Combinatorial Analysis

Raymond Bian

January 19, 2024

Contents

Lecture 1: Syllabus and Review

1 Introduction

This course is basically just a second course in Combinatorics, and will cover a range of topics.

Definition 1. **Matroids** are the structures that capture whether or not the greedy algorithm works. They will be covered later in the course.

Now, for some examples and review:

Definition 2. We say points are in **convex position** if no point is inside a triangle made by 3 other points.

Example. Given a finite set of points on the plane, what is the maxmimum number of points such that no 3 are on a line, and no 4 are in convex position.

Proof. Informally, we know that the "outside" of our points has at most 3 points in the shape of a triangle. We can then place a point in the middle. However, if we try to add another point, then we find that 4 points are in convex position, which is a contradiction. Therefore, 4 points is the maximum size of such a set.

This example is actually part of a more general problem, shown below.

Theorem 1. (ES, 1935) The maxmimum number of points such that no 3 are on a line and no n are in convex position is $\leq 4^n$ and $\geq 2^{n-2}$.

Theorem 2. (Suk, 2017) This number is actually $\leq 2^{n+o(1)}$

Notation. Think of $o(1)$ as standing for a function $f(n)$ such that $\lim_{n\to\infty} f(n) = 0$. In other words, for every $\varepsilon > 0$, there exists n_0 such that $|f(n)| < \varepsilon$ for every $n \geq n_0$.

Example. How many distinct 5-letter words are there on the 26-letter english alphabet?

Proof. There are 26 options for each of the 5 slots, so there are 26^5 words.

Example. What if repetitions aren't allowed?

Proof. Each slot you lose an option, so there are $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = \frac{26!}{21!}$ words.

Example. How many ways are there to choose 5 students out of 35 to present?

Proof. There are $\binom{35}{5} = \frac{35!}{5! \cdot 30!}$ ways.

Lecture 2: Review of Proofs

We will now review the types of proofs covered in Math-3012, as well as guidelines for writing them in this class.

Notation. If F is a mapping from N to M, we write $F : N \to M$.

Notation. Sometimes, $N \backslash \{a\}$ will be instead written as $N - \{a\}$.

Proposition 1. Let N be an n-element set and M be an m-element set. Then, there are m^n mappings (or functions) from N to M.

Proof. (Inductive) We go by induction on n.

Base case.: For the base case $n = 0$, we consider the empty set $\varnothing$ to be a mapping from the empty set to M. So $m^0 = 1$ and the base case holds.

Inductive step.: Now, let $n \geq 1$ and assume that the proposition holds for $n-1$ by induction. So, let $a \in N$. There are m^{n-1} mappings $F' : N \backslash \{a\} \to M$. For each such F', we have m choices for where to send a. These mappings are all distinct, and every $F : N \to M$ can be obtained in this way. So, the number of mappings $F : N \to M$ is $m^{n-1} \cdot m = m^n$, as desired.

$\square$

Definition 3. A **bijection** is a function $f : X \to Y$ such that f is one-to-one and onto.

Corollary. An n-element set X has 2^n many subsets.

Proof. (Bijective) For each $A \subseteq X$, let $F_A : X \to \{0, 1\}$ such that for each $x \in X$,

$$F_A(x) = \begin{cases} 0 & \text{if } x \notin A \\ 1 & \text{if } x \in A \end{cases}.$$

These mappings $F_A, F_{A'}$ are distinct for distinct subsets $A, A' \subseteq X$, and every mapping $F : X \to \{0, 1\}$ is equal to F_A for some $A \subseteq X$. So by proposition 1, the corollary holds. $\square$

Lemma 1. For any non-negative integers n, k ($n, k \in Z_{\geq 0}$), we have $\binom{n}{k} = \binom{n}{n-k}$.

Proof. (Algebraic) We have

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(n-(n-k))!(n-k)!} \\ &= \binom{n}{n-k}, \end{aligned}$$

as desired. $\square$

Theorem 3. (Binomial Theorem) Let $n \in \mathbb{Z}_{\geq 0}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof. Consider

$$\underbrace{(x+y)(x+y)\dots(x+y)}_{n \text{ times}}.$$

For each $(x+y)$ term, we select either the x or the y, and there are $\binom{n}{k}$ ways to select k x's and $n-k$ y's. The formula follows. $\square$

Corollary. For any $n \in \mathbb{Z}_{\geq 0}$, we have

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \text{ and } 0 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k.$$

Proof. Apply the binomial theorem with $x = y = 1$ to yield the first result, and with $x = -1, y = 1$ to yield the second. $\square$

1.1 Counting Review

Definition 4. A **permutation** is a bijection from a finite set to itself.

Example. One such bijection could be $1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 5, 5 \mapsto 3$.

Lemma 2. The number of such bijections is $n!$.

Proof. Exercise to the student! $\square$

Lecture 3: Permutations and Cycles

Notation. $\tau : X \to X$ is a permutation **on** X. Can also be denoted by $\sigma : X \to X$.

We will show that all permutations τ can be "decomposed" into "cycles".

Example. From the example earlier, $(1, 2)$ is a cycle, and $(3, 4, 5)$ is another cycle.

For the following, let $\tau : X \to X$.

Definition 5. A **cycle** of τ is a tuple (ordered set of elements) $(x_1, x_2, \dots, x_k)$ such that $x_1, x_2, \dots, x_k$ are distinct elements of X, and $\tau(x_1) = x_2, \tau(x_2) = x_3, \dots, \tau(x_{k-1}) = x_k, \tau(x_k) = x_1$. We call $x_1, x_2, \dots x_k$ the **elements** of the cycle.

Lemma 3. If $(x_1, x_2 \dots, x_k)$ and $(y_1, y_2, \dots y_r)$ have an element in common, then $\{x_1, x_2, \dots x_k\} = \{y_1, y_2, \dots y_r\}$.

Proof. Note that since $(x_1, x_2, \dots, x_k)$ is a cycle, $(x_2, x_3, \dots, x_k, x_1)$ is also a cycle. Because of this, we can assume that $x_1 = y_1$. So

$x_2 = \tau(x_1) = \tau(y_1) = y_2$. Then, we have that $x_2 = y_2$. We can repeat this process until $x_k = y_k$ (swap x, y if $k > r$). Then, we have $x_1 = \tau(x_k) = \tau(y_k) = y_1$, which means that $r = k$. Therefore, all cycles are pairwise disjoint. $\square$

Lemma 4. For every $x \in X$, there exists a cycle of τ which has x as an element.

Proof. Consider visiting each element $x, \tau(x), \tau(\tau(x)), \ldots,$ until the first time we re-visit any element. This will eventually happen, because X is finite. Then, let's suppoose that we have visited elements $x_1, x_2, \ldots x_k$ so far, such that $x_1, x_2, \ldots, x_k$ are distinct, and that $\tau(x_k) = x_i$ for some $i \in \{1, 2, \ldots, k\}$. We cannot have $i \geq 2$ because then both x_{i-1} and x_k would both map to x_i, which is a contradiction because a permutation is a bijection. Therefore, $i = 1$ and we have established our cycle. $\square$

Corollary. There exists cycles $C_1, C_2, \ldots, C_t$, so that every element of X is an element in exactly one such cycle.

Definition 6. The **cycle notation** for τ is written as

$$\tau = C_1 C_2 \ldots C_t.$$

Example. Find the cycle notation for the permutation τ of $\{1, 2, 3, 4, 5, 6\}$ where

$$\begin{aligned} \tau(1) &= 4 \\ \tau(2) &= 6 \\ \tau(3) &= 2 \\ \tau(4) &= 5 \\ \tau(5) &= 1 \\ \tau(6) &= 3. \end{aligned}$$

Proof. By inspection, we have a cycle $(1, 4, 5)$ and another cycle $(2, 3, 6)$. Therefore, $\tau = (1, 4, 5)(2, 3, 6)$.

Definition 7. A **transposition** is a cycle with exactly two elements.

Problem. How quickly does $n!$ grow as n gets large?

Lecture 4: Estimates for $n!$

Lemma 5. (Simplest) For any positive integer $n \in \mathbb{Z}_{>0}$,

$$2^{n-1} \leq n! \leq n^{n-1}.$$

Proof. We have for the lower bound

$$n! = \prod_{i=2}^{n} i \geq \prod_{i=2}^{n} 2 = 2^{n-1}.$$

And for the upper bound,

$$n! = \prod_{i=2}^{n} i \leq \prod_{i=2}^{n} n = n^{n-1}.$$

$\square$

Note that these bounds are very far off. Here is a motivating example.

Example. Suppose n students draw a card from a deck of n cards, replacing the card afterwards. What is the likelihood that all n cards drawn are distinct?

Proof. The probability is the number of desireable outcomes over the total number of outcomes. This is just

$$\frac{n!}{n^n}.$$

Note that if we use the upper bound from this lemma, we would get that the probability is at most $\frac{1}{n}$. In reality however, the true probability is much, much smaller.

Lemma 6. A better set of bounds are the following:

$$\left(\frac{n}{2}\right)^{\frac{n}{2}} \leq n! \leq \frac{(n+1)^n}{2^{\frac{n}{2}}}.$$

Proof. Left as an exercise! $\square$

Lemma 7. For any two $a, b \geq 2$, we have $a \cdot b \geq a + b$.

Lemma 8. (Arithmetic-Geometric Mean Inequality) For any two $a, b \geq 0$, we have

$$\sqrt{ab} \leq \frac{a+b}{2}.$$

With these last two lemmas, we can show the following:

Theorem 4. (Gauss) For any $n \in \mathbb{Z}_{>0}$,

$$n^{\frac{n}{2}} \le n! \le \frac{(n+1)^n}{2^n}.$$

Proof. We instead look at $(n!)^2$. Pairing 1 with n, 2 with $n-1$, etc, we have for the lower bound

$$\begin{aligned} n! &= \left(\prod_{i=1}^{n} i\right)\left(\prod_{i=1}^{n} i\right) \\ &= \prod_{i=1}^{n} i(n+1-i) \\ &= \prod_{i=1}^{n} \sqrt{i(n+1-i)} \\ &\ge \prod_{i=1}^{n} \sqrt{n} && \text{(Lemma 7)} \\ &\ge n^{\frac{n}{2}}. \end{aligned}$$

And for the upper bound, we have

$$\begin{aligned} n! &= \left(\prod_{i=1}^{n} i\right)\left(\prod_{i=1}^{n} i\right) \\ &= \prod_{i=1}^{n} i(n+1-i) \\ &= \prod_{i=1}^{n} \sqrt{i(n+1-i)} \\ &\le \prod_{i=1}^{n} \frac{i+n+1-i}{2} \\ &= \frac{(n+1)^n}{2^n}. \end{aligned}$$

□

Theorem 5. (Even better bound) For any $n \in \mathbb{Z}_{>0}$, we have

$$e\left(\frac{n}{e}\right)^n \le n! \le en\left(\frac{n}{e}\right)^n.$$

Proof. The lower bound will be given as a homework problem. The upper bound is as follows. Note that $\ln(n!) = \sum_{i=1}^{n} \ln(i)$. Then, we can take the integral of $\ln(x)$, which is greater than this sum.

$$\begin{aligned} \sum_{i=1}^{n} \ln(i) &\le \int_{1}^{n+1} \ln(x)dx \\ &= (n+1)\ln(n+1) - n. \end{aligned}$$

Thus

$$\begin{aligned} n! &\le e^{(n+1)\ln(n+1)-n} \\ &= \frac{e^{(n+1)\ln(n+1)}}{e^n} \\ &= \frac{\left(e^{\ln(n+1)}\right)^{n+1}}{e^n} \\ &= \frac{(n+1)^{n+1}}{e^n}. \end{aligned}$$

Applying this for $n(n-1)!$ gives the bound. □

Lecture 5: Asymptotic Analysis

Theorem 6. Stirling's Formula says that

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Definition 8. For two functions $f, g : \mathbb{Z}_{>0} \to \mathbb{R}$, we write $f \sim g$ and say f is asymptotic to g if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

Also note that $f \sim g \Leftrightarrow g \sim f$.

Example. $2n + \sqrt{n} \sim 2n$.

Proof. This is because

$$\lim_{n\to\infty} \frac{2n+\sqrt{n}}{2n} = 1.$$

Example. (Informal) How many digits are in 100!?

Proof. Using Stirling's Formula, we have that

$$100! \sim \sqrt{2\pi 100}\left(\frac{100}{e}\right)^{100} = 9.324\ldots \times 10^{157}.$$

, whereas $100! = 9.332\ldots \times 10^{157}$ (very close approximation).

Definition 9. The n-th harmonic number

$$H_n = \sum_{i=1}^{n} \frac{1}{i}.$$

Theorem 7. (Euler-Mascheroni) $H_n \sim \ln(n)$.

Proof. Omitted. □

Lemma 9. For any positive integer $n \in \mathbb{Z}_{>0}$, we have

$$\frac{\lfloor \log_2(n) \rfloor}{2} \le H_n \le \lfloor \log_2(n) \rfloor + 1.$$

Proof. We can break up the proof into parts of size $2, 4, 8, 16 \ldots$. Let $S_k = \{i \in \mathbb{Z}_{>0} : 2^{k-1} \le i \le 2^k - 1\}$ for any $k \in \mathbb{Z}_{>0}$. Note that $|S_k| = 2^{k-1}$. Also, for every $x \in S_k$, we have

$$\frac{1}{2^k} < \frac{1}{x} \le \frac{1}{2^{k-1}}.$$

Therefore, we have

$$\begin{aligned}
H_n = \sum_{i=1}^{n} \frac{1}{i} &= \sum_{k=1}^{\lfloor \log_2(n) \rfloor} \sum_{x \in S_k} \frac{1}{x} \\
&\ge \sum_{k=1}^{\lfloor \log_2(n) \rfloor} \sum_{x \in S_k} \frac{1}{2^k} \\
&= \sum_{k=1}^{\lfloor \log_2(n) \rfloor} 2^{k-1}/2^k \\
&= \sum_{k=1}^{\lfloor \log_2 n \rfloor} \frac{1}{2} \\
&= \frac{\lfloor \log_2(n) \rfloor}{2}.
\end{aligned}$$

In the other direction, we have

$$\begin{aligned}
H_n &\le \sum_{k=1}^{\lfloor \log_2(n) \rfloor + 1} \sum_{x \in S_k} \frac{1}{x} \\
&\le \sum_{k=1}^{\lfloor \log_2(n) \rfloor + 1} \frac{|S_k|}{2^{k-1}} \\
&= \lfloor \log_2(n) \rfloor + 1.
\end{aligned}$$

□

Definition 10. Let $f, g : \mathbb{Z}_{>0} \to \mathbb{R}$. We say $f = O(g)$ or f is big-O of g if there exists n_0, C, such that

$$|f(n)| \le C \cdot g(n) \quad \forall n \ge n_0.$$

Note. If $f, g : \mathbb{Z}_{>0} \to \mathbb{R}$ and $f \sim g$, we have

$$f = O(g) \quad \text{and} \quad g = O(f).$$

If $\varepsilon = 1$ for all significantly large n, $\frac{f(n)}{g(n)} \le 2$.

Example. $\sum_{i=1}^{n} \frac{1}{i} = O(\log n)$.

Lemma 10. Let $a, \alpha, \beta > 0$ be fixed. Then as $n \to \infty$,

- $n^\alpha = O(n^\beta)$ if $\alpha < \beta$.
- $n^\alpha = O(a^n)$ if $a > 1$.
- $(\ln(n))^\alpha = O(n^\beta)$.