MAT 344 Lecture Notes

Tianyu Du

February 20, 2019

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 $\{1, 2, \dots, n\}$.

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.

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

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 $s = x_1 x_2 \dots x_n$ 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

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

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

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

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

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

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 $C(N-Z+k-2, k-2)$.

(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

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 $i \in \{1, \dots, t-1\}$, 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* is the **Catalan number**

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

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

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

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

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

2 Induction

Theorem 2.1 (Well-Ordering Principle)**.** Every non-empty set of Z_{++} has a least element.

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

Definition 2.1. Recursive definition

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

Remark 2.1. **Recursive definitions** can also be recast as **inductive definitions**.

Definition 2.2 (Summation)**.** Summation operator beginning with index 1, $\sum : \mathcal{F}_1 \times Z_{++} \to \mathbb{R}$, 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

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

Proof. Contrapositive form of the theorem 3.1 ∎

Theorem 3.3 (Erods/Szekeres)**.** Let $m, n \in \mathbb{Z}_+$, then any sequence of $mn+1$ *distinct* real numbers either

(i) has an increasing subsequence of $m+1$ terms,

(ii) or it has a decreasing subsequence of $n+1$ terms.

Proof. Let $\sigma = (x_1, x_2, \ldots, x_{mn+1})$ be a sequence with length $mn+1$ consisting of distinct reals.
For each $i \in [mn+1]$ define a_i as the maximum length of an increasing subsequence of σ *beginning with* x_i.
Define b_i as the maximum length of a decreasing subsequence of σ *ending with* x_i.
Case (i)

$$\exists i \in [mn+1] \; s.t. \; a_i \geq m+1 \lor b_i \geq n+1 \tag{3.3}$$

then the theorem is proven.
Case (ii) Suppose otherwise

$$\forall i \in [mn+1] \; a_i \leq m \land b_i \leq n \tag{3.4}$$

construct function $f : [mn+1] \to [m] \times [n]$ defined as

$$f(i) \equiv (a_i, b_i) \tag{3.5}$$

Note that $|[mn+1]| > |[m] \times [n]|$ so f cannot be injective, so there exists $j \neq k \in [mn+1]$ such that $(a_j, b_j) = (a_k, b_k)$.
WLOG, assume $j < k$.
Since all elements in σ are distinct, $j \neq k \implies x_j \neq x_k$.
Sub-case (i) $x_j < x_k$, then any increasing subsequence beginning with x_k can be extended by prepending x_j, so $a_j > a_k$.
Sub-case (ii) $x_j > x_k$, then any decreasing subsequence ending with x_j can be extended by appending x_k, so $b_k > b_j$.
Either sub-case leads to a contradiction, so **case (ii)** is impossible. ■

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 $g \in \mathcal{O}(f)$

$$\exists c \in \mathbb{R}, n^* \in \mathbb{N} \ s.t. \ \forall n \in \mathbb{N}, n \geq n^* \implies g(n) \leq cf(n) \tag{3.6}$$

Definition 3.2. Let $f, g : \mathbb{N} \to \mathbb{R}$ be a function. If $f(n) > 0 \ \forall n \in \mathbb{N}$, then the **little oh** $o(f)$ is the collection of functions such that, for every $g \in o(f)$,

$$\lim_{n \to \infty} \frac{g(n)}{f(n)} = 0 \tag{3.7}$$

Definition 3.3. Let $f, g : \mathbb{N} \to \mathbb{R}$, then the **little oh**, $o(f)$ is defined as the collection of functions such that $g \in o(f)$ if and only if

$$\exists c \in \mathbb{R}, n^* \in \mathbb{N}, \ s.t. \ \forall n \in \mathbb{N}, n \geq n^* \implies |g(n)| < c|f(n)| \tag{3.8}$$

Definition 3.4. 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

$$\lim_{n \to \infty} \pi(n) \frac{\ln(n)}{n} = 1 \tag{3.9}$$

Definition 3.5. The class of **polynomial time** problems, denoted as $\mathcal{P}$, is the set of decision problems for which there exists one polynomial run time algorithm as the solution.

Definition 3.6. The class of **nondeterministic polynomial time** problems, denoted as $\mathcal{NP}$, is the set of decision problems for which there is a certificate for a yes answer whose correctness can be verified in polynomial time.