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 $E_1, E_2, \dots, E_r$ be, not necessarily distinct, subsets of S. For any subset M of the indexing set $\{1, 2, \dots, r\}$, 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 $E_1, E_2, \dots, E_r$, 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 cloesd 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. $\sum\limits_{d|n} \phi(d) = n$.

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

$$\mu(d) := \begin{cases} 1, & \text{if } d \text{ is a product of even number of distinct primes,} \\ -1, & \text{if } d \text{ is a product of odd number of distinct primes,} \\ 0, & \text{if otherwise; the number } d \text{ is not square-free.} \end{cases} \tag{1.14}$$

Theorem 1.10.

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

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 $\operatorname{succ}(x)$.

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

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

August 5th.

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. Denote the above matrix on the right by Z. Note that $Z=I+N$ where I is the identity matrix and N is upper triangular with 0's on the diagonal. Z^{-1} can be computed by taking a power series, and noting that N^n is 0.

$$Z^{-1}=(I+N)^{-1}=I-N+N^2-N^3+\cdots+(-1)^{n-1}N^{n-1} \tag{1.24}$$

Let $M=[\mu(x_i,x_j)]$. We find the (x_i,x_j) entry of MZ as

$$\sum_{y\in P} M_{x_i,y}Z_{y,x_j} = \sum_{y\in P}\mu(x_i,y)\zeta(y,x_j) = \sum_{y\le x_j}\mu(x_i,y) = \sum_{x_i\le y\le x_j}\mu(x_i,y). \tag{1.25}$$

Noting that $\mu(x_i,x_j) = -\sum_{x_i\le z<x_j}\mu(x_i,z)$, we get the above expression to be 1 if $x_i=x_j$ and 0 otherwise. Thus, $MZ=I$. This is the used definition of the the Möbius functon. $ZM=I$ may be verified similarly.

Theorem 1.19. *Let $(P,\le)$ be a finite poset, with $f,g:P\to\mathbb{Z}$ functions. Then,*

1. $f(x)=\sum_{y\le x} g(y)$ *if and only if* $g(x)=\sum_{y\le x}\mu(y,x)f(y)$, *and*
2. $f(x)=\sum_{x\le y} g(y)$ *if and only if* $g(x)=\sum_{x\le y}\mu(x,y)f(y)$.

This is the Möbius inversion formula for a poset.

Proof. We have

$$\sum_{y\le x}\mu(y,x)f(y) = \sum_{y\le x}\left(\sum_{z\le y}\mu(y,x)g(z)\right) = \sum_{z\le x}\sum_{z\le y\le x}\mu(y,x)g(z) = \sum_{z\le x}g(z)\sum_{z\le y\le x}\mu(y,x) = g(x) \tag{1.26}$$

since $\mu(y,x)$ at the end will be zero if $z\neq x$. To show the converse, we have

$$\sum_{y\le x}g(y) = \sum_{y\le x}\sum_{z\le y}\mu(z,y)f(z) = \sum_{z\le x}f(z)\left(\sum_{z\le y\le x}\mu(z,y)\right) = f(x) \tag{1.27}$$

since $\mu(z,y)$ is zero if $z\neq x$. ■

Example 1.20. Verify that if the poset is the positive integers with the standard ordering $\le$, then

$$\mu(i,j)=\begin{cases}1 & \text{if } i=j,\\ -1 & \text{if } i=j-1,\\ 0 & \text{if otherwise.}\end{cases} \tag{1.28}$$

Example 1.21. Let our poset be $(2^S,\subseteq)$ for a set S. For fixed subsets $U,T\in 2^S$, we have

$$\sum_{U\subseteq R\subseteq T}(-1)^{\#T-\#S} = \begin{cases}1 & \text{if } U=T,\\ 0 & \text{if otherwise.}\end{cases} \tag{1.29}$$

To show this, without the loss of generality, we will assume that $U=\emptyset$. Denoting $\#T=n$, we have

$$\sum_{R\subseteq T}(-1)^{\#R} = \sum_{k=0}^{n}\binom{n}{k}(-1)^k = 0. \tag{1.30}$$

Here, $Z(R,T) = 1$ if $R \subseteq T$ and 0 otherwise. Also, $M(R,T) = (-1)^{\#T-\#R}$ if $R \subseteq T$ and 0 otherwise. Since $MZ = I$, $M(R,T)$ must be the Möbius function for $(2^S, \leq)$.

Chapter 2

RECURRENCE RELATIONS AND GENERATING FUNCTIONS

2.1 Generating Functions

August 7th.

We begin with ordinary ones.

Definition 2.1. For a sequence $(a_n)_{n\geq 0} \subseteq \mathbb{R}$, the *ordinary generating function* associated with this sequence is defined as

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots . \tag{2.1}$$

Note that we are not concerned with convergence right now. We deconstruct our abstraction of ideas into levels, starting with the first level as regarding ordinary generating functions as algebraic objects. One can multiply and add them to create new generating functions. The second level is regarding them as analytic objects, only if the radius of convergence is positive.

The above is known as *Z-transform*, where a sequence is mapped onto a function. When using the word transform, we generally mean a 'change of basis'; in this case, we are changing from a sequence space to a function space.

Definition 2.2. For a sequence $(a_n)_{n\geq 0} \subseteq \mathbb{R}$, the *exponential generating function* associated with this sequence is defined as

$$f(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = a_0 + a_1 x + \frac{a_2}{2!} x^2 + \cdots . \tag{2.2}$$

Again, we have transformed from a sequence space to a function space. One can also transform from a random variable space to a function space.

Definition 2.3. For a random variable X taking values in $\mathbb{R}$, the *moment generating function* associated with this random variable is defined as

$$M_X(t) = E[e^{tX}] = \sum_{n=0}^{\infty} \frac{E[X^n]}{n!} t^n = 1 + E[X]t + \frac{E[X^2]}{2!} t^2 + \cdots . \tag{2.3}$$

2.1.1 Algberaic Operaions

We give a kind of correspondence between algebraic operations and combinatorial interpretations.

1. Multiplying by x^k maps $a_0 + a_1x + a_2x^2 + \cdots$ to $a_0x^k + a_1x^{k+1} + a_2x^{k+2} + \cdots$. This corresponds to shifting the sequence $(a_0, a_1, \ldots)$ right by k places. This is known as the *shift operator*.
2. Multiplication is also defined; for two functions $a_0 + a_1x + a_2x^2 + \cdots$ and $b_0 + b_1x + b_2x^2 + \cdots$, their product is given by $a_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots$. This corresponds to combining objects of size k and size $n - k$ chosen independently.
3. Differentiation maps $a_0 + a_1x + a_2x^2 + \cdots$ to $a_1 + 2a_2x + 3a_3x^2 + \cdots$. This corresponds to weighing the sequence values by their index, with a shift of one place to the right.

Example 2.4. Suppose we have k boxes labelled 1 through k, and box i contains r_i balls for $1 \leq i \leq k$. We wish to encode all possible configurations in a kind of book-keeping device. For a particular $(r_1, \ldots, r_k)$, we have

$$\sum_{r_i \geq 0} x_1^{r_1} \cdots x_k^{r_k} = (1 + x_1 + x_1^2 + \cdots)(1 + x^2 + x_2^2 + \cdots) \cdots (1 + x_k + x_k^2 + \cdots). \tag{2.4}$$

We find the number of partitions of n (balls) into k numbers (boxes), where each number if non-negative. Disregarding the order, we set all the x_i's equal to each other. Thus, we wish to find the coefficient of x^n where $r_1 + \cdots + r_k = n$. From the sum above, we have

$$(1 + x + x^2 + \cdots)^k = (1 - x)^{-k} = \sum_{j=0}^{\infty} \binom{k-1+j}{j} x^j x^j. \tag{2.5}$$

Therefore, the required coefficient is $\binom{k-1+n}{n}$.

We briefly introduce the idea of rings. A *ring* $(R, +, *)$ is a set R with two operations $+$ and $*$ such that $(R, +)$ is an abelian group, $(R, *)$ is a monoid, and the distributive law holds. Some examples of rings include $\mathbb{Z}$, $M_n(\mathbb{C})$, and $\mathbb{C}[x]$. Another example is the ring of formal power series $\mathbb{C}[[x]]$, which consists of all series of the form $a_0 + a_1x + a_2x^2 + \cdots$ where $a_i \in \mathbb{C}$. We ask which elements of this ring are invertible.

We claim that $a_0 + a_1x + a_2x^2 + \cdots$ is invertible if and only if $a_0 \neq 0$. We find $b_0 + b_1x + b_2x^2 + \cdots$ such that

$$(a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots) = 1. \tag{2.6}$$

This first gives us $a_0b_0 = 1$, so $b_0 = \frac{1}{a_0}$. The next term gives us $a_0b_1 + a_1b_0 = 0$, so $b_1 = -\frac{a_1}{a_0^2}$. Continuing this process, we find that the coefficients of b can be expressed in terms of the coefficients of a as

$$b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}. \tag{2.7}$$

There is also the ring homomorphism $\mathrm{ev}_z : \mathbb{C}[[x]] \to \mathbb{C}$ where $x \mapsto z$, with $z \in \mathbb{C}$.

Example 2.5. Let d_n denote the number of derangements of $\{1, 2, \ldots, n\}$. We consider a derangement Π of $\{1, 2, \ldots, n + 1\}$ where

- Case I: $\Pi(n + 1) = i$ and $\Pi(i) = n + 1$ for some i. The number of such derangements is nd_{n-1}.
- Case II: $\Pi(n + 1) = i$ and $\Pi(j) = n + 1$ for some $i \neq j$. The number of such derangements is $d_{n+1} = nd_n$.

Thus, the total number of derangements is $d_{n+1} = n(d_n + d_{n-1})$. Here, $d_0 = 1$, $d_1 = 0$, and $d_2 = 1$. The exponential generating function, here, is

$$D(x) = \sum_{n=0}^{\infty} d_n \frac{x^n}{n!} \implies D'(x) = \sum_{n=1}^{\infty} nd_n \frac{x^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} d_{n+1} \frac{x^n}{n!} = \sum_{n=1}^{\infty} \frac{d_n}{(n-1)!} x^n + \sum_{n=1}^{\infty} \frac{d_{n-1}}{(n-1)!} x^n. \tag{2.8}$$

This gives us

$$D'(x) = xD'(x) + xD(x) \implies \frac{D'(x)}{D(x)} = \frac{x}{1-x} \implies D(x) = C\left(\frac{e^{-x}}{1-x}\right). \tag{2.9}$$

Plugging in $x = 0$ givens $C = 1$. Thus, the exponential generating function is

$$D(x) = \frac{e^{-x}}{1-x} = (1 + x + x^2 + x^3 + \cdots)(1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \cdots). \tag{2.10}$$

The coefficient of x^n in the above series is $\frac{d_n}{n!}$, giving us

$$d_n = n! \sum_{k=0}^{n} a_k b_{n-k} = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + (-1)^n \frac{1}{n!}\right). \tag{2.11}$$

Example 2.6. Suppose we wish to find number of ways to make n change with the denominations 1, 2, and 5. We use generating functions. Thus,

$$(1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^5 + x^{10} + \cdots) = \frac{1}{(1-x)(1-x^2)(1-x^5)}. \tag{2.12}$$

From above, taking the n^{th} derivative of the fraction,dividng it by $n!$, and evaluating at $x = 0$ provides the number of ways to make change for n.

2.1.2 Extended Binomial Theorem

August 8th.

We begin by extending the definition of a binomial coefficient.

Definition 2.7. For any $u \in \mathbb{R}$ and positive integer k, we define the *extended binomial coefficient* as

$$\binom{u}{k} = \frac{u(u-1)(u-2)\cdots(u-k+1)}{k!} \tag{2.13}$$

with $\binom{u}{0} = 1$.

Theorem 2.8. *For positive integers n and r, we have*

$$\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}. \tag{2.14}$$

Proof. We simply have

$$\binom{-n}{r} = (-1)^r \frac{n(n+1)\cdots(n+r-1)}{r!} = (-1)^r \binom{n+r-1}{r}. \tag{2.15}$$

■

Theorem 2.9 (The *extended binomial theorem*)**.** *For any $u \in \mathbb{R}$ and positive integer k, we have*

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k. \tag{2.16}$$

.

The extended binomial theorem helps to compute coefficients of generating functions such like $\frac{1}{(1+x)^5}$ or even $\sqrt{1+x}$.

Example 2.10. We compute the coefficient of x^{2026} in the generating function $G(x) = \frac{1}{(1-x)^2(1+x)^2}$. We break down as partial fractions to get

$$\begin{aligned} G(x) = \frac{1}{(1-x)^2(1+x)^2} &= \frac{1}{4}\left(\frac{1}{1-x} + \frac{1}{(1-x)^2} + \frac{1}{1+x} + \frac{1}{(1+x)^2}\right) && (2.17)\\ &= \frac{1}{4}\sum_{k=0}^{\infty}\left((-1)^k\binom{-1}{k} + (-1)^k\binom{-2}{k} + \binom{-1}{k} + \binom{-2}{k}\right)x^k. && (2.18) \end{aligned}$$

The odd terms vanish, so we set k to be even to get the coefficient of x^k as

$$\frac{1}{4}\left(2\binom{-1}{k} + 2\binom{-2}{k}\right) = 1 + \frac{k}{2}. \tag{2.19}$$

Setting $k = 2026$ gives the desired solution of 1014.

2.1.3 Bernoulli Numbers

Definition 2.11. In power series of $\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k\frac{t^k}{k!}$, the coefficients B_k are known as the *Bernoulli numbers*.

Here, B_0 is defined to be 1. One can also recursively define them as $B_0 = 1$ and B_j for $j \geq 1$ such that $\sum_{k=0}^{n}\binom{n+1}{k}B_k = 0$ for $n \geq 1$

One also has a useful formula for the Bernoulli numbers.

Theorem 2.12 (*Faulhaber's formula*)**.** *We have*

$$\sum_{m=1}^{n} m^k = \frac{1}{k+1}\sum_{j=0}^{k}\binom{k+1}{j}B_j n^{k+1-j}. \tag{2.20}$$

Setting $k = 1$, we get

$$1 + 2 + \cdots + n = \frac{1}{2}\left(\binom{2}{0}B_0(n+1)^2 + \binom{2}{1}B_1(n+1)\right) = \frac{1}{2}\left((n+1)^2 - (n+1)\right) = \frac{1}{2}(n+1)n. \tag{2.21}$$

Similarly, one may verify for $k = 2$ or $k = 3$.

Proof. To this end, we use the *Bernoulli polynomials* B_k which are interpreted as coefficients in

$$\frac{te^{xt}}{e^t-1} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!} \tag{2.22}$$

with $B_k(0) = B_k$. We claim that $B_n(x) = \sum_{k=0}^{n}\binom{n}{k}B_k x^{n-k}$. We have

$$\frac{t}{e^t-1}e^{xt} = \left(\sum_{k=0}^{\infty} B_k\frac{t^k}{k!}\right)e^{xt} = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{\infty}\binom{n}{k}B_k x^{n-k}\right)\frac{t^n}{n!}. \tag{2.23}$$

Summing gives us $\dfrac{t(e^{nt}-1)}{(e^t-1)^2}$

$$\begin{aligned} &= \sum_{m=0}^{n-1}\frac{te^{mt}}{e^t-1} = \frac{t}{e^t-1}\sum_{m=0}^{n-1}(1 + mt + m^2\frac{t^2}{2!} + \cdots) = \frac{t}{e^t-1}\left(n + \sum_{m=0}^{n-1} m\frac{t}{1!} + \cdots + \sum_{m=0}^{n-1} m^k\frac{t^k}{k!} + \cdots\right)\\ &\implies \frac{t(e^{nt}-1)}{e^t-1} = \frac{te^{nt}}{e^t-1} - \frac{t}{e^t-1} = \sum_{k=0}^{\infty}(B_n(x) - B_k(0))\frac{t^k}{k!} = t\left(n + (\cdots)\right). && (2.24) \end{aligned}$$

Matching the terms gives us

$$1 + 2^k + \cdots + n^k = \frac{1}{k+1}\left(B_{k+1}(n+1) - B_{k+1}(0)\right) = \frac{1}{k+1}\left(\sum_{j=0}^{k+1} B_j (n+1)^{k-j}\right) - B_{k+1}(0). \tag{2.25}$$

■

2.2 The Pigeonhole Principle

August 12th.

The *pigeonhole principle* simply states that if there are N objects places into k boxes, then some box contains at least $\lceil \frac{N}{k} \rceil$ objects.

Proof. Assume, if possible, that every box has less than $\lceil \frac{N}{k} \rceil$ objects. Then the total number of objects is at most $k \cdot \lceil \frac{N}{k} \rceil$. We take cases.

- Case I, where $k \mid N$. Then $\frac{N}{k}$ is a positive integer, and the total number of objects is less than $k \cdot \frac{N}{k} = N$. This is a contradiction.
- Case II, where $k \nmid N$. Then every box has at most $\lfloor \frac{N}{k} \rfloor$ objects, which is less than $\frac{N}{k}$. Multiplying by k tell us that the total number of objects is less than $k \cdot \frac{N}{k}$ which is, again, a contradiction.

■

Theorem 2.13 (The *Erdös-Szekeres theorem*)**.** *Any sequence of $mn+1$ distinct real numbers either contains an increasing subsequence of length $n+1$ or a decreasing subsequence of length $m+1$.*

Proof. Suppose the sequence of numbers is $a_1, a_2, \ldots, a_{mn+1}$. Assign a pair of numbers (b_i, c_i) to each index i, where b_i is the length of the longest increasing subsequence starting at i and c_i is the length of the longest decreasing subsequence starting at i.

If $b_i \geq n+1$ for some i, or if $c_i \geq m+1$ for some i, we are done. Else, we have $b_i \leq n$ and $c_i \leq m$ for all i. Since both are less than or equal to their respective bounds, the most number of distinct pairs (b_i, c_i) is mn. Thus, by the pigeonhole principle, there exists some $i \neq j$ such that $(b_i, c_i) = (b_j, c_j)$. Without loss of generality, assume $i < j$.

- Case I, where $a_i < a_j$. Then a_i can be (pre)appended to any increasing sequence starting at a_j which is a contradiction since $b_i > b_j$.
- Case II, where $a_i > a_j$. Then a_i can be (pre)appended to any decreasing sequence starting at a_j which is a contradiction since $c_i > c_j$.

■

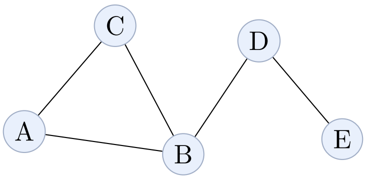
Dirichlet's principle states that in any set of $n+1$ integers, two of them must leave the same remainder modulo n. This is easy to see since there are only n possible remainders (namely $0, 1, \ldots, n-1$) and $n+1$ integers. By the pigeonhole principle, at least two of the integers must fall into the same remainder class.

Chapter 3

GRAPHS

3.1 Introduction

A *graph* is a pair $G = (V, E)$, where V is a set whose elements are called *vertices* and $E \subseteq V \times V$ is a set of unordered pairs $\{v_1, v_2\}$ of vertices, whose elements are called edges. Here, (v_1, v_2) and (v_2, v_1) are undistinguishable, and are simply denoted by $\{v_1, v_2\}$ or $v_1 v_2$.



The above shows a simple undirected graph on five vertices $V = \{A, B, C, D, E\}$ with edges $E = \{AB, AC, BC, BD, DE\}$. Here, simple and undirected are also terms to be defined in the context of graph theory.

Definition 3.1. A graph is called a *simple graph* if it has no loops (edges connecting a vertex to itself) and no multiple edges (more than one edge connecting the same pair of vertices). Otherwise, it is termed a *multigraph*. A graph is called an *undirected graph* if its edges have no orientation; that is, the edge uv is identical to the edge vu. Otherwise, it is termed a *directed graph*.

In directed graphs, or *digraph*s, one deals with $G = (V, E, s, t)$, where $s : E \to V$ gives the *source node* of an edge and $t : E \to V$ gives the *target node* of an edge. In this edge set E, $uv \neq vu$, unlike the case of a simple graph.

Structure-preserving maps are useful in graph theory too.

Definition 3.2. Suppose we have two graphs $G = (V(G), E(G))$ and $H = (V(H), E(H))$. A function $f : V(G) \to V(H)$ is said to be a *graph homomorphism* if f preserves adjacency; that is, if $v_1 v_2 \in E(G)$, then $f(v_1)f(v_2) \in E(H)$. If f is also bijective and f and f^{-1} are both graph homomorphisms, then f is termed a *graph isomorphism*.

We also term the group $\mathrm{Aut}(G)$ as the group of all graph isomorphisms of G, with the group operation of composition.

Definition 3.3. Suppose we have two digraphs $G_1 = (V_1, E_1, s_1, t_1)$ and $G_2 = (V_2, E_2, s_2, t_2)$. A *digraph homomorphism* is two maps $f_V : V_1 \to V_2$ and $f_E : E_1 \to E_2$ such that

$$s_2(f_E(e)) = f_V(s_1(e)) \quad \text{and} \quad t_2(f_E(e)) = f_V(t_1(e)). \tag{3.1}$$

That is, the source node of every image edge is the image node of every source node, and the target node of every image edge is the image node of every target node.

One also discusses the neighbours of nodes.

Definition 3.4. The *degree of a node*, or the *valency of a node*, is simply defined as the number of edges incident with the vertex. If v is such a node in a graph (V, E), then $\deg(v) = \#\{u \in V \mid vu \in E\}$. In digraphs, one defines the *out-degree of a node* v as the number of edges with v as the source node, and the *in-degree of a node* v as the number of edges with v as the target node.

A *regular graph* is one where every vertex has the same degree. We now discuss the first ever theorem (historically) in graph theory.

Theorem 3.5. *A finite (simple) graph G has an even number of vertices of odd degree.*

Proof. Let $G = (V, E)$ be a graph. One can deduce that

$$2 \cdot \#E(G) = \sum_{v \in V(G)} \deg(v). \tag{3.2}$$

Thus, there must be an even number of vertices of odd degree to keep the term on the left even. ■

3.2 Walks, Paths, and Cycles

Definition 3.6. A *walk on a graph G* is an alternating sequence of vertices and edges

$$(v_0, e_1, v_1, e_2, v_2, \dots, e_k, v_k) \tag{3.3}$$

such that for all i, e_i is an edge between v_{i-1} and v_i. The *length of a walk*, in this case, is termed k.

Definition 3.7. If the edges $e_1, e_2, \dots, e_k$ are distinct, then the walk is called a *path on a graph*. A *simple path* is one where the vertices $v_0, v_1, \dots, v_k$ are also all distinct. Finally, a *simple closed path*, or a *cycle on a graph*, is one where $v_0 = v_k$ and the rest are distinct.

A *metric on a graph* between two vertices $d(v_1, v_2)$ is defined as the length of the shortest walk between v_1 and v_2. This walk is always a path since if it's not, there is a repetition of edges, and appropriate middle edges and vertices can be deleted to form a path or a shorter walk. If no such path exists, then $d(v_1, v_2) = \infty$. Thus, a finite *connected graph* G is one where $d(v_1, v_2) < \infty$ for all $v_1, v_2 \in V(G)$.

August 21st.

3.2.1 The Königsberg Bridge Problem

The following figure illustrates the famous problem of the *Königsberg bridge problem*.

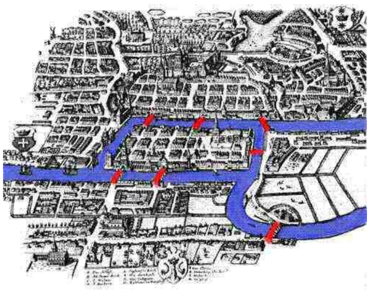


Figure 3.1: The Seven Bridges of Königsberg

Euler asked the question if one could cross each of the seven bridges exactly once and come back to the same side of the riverbank; this is formally considered as the first ever problem in graph theory.

Here, an *Eulerian circuit* is defined, which is a closed path using every edge in the graph exactly once. A graph with an Eulerian circuit is termed an *Eulerian graph*.

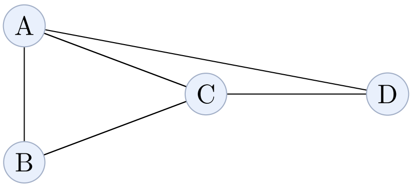


Figure 3.2: Graph Representation of the Seven Bridges of Königsberg

(Above graph to be fixed.)

Theorem 3.8. *A finite multigraph G is Eulerian if and only if G is connected and is a edge-disjoint union of cycle $G = C_1 \cup C_2 \cup \cdots \cup C_m$ where C_i's are cycles with no common edges.*

Proof. Suppose $G = C_1 \cup C_2 \cup \cdots \cup C_m$ where C_i's are edge-disjoint cycles. For $m = 2$, choose $v \in V(C_1) \cap V(C_2)$; such a v must exist or else the graph is disconnected. Starting at v, exhaust all edges in C_1 using the trivial Eulerian circuit and return to v. Do the same with C_2, and you have found the Eulerian circuit. Now apply the induction hypothesis; for an arbitrary m, choose $v \in V(C_1 \cup C_2 \cup \cdots \cup C_{m-1}) \cap V(C_m)$. Again, such a v must exist since G is connected. Starting at v, exhaust all edges in C_1 using the trivial Eulerian circuit and return to v, then use the Eulerian circuit in $C_1 \cup C_2 \cup \cdots \cup C_{m-1}$ formed via the induction hypothesis.

For the converse, an Eulerian circuit on the graph involves all edges and returns to the same vertex, so G must be connected. To show the disjoint union of cycles, find a cycle in the Eulerian circuit; there must exist at least one since, if not, the circuit itself is a cycle. Delete the edges from this cycle, and join the starting vertex and ending vertex in of this cycle in the circuit. Repeat the same until the resulting Eulerian circuit is a cycle. The disjoint union of this cycle and the cycles removed is the starting circuit. ■

One can show a better result.

Theorem 3.9. *A finite multigraph G is Eulerian if and only if G is connected and every vertex has an even degree.*

Proof. If G is Eulerian, then G is connected by the previous theorem, and $G = C_1 \cup C_2 \cup \cdots \cup C_m$, a union of disjoint cycles. Also, for $v \in V(G)$,

$$\deg_G(v) = \sum_{i=1}^{m} \deg_{C_i}(v) = 2\left(\sum_{i=1}^{m} \mathbf{1}_{\{v \in C_i\}}\right). \tag{3.4}$$

Thus, $\deg_G(v)$ is even for all $v \in V(G)$.

For the converse implication, assume G is connected and every vertex has an even degree. We will show that G is Eulerian. Start by choosing any cycle C_1 in G. Remove the edges of C_1 from G to form a subgraph G'. Since every vertex in G has even degree, removing the edges of C_1 leaves every vertex in G' with even degree. If G' is connected, repeat the process to find another cycle C_2 in G'. Continue this process until no edges remain. If G' is disconnected at any step, then each connected component of G' must also have all vertices of even degree. By the same argument, we can find cycles in each connected component and remove their edges. Eventually, all edges of G are partitioned into disjoint cycles. Since G is connected, these cycles can be combined into a single Eulerian circuit by appropriately traversing edges between cycles. Thus, G is Eulerian. ■

3.3 Adjacency

For a simple graph $G = (V, E)$, an *adjacency matrix* can be defined of dimension $\#V \times \#V$, with $a_{v,w} = 1$ if $vw \in E$, and $a_{v,w} = 0$ otherwise. For a multigraph, $a_{v,w}$ is the number of edges between vertices v and w. Similarly, for a directed graph, $a_{v,w} = 1$ if $vw \in E$ and $a_{w,v} = 0$ otherwise. For an undirected graph, the adjacency matrix A is symmetric and consists of only 1's and 0's.

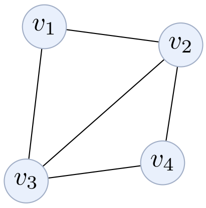


Figure 3.3: A simple graph with four vertices

The adjacency matrix for the graph in Figure 3.3 is given as $A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$. For two graphs G_1 and G_2 to be isomorphic, one can show that $A(G_1)$ must be similar to $A(G_2)$. Moreover, to count the number of walks from v to w of length k, one can use the k-th power of the adjacency matrix: the entry (i, j) of A^k gives the number of walks of length k from vertex v_i to vertex v_j.

August 28th.

Theorem 3.10. *Let $G = (V, E)$ be a simple graph with n vertices $V = \{1, 2, \ldots, n\}$ and adjacency matrix A. Then the $(i, j)^{th}$ entry of A^k gives the number of walks of length k from vertex i to vertex j.*

Proof. $k = 1$ is trivial, as a walk of length 1 is just showing there exists an edge between the two vertices. Let $k = 2$. Then the $(i, j)^{\text{th}}$ entry of A^2 is given as

$$(A^2)_{i,j} = \sum_{m=1}^{n} a_{im} a_{mj} \tag{3.5}$$

where a_{ij} is 1 if i and j are neighbours and zero otherwise. Thus, $a_{im}a_{mj}$ represents if vertex m is an immediate intermediate vertex between i and j. Thus, the number of walks of length 2 from i to j is equal to the number of such intermediate vertices m.

Assume the result holds for an arbitrary k; that is, $(A^k)_{i,j}$ gives the number of walks from i and j of length k. Then, for $k + 1$, we have

$$(A^{k+1})_{i,j} = \sum_{m=1}^{n} (A^k)_{i,m} a_{mj}. \tag{3.6}$$

Any walk from i to j must have a neighbour of j at the k^{th} step. By the induction hypothesis, $(A^k)_{i,m}$ represents the number of walks from i to m of length k. Thus, the total number of walks from i to j of length $k + 1$ is the sum over all possible intermediate vertices m. ■

Theorem 3.11. *Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $A(G)$ where $G = (V, E)$ is a simple graph. Then the number of closed walks of length k is given by $\sum_{i=1}^{n} \lambda_i^k$.*

Proof. The number of such closed walks of length k is, clearly, $\operatorname{tr} A^k$. The eigenvalues of A^k are $\lambda_1^k, \ldots, \lambda_n^k$, and the trace is the sum of all eigenvalues; the result immediately follows. ■

Remark 3.12.

- For $k = 2$, $\frac{1}{2} \operatorname{tr} A^2$ provides the number of edges in the graph.
- For $k = 3$, $\frac{1}{6} \operatorname{tr} A^3$ provides the number of triangles in the graph.

Example 3.13. G is connected if and only if the largest eigenvalue of A has multiplicity 1. This is known as the *Perron-Frobenius theorem* will be taken as granted for now, without providing a proof.

Proposition 3.14. *For any eigenvalue λ of $G = (V, E)$, it holds that $|\lambda| \leq \max_{v \in G} \deg(v)$.*

Proof. Pick a corresponding eigenvector $x \neq 0$ with $Ax = \lambda x$, where A is the adjacency matrix. Pick $x_j = \|x\|_\infty = \max_i |x_i|$. Then we have

$$|\lambda|\,|x_j| = |\lambda x_j| = \left|\sum_{i=1}^{n} A_{ji} x_i\right| \leq \sum_{i=1}^{n} A_{ji}\,|x_i| \leq |x_j| \sum_{i=1}^{n} A_{ji} = |x_j| \deg(j) \implies |\lambda| \leq \deg(j) \leq \max_{v \in G} \deg(v). \tag{3.7}$$

■

Proposition 3.15. *Let spectrum of $G = \{\lambda_1, \ldots, \lambda_n\}$ be the list of eigenvalues where $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Then*

$$\frac{1}{n} \sum_{v \in G} \deg(v) \leq \lambda_n \leq \max_{v \in G} \deg(v). \tag{3.8}$$

Proof. Let $e = (1\ 1\ \cdots\ 1)^t$, and let $d = Ae = (\deg(v_1)\ \deg(v_2)\ \cdots\ \deg(v_n))^t$. Then $e^t Ae = ed = \sum_{v \in G} \deg(v)$. Then $\sup_{\|x\|=1} \langle x, Ax \rangle = \lambda_{\max}(A) \geq \frac{e^t}{\sqrt{n}} A \frac{e}{\sqrt{n}} = \frac{1}{n} \sum_{v \in G} \deg(v)$. The second inequality is just the one above. ■

Theorem 3.16. *A finite multigraph G is Eulerian if and only if G is connected and every vertex has an even degree.*

Proof. If G is Eulerian, then it is connected and every vertex has an even degree by definition. Conversely, suppose G is connected and every vertex has an even degree. Take 'a' longest trail, one where edges are not repeated, starting at $x \in V(G)$. We claim that this trail is actually closed. Let, if possible, the endpoint be $y \neq x$. There must have been an "entering" edge followed by an "exiting" edge. In the last step, one has entered y but never exited it. So, an odd number of edges incident with y appear in this trail. As $\deg(y)$ is even, there must be an unused edge incident with y. If we append that edge to the trail, we have a longer trail, contradicting our assumption.

We make another claim that this trail exhausts all edges. To show this, start by deleting all edges appearing in this trail. Assume that the graph so-obtained has at least one edge. In the trail, T, if a vertex y appears all its incident edges must also appear. Let z be a vertex not appearing on T. Then none of the vertices in T are neighbours of z, showing G not connected which is a contradiction. ■

Hamiltonian Graphs

August 29th.

Definition 3.17. A cycle in $G = (V, E)$ is said to be a *Hamiltonian cycle* if the vertices in the cycle are all distinct, except the starting and ending vertices, and all vertices are exhausted. A simple graph with a Hamiltonian cycle is termed a *Hamiltonian graph*.

Example 3.18.

- Trivially, all polygons with n vertices C_n are Hamiltonian graphs.
- The complete graph K_n is Hamiltonian for all $n \geq 3$.

If $G = (V, E)$ is a graph, then a *subgraph* $H = (V(H), E(H))$ is such that $V(H) \subseteq V(G)$ and $E(H) \subseteq V(H)$ where $E(H)$ are edges connecting vertices in $V(H)$. A *spanning subgraph* is such that $V(H) = V(G)$. We note that G is Hamiltonian if and only if C_n is a spanning subgraph of G.

Our goal now is to find a characterizing condition for Hamiltonian graphs (similar to the characterization of Eulerian graphs), and if a graph is Hamiltonian, then finding the (a) Hamiltonian cycle. The proof of providing a characterization is out of the scope of this course, while the latter problem is NP-hard and not always computationally tactible.

Definition 3.19. The *Hamiltonian closure of a graph G*, denoted by $\mathrm{cl}(G)$, is the graph obtained by repeatedly adding an edge between non-adjacent vertices u, v such that $\deg(u)+\deg(v) \geq n = \#V(G)$.

Proposition 3.20. *With $\#V(G) = n \geq 3$, let G be a simple graph. If $\deg(v) \geq \frac{n}{2}$ for all $v \in V(G)$, then G is Hamiltonian.*

Lemma 3.21. *A graph G is Hamiltonian if and only if $\mathrm{cl}(G)$ is Hamiltonian.*

Proof. If G is Hamiltonian, then clearly $\mathrm{cl}(G)$ is Hamiltonian since adding edges cannot remove Hamiltonian cycles. Conversely, suppose $\mathrm{cl}(G)$ is Hamiltonian. Assume the contrary that there exists G with $\#V(G) = n$ and u an v are *not* neighbours in G with $\deg(u) + \deg(v) \geq n$, but G is not Hamiltonian. $G + uv$ is Hamiltonian, however. Suppose the intermiedate graphs obtained to get the closure are given as

$$G = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_t = \mathrm{cl}(G) \tag{3.9}$$

where $\mathrm{cl}(G)$ is Hamiltonian. Then every Hamiltonian cycle in $G + uv$ must contain the edge uv. Let this Hamiltonian cycle be $(v, v_1, \ldots, v_{n-1}, v_n = u, v_{n+1} = v)$. Let $P = \{v_i \mid 2 \leq i \leq 2 \text{ and } v_1 v_i \in E(G)\}$ and $Q = \{v_i \mid 2 \leq i \leq n \text{ and } v_{i-1} v_n \in E(G)\}$ (P and Q are defined with respect to G and *not* $G + uv$). Then $\#P = \deg(v)$, $\#Q = \deg(v_n)$, and $\#P + \#Q = \deg(u) + \deg(v) \geq n$. Moreover, $P \cup Q \subseteq \{v_2, \ldots, v_n\}$. $P \cap Q$ is non-empty since

$$\#(P \cup Q) = \#P + \#Q - \#(P \cap Q) \geq n - \#(P \cap Q) \implies \#(P \cap Q) \geq n - \#(P \cup Q) \geq 1. \tag{3.10}$$

Thus, there exists some $v_i \in P \cap Q$ with $2 \leq i \leq n$, that is, $v_1 v_i \in E(G)$ and $v_{i-1} v_n \in E(G)$. Then the cycle $(v = v_1, v_i, v_{i+1}, \ldots, v_n = u, v_{i-1}, v_{i-2}, \ldots, v_2, v_1)$ is a Hamiltonian cycle not using the added edge uv—a contradiction. ■

3.4 Bipartite Graphs

A simple graph $G = (V, E)$ is said to be bipartite if there exists a partition of $V(G)$ as $V = V_1 \sqcup V_2$ such that no pairs of vertices in V_1 are edges, and no pairs of vertices in V_2 are edges; that is, there exist $V_1, V_2 \subseteq V$ such that

$$V_1 \cap V_2 = \emptyset,\ V_1 \sqcup V_2 = V,\ E \subseteq V_1 \times V_2. \tag{3.11}$$

Theorem 3.22 (*Kőnig's theorem*)**.** *A graph G is bipartite if and only if it has no odd cycles.*

Index