if there exists a natural number for which it is true, there exists a least natural number for which it is true. In other words, every non-empty set of natural numbers has a least element.

5 Properties of Prime Factorizations

Prime factorization decomposes a number into its prime factors. The unique factorization theorem asserts that every integer greater than 1 can be expressed as a product of prime numbers in a unique way.

6 Modular Arithmetic & Chinese Remainder Theorem

Modular arithmetic involves operations on remainders when dividing by a fixed integer (the modulus). The Chinese Remainder Theorem states that given k co-prime integers and k values (modulo each of those integers, respectively), there exists a unique solution to this series of congruences, modulo the product of the co-prime integers.

7 Totient Function

The totient function, denoted as $\phi(n)$, counts the positive integers less than or equal to n that are coprime to n. It can be calculated as

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Also,

$$gcd(n_1, n_2) = 1 \implies \phi(n_1 \cdot n_2) = \phi(n_1) \cdot \phi(n_2)$$

8 Modular Exponentiation & Euler's Theorem

Modular exponentiation calculates large powers efficiently in modular arithmetic. Euler's Theorem generalizes Fermat's Little Theorem and provides an efficient way to find remainders when exponentiating in modular arithmetic. Euler's theorem states that

$$gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \pmod{n}$$

9 Application of Modular Exponentiation in RSA

RSA (Rivest–Shamir–Adleman) is a widely used public-key encryption system that relies on modular exponentiation and Euler's theorem. It ensures secure communication over untrusted networks by encrypting and decrypting messages using modular exponentiation. Its security lies in the fact that products of large primes cannot be factorized in polynomial time.

10 Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange is a protocol that allows two parties to exchange a secret key over public communication channels securely. It relies on the difficulty of discrete logarithms, which cannot be solved in polynomial time. Given Alice & Bob, both of whom have private keys a & b respectively, they share (publicly) their public keys: $g^a \pmod p$ where p is a prime and g is a primitive root of p, for Alice and similarly for B. Due to the difficulty of discrete logarithms, it is not feasible to compute the private key from the public key. Now, Alice & Bob raise each other's public keys to the power of their own private key, and both result with $g^{ab} \pmod p$, which cannot be computed by an outside party in polynomial time. Also, Alice and Bob now have a symmetric shared key between themselves, without revealing to each other their own private keys, and only communicating over a public network.

11 Sets & Relations

Sets are fundamental mathematical objects used to collect elements. Relations are used to establish connections between elements of sets. Relations can be reflexive, symmetric, transitive, or equivalence relations if they are all three.

12 Posets, Chains & Anti-chains

Partially Ordered Sets are sets with a partial order relation that is reflexive, antisymmetric, and transitive. They are used to model hierarchical structures. Chains are subsets of a poset where any two elements are comparable. Anti-chains are subsets where no two elements are comparable.

13 Mirsky's Theorem & Dilworth's Theorem

Mirsky's Theorem states that the size of the largest chain in any poset is the minimum size of an anti-chain cover. Similarly, Dilworth's Theorem states that the size of the largest anti-chain in any poset is the minimum size of a chain cover.

14 Walks, Paths & Cycles

In graph theory, walks, paths, and cycles are fundamental concepts. Walks are sequences of vertices connected by edges, paths are walks with distinct vertices and cycles are closed paths.

15 Eulerian Trails & Circuits, Hamiltonian Cycle

Eulerian trails are walks that visit every edge exactly once, while Eulerian trails are *closed* walks that visit every edge exactly once. Also, Hamiltonian cycles are cycles that visit every

vertex (exactly once, since cycles do not repeat nodes) and return to the starting vertex.

16 Coloring of Graphs

Proper graph colouring assigns colours to vertices such that adjacent vertices have different colours. The chromatic number is the minimum number of colours needed.

17 Bipartite & Complete Graphs

Bipartite graphs have vertices divided into two sets with edges only between sets. Complete graphs have edges between every pair of vertices. Chromatic number of a bipartite graph is 2, while that of a complete graph is the number of nodes in said graph.

18 Cliques & Independent Sets

Cliques are subsets of vertices where every pair is adjacent, and clique number is the size of the largest clique. Independent sets are subsets where no two vertices are adjacent, and independence number is the size of the largest independent set.

19 Matching in a Graph, Hall's Theorem

A matching is a set of edges with no common vertices. A perfect matching is one where every node is matched, and a complete matching of a bipartite is one where every element from the first subset is matched. Hall's Theorem provides a condition for the existence of a complete matching in bipartite graphs, in terms of shrinking of sets. It says that a bipartite graph $G = (X, Y, E)$ has a complete matching *iff* no subset of X is shrinking.

20 Trees

Trees are acyclic, connected graphs. They have important applications in computer science and data structures. Forests are acyclic graphs. For any pair of nodes in a tree, there is exactly one path between them. Also, the number of edges in a tree is 1 less than the number of nodes. Both of these are easy to see via induction on trees. Interestingly enough, if number of edges of a graph is 1 less than number of vertices and it is connected, then it must be a tree.

21 Perfect Graphs

Perfect graphs are graphs where the chromatic number is equal to the clique number, for itself and every induced subgraph. The Perfect Graph Theorem states that the complement of a graph is perfect *iff* the graph is perfect. The complement of a graph is the graph with

same set of vertices, but with there is an edge between 2 vertices if and only if there isn't in the original graph.

22 Countability & Discussion of Infinities

A set is countable if there exists a bijection from it to the natural numbers. However, not all sets are countable. Some sets, such as the real numbers $\mathbb{R}$, are uncountable. Cantor's diagonal argument is a famous proof demonstrating the uncountability of the real numbers. It shows that there are more real numbers between 0 and 1 than there are natural numbers. This is is done by supposing the bijection exists, listing the real numbers in binary decimal format one after the other, and picking the opposite of the ith decimal digit of the ith number and concatenating all of them to construct a new number that does not belong to this bijection, creating a contradiction.

The power set of a set A is the set of all subsets of A. Cantor's theorem uses an elegant proof to show that for any set, it's power set has greater cardinality. Also, it can be shown that the cardinality of $2^{\mathbb{N}}$, ie, the power set of the natural numbers, is equal to that of the real numbers.

(Solving problems on bijections, cardinality and infinite sets was probably my favourite part of this reading project)

23 Conclusion

Discrete structures play a crucial role in computer science and mathematics. The topics covered in this report are fundamental to understanding various aspects of discrete mathematics and the underlying logic and structure to the results.