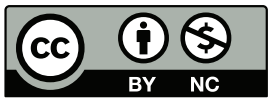
MAT344H1S Introduction to Combinatorics
Lecture Notes

Tianyu Du

April 5, 2019



`Github Page` `https://github.com/TianyuDu/Spikey_UofT_Notes`
`Note Page` `TianyuDu.com/notes`

Contents

1 Strings, Sets, and Binomial Coefficients

1.1 Strings and Sets

Notation 1.1. Let $n \in \mathbb{Z}_{++}$, and we use $[n]$ to denote the n-element set $\{1, 2, \ldots, n\}$.

Definition 1.1. Let X be a set, then an **X-string of length** (or a **word/array**) n is a function $s : [n] \to X$, and X is called the **alphabet** of the string, and each $x \in X$ is called a **character** or letter.

Remark 1.1. An X-string defined by $s : [n] \to X$ with length n can be equivalently defined as a **sequence** consisting elements in X.

$$s(1)s(2)\ldots s(n) \tag{1.1}$$

Definition 1.2. In the case $X = \{0, 1\}$, strings generated from X are called **binary strings**. When $X = \{0, 1, 2\}$, strings are called **ternary strings**.

Definition 1.3. Let X be a *finite* set and let $n \in \mathbb{Z}_{++}$. An X-string $s = x_1x_2\ldots x_n$ is a **permutation** of size m if $x_i \neq x_j \ \forall x_i, x_j \in s$.

Proposition 1.1. If X is an m-element set and $m \geq n \in \mathbb{Z}_{++}$, then the number of X-strings of length n that are permutations is

$$P(m, n) := \frac{m!}{(m-n)!} \tag{1.2}$$

Definition 1.4. Let X be a *finite* set and let $0 \leq k \leq |X|$. Then $S \subseteq X$ with $|S| = k$ is a **combination** of size k.

Proposition 1.2. Let $n, k \in \mathbb{Z}$ such that $0 \leq k \leq n$, then the number of combinations is

$$\binom{n}{k} := \frac{P(n, k)}{n!} = \frac{n!}{k!(n-k)!} \tag{1.3}$$

Proposition 1.3. For all integers n and k with $0 \leq k \leq n$

$$\binom{n}{k} \equiv \binom{n}{n-k} \tag{1.4}$$

Example 1.1. Binomial coefficients can be used to find the number of integer solutions of

$$\sum_{i=1}^{k} x_i \leq N \tag{1.5}$$

given appropriate integers $k, N \in \mathbb{Z}$.

(i) $x_i > 0 \ \forall i \in [k]$ and equality holds, then $C(N-1, k-1)$.

(ii) $x_i \geq 0 \ \forall i \in [k]$ and equality holds, then $C(N+k-1, k-1)$.[1]

(iii) $x_i > 0 \ \forall i \neq j, x_j = Z$ and equality holds, then $C(N-Z-2, k-2)$.

(iv) $x_i > 0 \ \forall i \in [k]$ and strict inequality holds, then $C(N-1, k)$.[2]

(v) $x_i \geq 0 \ \forall i \in [k]$ and strict inequality holds, then $C(N+k-1, k)$.

(vi) $x_i \geq 0 \ \forall i \in [k]$ and *weak* inequality holds, $C(N+k, k)$ [3].

$$\binom{N+k-1}{k-1} + \binom{N+k-1}{k} = \binom{N+k}{k} \tag{1.6}$$

[1] Simulate choosing $x_i + 1$ instead of x_i.
[2] Image there is a placeholder $x_{k+1} > 0$.
[3] This can be calculated by adding case (ii) and case (v) together, and apply Pascal's identity

Remark 1.2. Common tricks on finding the number of integer solutions.

- If $\sum \leq N$, add another variable such that $\sum = N$ with construct $\tilde{x} \geq 0$.
- If $x_i \geq 0$, construct new variable $\tilde{x_i} \geq 1$ and increase N by 1.

Definition 1.5. Define a **plane** as $\mathbb{Z}^2$, then a **lattice path** in the plane is a *sequence* of elements in $\mathbb{Z}^2$

$$((x_i, y_i))_{i=1}^{t} \tag{1.7}$$

such that for every $i \in \{1, \ldots, t-1\}$, either

(i) (*Horizontal move*) $x_{i+1} = x_i + 1 \wedge y_{i+1} = y_i$

(ii) Or (*vertical move*) $x_{i+1} = x_i \wedge y_{i+1} = y_i + 1$

Lemma 1.1. Let $(p, q), (m, n) \in \mathbb{Z}^2$, then the number of lattice paths from (p, q) to (m, n) is

$$\binom{(p-m)+(q-n)}{p-m} \tag{1.8}$$

Proof. The lattice is isomorphic to a H, V-string with length $(p-m)+(q-n)$. There are exactly $p-m$ horizontal moves as well as exactly $q-n$ vertical moves. ■

Theorem 1.1. Given $n \in \mathbb{Z}_+$, the number of lattice paths from $(0, 0)$ to (n, n) which *never go above the diagonal line (could be on the diagonal)* is the **Catalan number**

$$C(n) := \frac{1}{n+1}\binom{2n}{n} \tag{1.9}$$

Proof. Omitted ■

Theorem 1.2 (Binomial Theorem)**.** Let $x, y \in \mathbb{R}$, then $\forall n \in \mathbb{Z}_+$

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i \tag{1.10}$$

Theorem 1.3 (Multinomial Theorem)**.** Let $r \in \mathbb{Z}_+$, $\{x_i\}_{i=1}^{r} \in \mathcal{P}(\mathbb{R})$. Then for every $n \in \mathbb{Z}_+$,

$$(\sum_{i=1}^{r} x_i)^n = \sum_{|\alpha|=n} \binom{n}{\alpha} (x_i)^\alpha \tag{1.11}$$

where $\alpha \equiv (\alpha_i)_{i=1}^{r}$, $\alpha_i \in \mathbb{Z}_{++}$ $\forall i$ is a **multi-index**, and

$$(x_i)^\alpha \equiv \sum_{i=1}^{r} x_i^{\alpha_i} \tag{1.12}$$

$$|\alpha| \equiv \sum_{i=1}^{r} \alpha_i \tag{1.13}$$

$$\binom{n}{\alpha} \equiv \frac{n!}{\alpha_1! \alpha_2! \ldots \alpha_r!} \tag{1.14}$$

2 Induction

Theorem 2.1 (Well-Ordering Principle)**.** Every non-empty set of $\mathbb{Z}_{++}$ has a least element.

Proof. Prove using principle of mathematical induction and contradiction. ■

Definition 2.1. A function $f : \mathbb{Z} \to \mathbb{R}$ is defined **recursively** if $f(n) := F(\{f(i) : i < n\})$ for some function F.

Theorem 2.2 (The Principle of Mathematical Induction)**.** If S is any set of natural numbers with properties that

1. 1 is in S, and
2. $k + 1$ is in S whenever k is any number in S.

then $S = \mathbb{Z}_+$.

Proposition 2.1. Recursive definitions can also be recast as **inductive definitions**(closed form).

Definition 2.2 (Summation)**.** Summation operator beginning with index 1, $\sum : \mathcal{F}_1 \times \mathbb{Z}_{++} \to \mathbb{R}$, where $\mathcal{F}_1$ is the set of unary real-valued functions, is defined inductively as

$$\sum_{i=1}^{1} f(i) \equiv f(1) \tag{2.1}$$

$$\sum_{i=1}^{k+1} f(i) \equiv \sum_{i=1}^{k} f(i) + f(k+1) \tag{2.2}$$

Theorem 2.3 (The Principle of Complete Mathematical Induction)**.** If S is any set of natural numbers with the properties that

1. $1 \in S$, and
2. $\{1, 2, \ldots, k\} \subset S \implies k + 1 \in S$,

then $S = \mathbb{Z}_+$.

3 Pigeon Hole Principle and Complexity

3.1 Pigeon Hole Principle

Theorem 3.1. Let $f : X \to Y$ be a function, then

$$f \text{ injective} \implies |X| \leq |Y| \tag{3.1}$$

Theorem 3.2 (Pigeon Hole Principle)**.** Let $f : X \to Y$, and suppose $|X| > |Y|$, then f is not injective, that's

$$\exists x_1 \neq x_2 \in X \text{ } s.t. \text{ } f(x_1) = f(x_2) \tag{3.2}$$

Proof. Contrapositive form of the theorem 3.1 ■

Theorem 3.3 (Generalized Pigeon Hole Principle)**.** Let $f : X \to Y$ be a mapping such that

$$|X| > (m-1)|Y| \tag{3.3}$$

then there exists $\{x_1, \ldots, x_m\} \subseteq X$ such that $f(x_i) = f(x_j)$ $\forall i, j$.

Proof. For each $y \in Y$, we can divide X into $|Y|$ partitions, where each partition is defined as the pre-image of one particular $y \in Y$. Let $\{X_i\}$ denote the set of partitions.
We are trying to find the minimum value of $\max_i\{|X_i|\}_{i=1}^{|Y|}$, that's

$$\min_{\text{valid partition}} \max_i \{|X_i|\}_{i=1}^{|Y|} \tag{3.4}$$

the minimum is attained when each partition of X has the same cardinality, which is strictly greater than $m-1$.
For each of those partitions, it's a pre-image for some value $y \in Y$ with size at least m. ■

3.2 Complexity

Definition 3.1. Let $f, g : \mathbb{N} \to \mathbb{R}$ be a function, then the **big oh** $\mathcal{O}(f)$ is a collection of functions such that, for every $g \in \mathcal{O}(f)$

$$\exists c \in \mathbb{R}, n^* \in \mathbb{N} \; s.t. \; \forall n \in \mathbb{N}, n \geq n^* \implies g(n) \leq cf(n) \tag{3.5}$$

Definition 3.2. Define $\pi : \mathbb{Z}_{++} \to \mathbb{Z}_+$ as $\pi(n) \equiv$ *the number of primes among the first n positive integers.*

Theorem 3.4 (Prime Number Theorem)**.** $\pi(n)$ grows at a rate the same as $\frac{n}{\ln(n)}$. That's

$$\lim_{n\to\infty} \pi(n)\frac{\ln(n)}{n} = 1 \tag{3.6}$$

4 Graph Theory

4.1 Definitions

Definition 4.1. A graph $\mathcal{G}$ is defined as an order pair of sets (V, E). **Vertex** set V is a set consisting of **vertex** objects. **Edge set** E contains **edges** as pairs of elements in E.

Definition 4.2. A graph $\mathcal{G}$ is called a **simple graph** if it is unweighted, undirected and contains no loop or multiple edges. That's, if $\mathcal{G} \equiv (V, E)$ is a simple graph, then

1. (Undirected) $\forall x, y \in V, \; xy \in E \iff yx \in E$.
2. (No loop) $\forall xy \in E, x \neq y$.
3. (No multiple edge) all elements in E are distinct.
4. Vertices or edges in $\mathcal{G}$ have no weight.

Graphs with multiple edges or loops are called **multi-graphs**.

Remark 4.1. In this course, unless explicitly mentioned, we consider simple graphs only.

Definition 4.3. Let $x, y \in V$, if $xy \in E$, then x and y are **adjacent**, and edge xy is **incident to** vertices x and y. If $xy \notin E$, we say x and y are **non-adjacent**.

Definition 4.4. Let $\mathcal{G} \equiv (V, E)$ and $x \in V$, then the **neighbourhood** of x is defined as

$$\mathcal{N}(x) \equiv \{y \in V : xy \in E\} \tag{4.1}$$

Then the **degree** of x in graph $\mathcal{G}$ is defined as

$$\deg_{\mathcal{G}}(x) \equiv |\mathcal{N}(x)| \tag{4.2}$$

Definition 4.5. Let $\mathcal{G} \equiv (V, E)$ and $\mathcal{H} \equiv (W, F)$, we say $\mathcal{H}$ is a **subgraph** of $\mathcal{G}$ when $W \subseteq V$ and $F \subseteq E$. $\mathcal{H}$ is an **induced subgraph** if

$$F = \{xy \in E : x, y \in W\} \tag{4.3}$$

$\mathcal{H}$ is a **spanning subgraph** if $W = V$.

Definition 4.6. A **clique** is a complete subgraph.

Definition 4.7. $\mathcal{G} \equiv (V, E)$ is a **complete graph** ($\mathbf{K}_n$) if

$$E = \{xy : \text{ distinct pair } x, y \in V\} \tag{4.4}$$

Definition 4.8. A graph $\mathcal{G} \equiv (V, E)$ is a **independent graph** ($\mathbf{I}_n$) if for every distinct pair $(x, y) \subset V$, $xy \notin E$.

Definition 4.9. A **walk** in graph $\mathcal{G} \equiv (V, E)$ is a *sequence of vertices* $(x_1, x_2, \ldots, x_n)$ such that

$$x_i x_{i+1} \in E \ \forall i \in \{1, \ldots, n-1\} \tag{4.5}$$

Definition 4.10. A **path** is a walk with *distinct* vertices. The length of path is defined as the number of edges in it.

Definition 4.11. A **cycle** is a *path* $(x_1, x_2, \ldots, x_n)$ with $n \geq 3$ such that $x_1 x_n \in E$.

Definition 4.12. A **circuit** is a closed *walk*.

	Distinct Vertices	Repeated Vertices
Closed	**Cycle**	**Circuit**
Not Closed	**Path**	**Walk**

Figure 4.1: Definitions

Definition 4.13. Two graphs $\mathcal{G} \equiv (V, E)$ and $\mathcal{H} \equiv (W, F)$ are **isomorphic**, denoted as $\mathcal{G} \cong \mathcal{H}$, if there exists a bijection $f : V \to W$ such that

$$\forall x, y \in V, \ xy \in E \iff f(x)f(y) \in F \tag{4.6}$$

Definition 4.14. A graph $\mathcal{G}$ is **connected** when for every distinct pair $x, y \in V$, there exists a path from x to y. Otherwise, $\mathcal{G}$ is **disconnected**.

Definition 4.15. Provided $\mathcal{G}$ is disconnected, then a **component** of $\mathcal{G}$ is a maximal connect subgraph of $\mathcal{G}$. That's, if $\mathcal{H}$ is a component, it is connected and any super-graph of $\mathcal{H}$ is disconnected.

Definition 4.16. A graph $\mathcal{G}$ is **acyclic** when it does not contain any cycle on three or more vertices.

Definition 4.17. A **forest** is an acyclic graph.

Definition 4.18. A **tree** is a connected acyclic graph.

Theorem 4.1. Let $\mathcal{G} \equiv (V, E)$ be a graph, then

$$\sum_{v \in V} \deg_{\mathcal{G}}(v) = 2|E| \tag{4.7}$$

Corollary 4.1. For any graph, the number of vertices with odd degree is even.

Definition 4.19. Let $\mathcal{T}$ be a tree, a vertex v is a **leaf** if $\deg_{\mathcal{G}}(v) = 1$.

Theorem 4.2. Every tree with $|V| \geq 2$ has at least two leaves.

Proof. Let $\mathcal{T}$ be a tree. The corollary above suggests that it cannot have one leaf. Consider the case it has no leaf, then since every vertex has at least degree of 2 and $\mathcal{T}$ is connected, there must exist a cycle, which leads to a contradiction. ■

4.2 Eulerian Graphs

Definition 4.20. Let $\mathcal{G} \equiv (V, E)$ be a graph, then a sequence of vertices $(v_0, v_1, \dots v_t)$ is an **Eulerian circuit** if (*transverse all edge once*)

(i) $v_0 = v_t$;

(ii) $v_i v_{i+1} \in E \ \forall i \in \{0, \dots, t-1\}$;

(iii) $\forall e \in E, \exists\ !i \in \mathbb{Z}\ s.t.\ v_i v_{i+1} = e$.

That's, it is a graph circuit which uses each graph edge exactly once.

Definition 4.21. A graph is **Eulerian** if it contains an eulerian circuit.

Remark 4.2. Some definitions require Eulerian graph to be connected but some don't, check with the lecture notes.

Theorem 4.3. A graph $\mathcal{G}$ is Eulerian $\iff$ it is 1) connected and 2) every vertex has even degree.(still holds for multi-graph)

4.3 Hamiltonian Graphs

Definition 4.22. Let $\mathcal{G} \equiv (V, E)$ be a graph, then a sequence of vertices $(v_0, v_1, \dots, v_t)$ is a **Hamiltonian cycle** if (*transverse all vertices once*)

1. $v_0 v_t \in E$;
2. $v_i v_{i+1} \in E \ \forall i \in \{0, \dots, t-1\}$;
3. $\forall v \in V, \exists!\ i \in \mathbb{Z}\ s.t.\ v_i = v$.

Definition 4.23. A graph containing Hamiltonian cycle is **Hamiltonian**.

Theorem 4.4. If $\mathcal{G}$ is a graph with n vertices, and $\deg_{\mathcal{G}}(v) \geq \lceil \frac{n}{2} \rceil\ \forall v \in V \implies \mathcal{G}$ is Hamiltonian.

4.4 Graph Colouring

Definition 4.24. Let $\mathcal{G} \equiv (V, E)$, and C is a set of elements called **colours**. Then a **proper colouring** of $\mathcal{G}$ is a function $\phi : V \to C$ such that

$$\forall x, y \in V,\ xy \in E \implies \phi(x) \neq \phi(y) \tag{4.8}$$

Definition 4.25. The least size of C such that we can construct a proper colouring with it is defined as the **chromatic number** of $\mathcal{G}$, denoted as $\chi(\mathcal{G})$.

Definition 4.26. A graph $\mathcal{G} \equiv (V, E)$ with $\chi(\mathcal{G}) \leq k$ is called **k-colourable graph**.

4.5 Bipartite Graph

Definition 4.27. A graph $\mathcal{G} = (V, E)$ is a **bipartite graph** when V can be partitioned into two sets V_1, V_2, such that subgraphs *induced* by V_1 and V_2 are *independent graphs*.

Theorem 4.5. A graph is 2-colourable $\iff$ it's bipartite.

Theorem 4.6. A graph is 2-colourable/bipartite $\iff$ it does *not* contain an odd cycle.

Proof.
($\implies$) Let $\mathcal{G} \equiv (V, E)$ be a 2-clourable graph with proper colouring $\phi : V \to \{\alpha, \beta\}$.
Define $V_1 \equiv \phi^{-1}(\alpha)$ and $V_2 \equiv \phi^{-1}(\beta)$. Clearly those two sets are disjoint and $V = V_1 \cup V_2$.
By definition of proper colouring, for every pair of $x_1, x_2 \in V_1$, $x_1x_2 \notin E$. The same holds for V_2.
Therefore subgraphs of $\mathcal{G}$ induced from V_1 and V_2 are themselves independent, and $\mathcal{G}$ it bipartite.
We've shown the equivalence between bipartite and 2-colourable.
Suppose there's an odd cycle in $\mathcal{G}$, $C = (x_1, x_2, \ldots, x_n)$, where n is odd.
WLOG, assume $x_1 \in V_1$, by nature of bipartite graph, $x_i \in V_2 \iff i$ even. Therefore $x_n \in V_1$, and for C to be a cycle, we require $x_1x_n \in E$, which contradicts the fact that $\mathcal{G}$ is bipartite and 2-colourable.
Modus Tollens
($\impliedby$) Suppose there exists an odd cycle $C = (x_1, x_2, \ldots, x_n)$ in $\mathcal{G}$, it's easy to show, by induction, that for any proper colouring ϕ of $\mathcal{G}$, $|\phi(C)| \geq 3$. This implies $|\phi(V)| \geq 3$, so $\mathcal{G}$ is not 2-colourable.
Modus Tollens ■

4.6 Planar Graphs

Definition 4.28. A **drawing** of a graph is a way of associating its vertices with points in $\mathbb{R}^2$ and its edges with simple polygonal arcs whose endpoints are the coordinates associated to the vertices that are the endpoints of the edge.

Definition 4.29. A **planar drawing** of a graph is on in which arcs corresponding to two edges intersect only at a point corresponding to a vertex to which they are both incident.

Definition 4.30. A graph $\mathcal{G}$ is **planar** if it has a planar drawing.

Definition 4.31. A **face** of a *planar drawing* of a graph is a region bounded by edges and vertices and not containing any other vertices or edges.

Theorem 4.7 (Euler's Formula)**.** Let $\mathcal{G}$ be a *connected planer graph* with V vertices and E edges. Then $\mathcal{G}$ has F faces where

$$V - E + F = 2 \tag{4.9}$$

Theorem 4.8 (Generalization of Euler's Formula)**.** If a graph $\mathcal{G}$ is planar, then

$$V - E + F = 1 + \#\text{ of components} \tag{4.10}$$

Proof. Induction on E.
Base Case $E = 0$, there are 1 face and V components, above formula holds.
Inductive Step Adding one edge either

1. Eliminate one component,
2. Or increase one face.

Suppose the new edge e reduces number of component by 1, it must be the case that it connects two components in the original graph, and there is only one edge between those two components, it's impossible for such single edge to form one extra face. ■

Remark 4.3. The converses of above theorems are not true, the notion of faces is not even well-defined if the graph is not planar.

Theorem 4.9. A planar graph with n vertices has at most $3n - 6$ edges when $n \geq 3$.

Theorem 4.10 (Kuratowski's Theorem)**.** A graph is planar $\iff$ it does not *contain* either $\mathbf{K}_5$ or $\mathbf{K}_{3,3}$.

Definition 4.32. Graph $\mathcal{G}$ **contains** $\mathcal{H}$ means $\mathcal{G}$ has a subgraph that is homeomorphic to $\mathcal{H}$.

Theorem 4.11 (Four Colour Theorem)**.** Every planar graph is 4-colourable.

4.7 Labeled Trees

Theorem 4.12 (Cayley's Formula)**.** The number T_n of labelled tress on n vertices is n^{n-2}.

Definition 4.33. Constructing Prufer code

(i) If $\mathbf{T} \approxeq \mathbf{K}_2$, return empty string and terminate.

(ii) Else, let v be the leaf of $\mathbf{T}$ with the smallest label and let u be its unique neighbour. Let i be the label of u, append i to the code.

Theorem 4.13. Constructing labelled tree from Prufer code $\mathbf{P}$ with length n

(i) There are $n+2$ vertices in total, define $V := [n+2]$.

(ii) Add edge $(\mathbf{P}[0], \min(V \backslash \mathbf{P}))$.

(iii) Drop above added vertices from code and set.

(iv) When $\mathbf{P} = \varnothing$, there should be 2 vertices left in V, add this edge.

5 Inclusion-Exclusion Principle

Theorem 5.1 (Generalized Inclusion-Exclusion Principle)**.** Let $\{S_i\}_{i=1}^N$ be a collection of N sets, then

$$\left|\bigcup_{i=1}^{N} S_i\right| = \sum_{\varnothing \neq J \subseteq [N]} (-1)^{|J|+1} \left|\bigcap_{i \in J} S_i\right| \tag{5.1}$$

where $\bigcap_{i\in J} |S_i|$ represents the number of elements satisfying at least $|J|$ conditions (where each one condition is specified by one S_i).

5.1 Counting Surjections

Theorem 5.2. The number of surjections $f : [n] \to [m]$ can be computed using principle of inclusion-exclusion. Let $S(n, m)$ denote the number of surjections from $[n]$ to $[m]$. We first count the *number of functions that's not surjections.*

$$N(S) = \underbrace{\binom{m}{1}(m-1)^n}_{f \text{ omit at least 1 element}} - \underbrace{\binom{m}{2}(m-2)^n}_{f \text{ omit at least 2 elements}} + \underbrace{\binom{m}{3}(m-3)^n}_{f \text{ omit at least 3 elements}} - \dots \tag{5.2}$$

$$= \sum_{k=1}^{m} (-1)^{k+1} \underbrace{\binom{m}{k}(m-k)^n}_{f \text{ omit at least } k \text{ elements}} \tag{5.3}$$

$$\implies S(n,m) = \underbrace{m^n}_{\text{all } f} - N(S) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n \tag{5.4}$$

6 Derangements and Euler's ϕ

6.1 Derangements

Definition 6.1. Derangements are *bijective* functions $f : [n] \to [n]$ (rearrangements of n integers) such that

$$\forall i \ f(i) \neq i \tag{6.1}$$

and the number of derangements is denoted as d_n.

Theorem 6.1.

$$d_n = \underbrace{n!}_{\text{all } f} - \underbrace{\binom{n}{1}(n-1)!}_{\text{at least 1 } f(i)=i} + \underbrace{\binom{n}{2}(n-2)!}_{\text{at least 2 } f(i)=i} - \underbrace{\binom{n}{3}(n-3)!}_{\text{at least 3 } f(i)=i} + \dots \tag{6.2}$$

$$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \tag{6.3}$$

$$= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \tag{6.4}$$

Theorem 6.2 (Portion of Derangements)**.** Find the percentage of functions from $[n]$ to $[n]$ that are derangements.

$$\frac{d_n}{n!} = \sum_{k=0}^{n} (-1)^k \frac{1}{k!} \tag{6.5}$$

$$\implies \lim_{n\to\infty} \frac{d_n}{n!} = \frac{1}{e} \tag{6.6}$$

By Taylor's sereis $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$

Proposition 6.1.

$$d_n = \begin{cases} n \cdot d_{n-1} - 1 \text{ if } n \text{ is odd} \\ n \cdot d_{n-1} + 1 \text{ if } n \text{ is even} \end{cases} \tag{6.7}$$

Proposition 6.2.

$$d_n = (n-1)(d_{n-1} + d_{n-2}) \tag{6.8}$$

Example 6.1. The number of rearrangement on $[n]$ with *exactly* L elements matched (equivalently, as $n-L$ derangement)

$$|\{i \in [n] : \sigma(i) = i\}| = L \tag{6.9}$$

is

$$\binom{n}{L} d_{n-L} \tag{6.10}$$

6.2 Euler's ϕ

Example 6.2 (Combinatoric Interpretation for ϕ)**.** Draw n points in a circle, connect every pair k apart, for $1 \le k \le n$. Does it make C_n graph.

Theorem 6.3. If k *relatively prime* to n, then above rule of connecting nodes creates a C_n graph. Therefore, $\phi(n)$ essentially captures the number of k's that construct a C_n graph.

Theorem 6.4. Let $n \in \mathbb{N}$, and suppose n can be factorized into primes $p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_m^{k_m} - p_m^{k_m-1})$$

7 Generating Function

Theorem 7.1. Let

$$A(n) := \sum_{n=0}^{\infty} a_n x^n \tag{7.1}$$

$$B(n) := \sum_{n=0}^{\infty} b_n x^n \tag{7.2}$$

$$C(n) := A(n)B(n) \tag{7.3}$$

then

$$c_n = \sum_{k=j}^{n} a_j b_{n-j} \tag{7.4}$$

8 Recurrences

8.1 Solving Recurrence Relations

Definition 8.1. A **linear recurrence relation (LRR) of degree** k is a sequence $\{a_n\}$ such that for every n,

$$\sum_{i=0}^{k} c_i a_{n+i} = g(n),\ c_i \in \mathbb{R},\ c_0, c_k \neq 0 \tag{8.1}$$

Definition 8.2. A linear recurrence relation is said to be **homogenous** if $g(n) = 0$ for every n.

Remark 8.1. A recurrence relation sequence can be extended to both directions, so it can be defined as a function $f : \mathbb{Z} \to \mathbb{R}$ (instead of being only defined on $\mathbb{N}$).

Definition 8.3. The **advancement operator** $A : \mathbb{R}^{\mathbb{Z}} \to \mathbb{R}^{\mathbb{Z}}$ is defined as

$$Af(n) := f(n+1)\ \forall n \in \mathbb{Z} \tag{8.2}$$

Proposition 8.1. In general, a degree k LRR can be expressed using a degree k polynomial on A as

$$P(A)f(n) = g(n) \tag{8.3}$$

Remark 8.2. Procedure to solve for the closed form of a LRR:

(i) Solve for the **general solution**, note that there are infinitely many general solutions upon some *free parameters*.

(ii) Using the given *initial conditions*, we can find exact values of those free parameters and construct **particular solutions**.

8.1.1 Preliminary Case: Distinct Real Roots

Remark 8.3. Given that the roots of $P(A)$ are all distinct and real, for example

$$P(A) = (A - \alpha)(A - \beta) \tag{8.4}$$

then we can solve them separately

$$\begin{cases} (A-\alpha)f_1 = 0 \implies f_1(n) = \alpha^n b_1 \\ (A-\beta)f_2 = 0 \implies f_1(n) = \beta^n b_2 \end{cases} \tag{8.5}$$

Note that any f_1 satisfying $(A - \alpha)f_1 = 0$ automatically satisfies $P(A)f_1 = 0$, and the same holds for f_2. So we can combine the solutions to construct the general solution.

8.1.2 Generalized Case: Real Roots with Multiplicity

Remark 8.4. Let $P(A)$ be a degree k polynomial, let $\{r_i\}$ denote the set of roots of $P(A)$. For those roots with multiplicity one, they contribute exactly one basis

$$b_i r_i^n \tag{8.6}$$

to the general solution.
For those roots with multiplicity higher than one, for example, the multiplicity of r_j is $d > 1$. Then r_j contributes k basis elements

$$\{b_\ell n^\ell r_j^n\}_{\ell=0}^{d-1} \tag{8.7}$$

while constructing the general solution

8.1.3 Complex Roots

Remark 8.5. Generally, the existence of complex roots implies alternating patterns in sequence. And when aggregating basis of general solution together, i would be cancelled out.

9 Probability

Definition 9.1 (Probability Space)**.** A **probability space** is a triple $(\Omega, \mathcal{F}, P)$, where Ω denotes the *sample space*, $\mathcal{F}$ is a σ-algebra representing the *event space*. And $P : \mathcal{F} \to [0, 1]$ is a *probability measure* such that

$$P(\varnothing) = 0, \ P(\Omega) = 1 \tag{9.1}$$

$$P(\cup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} P(E_i) \ \forall \text{ pair-wise disjoint } \{E_i\}_{i=1}^{\infty} \subset \mathcal{F} \tag{9.2}$$

Proposition 9.1. On discrete probability space, the probability measure $P : \mathcal{F} \to [0, 1]$ can be induced from $p : \Omega \to [0, 1]$.

Assumption 9.1. In this course, while we are constructing the probability space, we always assume

$$\mathcal{F} := \mathcal{P}(\Omega) \tag{9.3}$$

Definition 9.2. Given probability space $(\Omega, \mathcal{F}, P)$, two events $E_1, E_2 \in \mathcal{F}$ are **independent** if and only if

$$P(E_1 \cap E_2) = P(E_1)P(E_2) \tag{9.4}$$

Proposition 9.2. Let $E_1, E_2 \in \mathcal{F}$ such that $E_1, E_2 \neq \varnothing$ and $E_1 \cap E_2 = \varnothing$, then $E_1 \not\perp E_2$.

Proof. Note $0 = P(E_1 \cap E_2) = P(E_1)P(E_2) \neq 0$. ■

Mutually exclusive non-empty events cannot be independent.

Definition 9.3. A **Bernoulli Trial** is a sequence of *independent and identical experiments* with two outcomes.

Definition 9.4. Conditional probability of event $F \in \mathcal{P}(\Omega)$ conditioned on event E is defined as

$$P(F|E) := \frac{P(F \cap E)}{P(E)} \tag{9.5}$$

Theorem 9.1 (Bayes' Theorem)**.**

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{9.6}$$

Definition 9.5. A **random variable** X on probability space is defined as a function $X : \Omega \to \mathbb{R}$.

Definition 9.6. The **expected value** of a random variable X defined on discrete probability space is defined as

$$\mathbb{E}[X] := \sum_{\omega \in \Omega} P(\{\omega\})X(\omega) \tag{9.7}$$

Proposition 9.3. Expectation operator is linear.

Proposition 9.4 (Binary/Indicator Random Variable)**.**

$$\mathbb{1}(\mathcal{P}(\Omega)) = \{0, 1\} \tag{9.8}$$

$$\mathbb{E}[\mathbb{1}] = P(\mathbb{1} = 1) \tag{9.9}$$

Definition 9.7. A game is **fair** if the money wined/lost from this game has expected value zero.

References

Keller, M. T., & Trotter, W. T. (2017). *Applied combinatorics*: Mitchel T. Keller, William T. Trotter. https://www.rellek.net/appcomb