DISCRETE MATHEMATICS I

Soumyashant Nayak, notes by Ramdas Singh

Third Semester

List of Symbols

Placeholder

Contents

Chapter 1

DISCRETE STRUCTURES

1.1 A Brief Introduction

July 22nd.

Discrete mathematics is primarily the study of tools for reasoning precisely the systematically about digital systems, logical problems, and combinatorial structures such as the integers, graphs, logical statements, and finite automata. Furthermore, combinatorics is the mathematics of counting and configuration; the counting, organizing, and analyzing discrete structures.

Bloch's principle, or Bloch's heuristics, states that every proposition on whose statement the actual infinity occurs can always be considered as a consequence of a proposition where it does not occur as a proposition on finite terms. The *Ramsey principle* states that complete disorder is impossible. In any sufficiently large structure, order or regularity must emerge. These two principles may be considered complimentary to each other.

1.2 Useful Methods

The method of *double counting* can be thought of a creative device or trick. Before strictly showing the statement, we utilise some examples.

Example 1.1. Suppose we wish to show that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. We first ask how many ways can a subset be chosen from $\{1, 2, \ldots, n\}$. The first method is to build a subset by deciding whether we want i to be a part of our subset for $i \in \{1, 2, ..., n\}$. The second method is find the number of subsets of caridnality i for $i \in \{1, 2, \ldots, n\}$ and add up all the results. This leads us to conclude $2^n = \sum_{k=0}^{n} \binom{n}{k}$ after equating the answers from both methods.

Theorem 1.2 (The *q-binomial theorem*)**.** *We use the following notation:*

$$\binom{n}{k}_q = \frac{(q^n - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1) \cdots (q - 1)}. \tag{1.1}$$

Simply stated, the q-binomial theorem is

$$\sum_{k=0}^{n} q^{\binom{k}{2}} \binom{n}{k}_q z^k = \prod_{i=0}^{n-1} (1 + q^i z). \tag{1.2}$$

The proof of the above theorem is performed by double counting; counting the number of pairs (U, B) where U is a k-dimensional subspace of $\mathbb{F}_q^n$ and B is the flag of nested subspaces of U.

Reccurrence Relations and Generating Functions

Perhaps, the most important example of a recurrence relation is the Fibonacci sequence, where the terms in the sequence are defined as $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Let us find the *generating function* of this sequence; we start by creating

$$F(t) = F_0 + F_1 t + F_2 t^2 + F_3 t^3 + \cdots, \tag{1.3}$$

the generating function of $(F_n)_{n=0}^{\infty}$. We can then work as follows—

$$\begin{aligned} tF(t) &= F_0 t + F_1 t^2 + \cdots, \\ t^2 F(t) &= F_0 t^2 + \cdots, \\ \implies (1 - t - t^2)F(t) = t \implies F(t) &= \frac{-t}{t^2 + t - 1}. \end{aligned} \tag{1.4}$$

If we look at $F_{n+1} = 1 \cdot F_n + 1 \cdot F_{n-1}$ and $F_n = 1 \cdot F_n + 0 \cdot F_{n-1}$, we may notice a matrix as $\begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix}$. Back substituting multiple times leads us to conclude $\begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. We can then diagonalize the centre matrix to decompose it as $P \begin{bmatrix} (1+\sqrt{5})^n/2^n & 0 \\ 0 & (1-\sqrt{5})^n/2^n \end{bmatrix} P^{-1}$; thus, the terms of the sequence are really linear combinations of the diagonal elements that appear.

Principle of Inclusion-Exclusion

July 24th.

Simply stated, for sets A and B, $\#(A \cup B) = \#A + \#B + \#(A \cap B)$. For three sets A, B and C, we have $\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(B \cap C) - \#(A \cap C) + \#(A \cap B \cap C)$. This can be extended to any finite number of finite sets.

Theorem 1.3 (The *principle of inclusion-exclusion*)**.** *Let S be an N-set ($\#S = N$), and let $E_1, E_2, \ldots, E_r$ be, not necessarily distinct, subsets of S. For any subset M of the indexing set $\{1, 2, \ldots, r\}$, let $N(M)$ denote the number of elements of S in $\bigcap_{i \in M} E_i$, and for $0 \leq j \leq r$, define*

$$N_j = \sum_{\#M = j} N(M). \tag{1.5}$$

Then the number of elements of S not in any of the E_i's is

$$\#(S \setminus \bigcup_{i=1}^{r} E_i) = N - N_1 + N_2 - N_3 + \cdots + (-1)^r N_r. \tag{1.6}$$

Proof. For $x \in S$, define $M : S \to \{0, 1\}$ as $M(x) = 1$ if $x \in \bigcap_{i \in M} E_i$ and 0 otherwise. Thus,

$$\sum_{x \in S} M(x) = \#(\bigcap_{i \in M} E_i) = N(M) \implies N_j = \sum_{\#M = j} \sum_{x \in S} M(x) = \sum_{x \in S} \sum_{\#M = j} M(x). \tag{1.7}$$

The alternating sum then becomes

$$\sum_{x \in S} 1 - \sum_{x \in S} \sum_{\#M = 1} M(x) + \cdots + (-1)^r \sum_{x \in S} \sum_{\#M = r} M(x) = \sum_{x \in S} \left(1 - \sum_{\#M = 1} M(x) + \cdots + (-1)^r \sum_{\#M = r} M(x) \right). \tag{1.8}$$

Call the term within the parentheses as $F(x)$. We deal with cases; if $x \notin \bigcup_{i=1}^{r} E_i$, then $F(x) = 1$. If x is in exactly $k \geq 1$ of the sets $E_1, E_2, \ldots, E_r$, then

$$F(x) = 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k \binom{k}{k} = (1 - 1)^k = 0. \tag{1.9}$$

This is independent of k; we conclude that the alternating sum reduces to the number of elements in S not in any of the E_i's. ∎

Corollary 1.4. *Retaining notation from the previous theorem, if* $S = \bigcup_{i=1}^{r} E_r$*, then*

$$N = N_1 - N_2 + \cdots + (-1)^{r-1} N_r. \tag{1.10}$$

We look at some examples of the principle in use.

Example 1.5. Let d_n be the number of permutations π of the set $\{1, 2, \ldots, n\}$ such that $\pi(i) \neq i$ for all $1 \leq i \leq n$. Such a permutation is called a *derangement*, where no point is fixed. We wish to count all such permutations. Let the set of all permutations of the set be S. Let E_i denote the set of all permutations that fix i, for $1 \leq i \leq n$. Thus, S without $\bigcup_{i=1}^{n} E_i$ would then denote the set of all derangements. Making use of the principle, we have

$$\#(S \setminus \bigcup_{i=1}^{n} E_i) = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right) \tag{1.11}$$

which is approximately $\frac{n!}{e}$ for larger n. Thus, the probability of choosing a derangemnet is e^{-1}.

Example 1.6. Suppose we have two sets X and Y with $\#X = n$ and $\#Y = k$. We ask how many surjective maps exists from X to Y. The set S, this time, is the set of all functions from X to Y, being Y^X. E_i denotes the set of functions from X to Y such that y_i is not in the image of X. The elments within S not in any of the E_i's are surjective maps. Clearly, $N_i = \binom{k}{i}(k-i)^n$, and the cardinality of $S \setminus \bigcup_{i=1}^{k} E_i$ is then

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n. \tag{1.12}$$

Example 1.7. We wish to show that the expression $\sum_{i=0}^{n} (-1)^i \binom{n}{i}\binom{m+n-i}{k-i}$ evaluates to $\binom{m}{k}$ if $m \geq k$, and 0 otherwise. To this end, fix $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$ and set $Z = X \cup Y$. We now ask how many k-subsets of Z consist of only points form Y. Let S be the set of all k-subsets of Z, and denote E_i to be the set of k-subsets of Z containing x_i for $1 \leq i \leq n$. The left hand side of our inclusion-exclusion principle evaluates to $\binom{m+n}{k}$. Each N_i evaluates to $\binom{n}{i}\binom{m+n-i}{k-i}$, proving our expression above.

The next example relates to the Euler totient function.

Example 1.8. Recall that, from the *fundamental theorem of arithmetic*, each natural number may be expressed uniquely (upto order) as the product of distinct primes raised to values, that is, $n = p_1^{a_1} \cdots p_r^{a_r}$. The *Euler totient function* $\phi : \mathbb{N} \to \mathbb{C}$ acts on the naturals and returns $\phi(n)$, the number of positive integers $k \leq n$ such that $\gcd(k, n) = 1$. Certainly, $\phi(p) = p - 1$ for a prime p. Our task is to find a closed form formula for $\phi(n)$.
Set $S = \{1, 2, \ldots, n\}$, and set E_i to be the set of integers in S divisible by p_i for $1 \leq i \leq r$. Clearly, the value $\#(S \setminus \bigcup_{i=1}^{r} E_i)$ returns the set of all numbers in $\{1, 2, \ldots, n\}$ coprime to n. Note that $N = n$. The value of N_1 is $\sum_{i=1}^{r} \frac{n}{p_i}$, the value of N_2 is is $\sum_{1 \leq i \leq j \leq r} \frac{n}{p_i p_j}$. The closesd form formula then becomes

$$\phi(n) = \#(S \setminus \bigcup_{i=1}^{r} E_i) = n - n\sum_{i=1}^{r} \frac{1}{p_i} + n \sum_{1 \leq i \leq j \leq r} \frac{1}{p_i p_j} + \cdots = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right). \tag{1.13}$$

Number Theory

We continue with the Euler totient function.

Theorem 1.9. $\sum_{d|n} \phi(d) = n.$

Proof. For each integer $m \in \{1, 2, \ldots, n\}$, the value $\gcd(m, n)$ is a divides n. Fix a divisor d of n. The number of integers m such that $\gcd(m, n) = d$ is equal to the number of integers m such that $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$, where $\frac{m}{d}$ runs over integers between 1 and $\frac{n}{d}$. Therefore, the number of such m is $\phi\left(\frac{n}{d}\right)$. Summing over all divisors d of n, we get:

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

which is the same as $\sum_{d|n} \phi(d)$. ■

The *Möbius function* is defined as

$$\mu(d) := \begin{cases} 1, & \text{if } d \text{ is a product of even number of distinct primes,} \\ -1, & \text{if } d \text{ is a product of odd number of distinct primes,} \\ 0, & \text{if otherwise; the number } d \text{ is square-free.} \end{cases} \tag{1.14}$$

Theorem 1.10.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{if } n = 1, \\ 0, & \textit{if otherwise.} \end{cases} \tag{1.15}$$

Proof. For $n = 1$, it is clear. For $n > 1$, rewriting n as $p_1^{a_1} \cdots p_r^{a_r}$ helps us see that

$$\sum_{d|n} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots = (1-1)^r = 0. \tag{1.16}$$

■

This property of the Möbius function proves to be useful.

July 29th.

Theorem 1.11 (The *Möbius inversion formula*)**.** *Suppose we have two function $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$ which relate as*

$$f(n) = \sum_{d|n} g(d). \tag{1.17}$$

Then the function g satisfies

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d). \tag{1.18}$$

Proof. We work as

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \left(\sum_{d'|d} g(d')\right) = \sum_{d|n,\ d'|d} \mu\left(\frac{n}{d}\right) g(d') = \sum_{d'|n,\ m|\frac{n}{d'}} g(d')\mu(m) \\ &= \sum_{d'|n} \left(g(d') \left(\sum_{m|\frac{n}{d'}} \mu(m)\right)\right) = g(n). \end{aligned} \tag{1.19}$$

■

Example 1.12. Let N_n denote the number of distinct circular binary sequences of length n, up to rotation. That is, two sequences are considered the same if one is a rotation of the other. We aim to compute N_n explicitly.
Let $M(d)$ denote the number of aperiodic circular binary sequences of length d, meaning sequences that are not periodic with any smaller period. Note that each such aperiodic sequence of length d contributes to sequences of length n whenever $d \mid n$. Indeed, every binary circular sequence of length n can be viewed as made up of $\frac{n}{d}$ repetitions of a primitive block of length d.
Thus, we have:

$$N_n = \sum_{d|n} M(d).$$

Now consider the total number of binary strings of length n, which is 2^n. Each such string can be arranged in a circle in n different ways, one for each rotation. However, many of these circular sequences are identical under rotation, so we overcounted by a factor of the size of the symmetry group.
Let $f(n) = 2^n$ be the total number of binary strings of length n. Each such string is generated by repeating an aperiodic sequence of length d exactly $\frac{n}{d}$ times, for some $d \mid n$. Since each aperiodic circular sequence of length d has d rotations, we get:

$$f(n) = 2^n = \sum_{d|n} d \cdot M(d).$$

Applying Möbius inversion to this relation, we obtain:

$$n \cdot M(n) = \sum_{d|n} \mu(d) \cdot 2^{n/d},$$

and hence,

$$M(n) = \frac{1}{n} \sum_{d|n} \mu(d) \cdot 2^{n/d}.$$

Substituting back into the formula for N_n, we get:

$$N_n = \sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \sum_{k|d} \mu(k) \cdot 2^{d/k}.$$

Interchanging the order of summation, we arrive at the classical formula:

$$N_n = \frac{1}{n} \sum_{d|n} \phi(d) \cdot 2^{n/d},$$

where ϕ is Euler's totient function.

Lemma 1.13 (*Burnside's lemma*)**.** *Let G be a permutation group acting on some finite set X. Let $\psi(g)$ denote the number of points of X fixed by $g \in G$. Then the number of orbits of G is $\frac{1}{|G|} \sum_{g \in G} \psi(g)$.*

In the above, by the set of points fixed by $g \in G$, we mean the set $\{x \mid g \cdot x = x\}$. By the *orbit* of x, we mean the set $\{g \cdot x \mid g \in G\}$.

Such inversion formulae are common in discrete math. The following are some examples.

Example 1.14.

- For an integer n, $f(n) = \sum_{i=1}^{n} g(i)$ if and only if $g(n) = f(n) - f(n-1)$. This is known as a *telescoping sum*.
- For an integer n, $f(n) = \sum_{d|n} g(d)$ if and only if $g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$. This is the Möbius inversion formula.

- For a set S, $f(S) = \sum_{T \subseteq S} g(T)$ if and only if $g(S) = \sum_{T \subseteq S} (-1)^{|S|-|T|} f(T)$.

Partially Ordered Sets

Definition 1.15. A *poset* S, or a *paritally ordered set*, is a (countable or finite) set of objects with a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ for all $x \in S$.
2. Antisymmetry: if $x \leq y$ and $y \leq x$, for some $x, y \in S$, then $x = y$.
3. Transitivity: if $x \leq y$ and $y \leq z$, for some $x, y, z \in S$, then $x \leq z$.

Some examples are as follows.

Example 1.16.

1. $(\{1, 2, \ldots, n\}, \leq)$ is a poset, with $a \leq b$ if $b - a$ is a non-negative integer.
2. $(\{1, 2, \ldots, n\}, \leq_1)$ is also a poset, where $a \leq_1 b$ if $a \mid b$.
3. $(\mathcal{P}(\{1, 2, \ldots, n\}), \leq_2)$ is also a poset; here, $S \leq_2 T$ if $S \subseteq T$. The power set is also denoted as $2^{\{1,2,\ldots,n\}}$.
4. The set of partitions of $\{1, 2, \ldots, n\}$, equippied with the partial ordering of refinement. By a partition, we mean $\{S_1, S_2, \ldots, S_r\}$ such that $S_i \cap S_j = \emptyset$ for $i \neq j$, and $\bigcup_{i=1}^{r} S_i = \{1, 2, \ldots, n\}$. Similarly, let $\{T_1, T_2, \ldots, T_d\}$ be another partition. Then $\{S_1, \ldots, S_r\} \leq \{T_1, \ldots, T_d\}$ if for $1 \leq i \leq r$, $S_i \subseteq T_k$ for some $1 \leq k \leq d$. Here, we term $\{S_1, \ldots, S_r\}$ a *refinement* of $\{T_1, \ldots, T_d\}$.

The idea of the Möbius function really comes from posets, where its definition is more generalized. Here, $\mu(d, n)$ can be thought of as a place-in for $\mu\left(\frac{n}{d}\right)$.

Definition 1.17. The *Möbius function of a poset* is defined as

$$\mu(x, y) = \begin{cases} 0 & \text{if } x \not\leq y, \\ 1 & \text{if } x = y, \\ -\sum_{x \leq z < y} \mu(x, z) & \text{if } x \lneq y. \end{cases} \tag{1.20}$$

Note that we need only compute $\mu(x, y)$ on all intervals $[x, y]$ $(x \leq y)$. We call an element y a *successor* of x if there exists no z satisfying $x \lneq z \lneq y$. Note that the successor may not be unique. Let us denote any successor by $\text{succ}(x)$.

If g and f are two functions defined and related as

$$g(x) = \sum_{y \leq x} f(y). \tag{1.21}$$

We now introduce the *zeta function* ζ defined as $\zeta(x, y) = 1$ if $x \leq y$ and 0 otherwise. Thus, the above equation can be rewritten as

$$g(x) = \sum_{y \leq x} f(y) = \sum_{y \in S} \zeta(y, x) f(y). \tag{1.22}$$

Lemma 1.18. *A finite partial order can always be embedded in a total ordering; that is, there exists an indexing $S = \{x_1, \ldots, x_n\}$ such that $x_i \leq x_j$ in S implies $i \leq j$.*

As a proof outline, pick a maximal element x of S. Label it x_n. Repeat the process with $S \setminus \{x\}$, then proceed inductively. The embedding is then clear.

Thus, using the lemma, we can rewrite the relation between g and f in matrix form as

$$\begin{pmatrix} g(x_1) & \cdots & g(x_n) \end{pmatrix} = \begin{pmatrix} f(x_1) & \cdots & f(x_n) \end{pmatrix} \begin{pmatrix} \zeta(x_1, x_1) & \cdots & \zeta(x_1, x_n) \\ \vdots & \ddots & \vdots \\ \zeta(x_n, x_1) & \cdots & \zeta(x_n, x_n) \end{pmatrix}. \tag{1.23}$$

Since $\zeta(x_i, x_j) = 0$ when $i > j$, the matrix on the right is upper triangular. Also, all the diagonal entries are 1.

Index