Ve203 Discrete Mathematics

Runze Cai

University of Michigan - Shanghai Jiao Tong University
Joint Institute

Spring 2022

JOINT INSTITUTE
交大密西根学院

Part IV

Counting and Algorithms

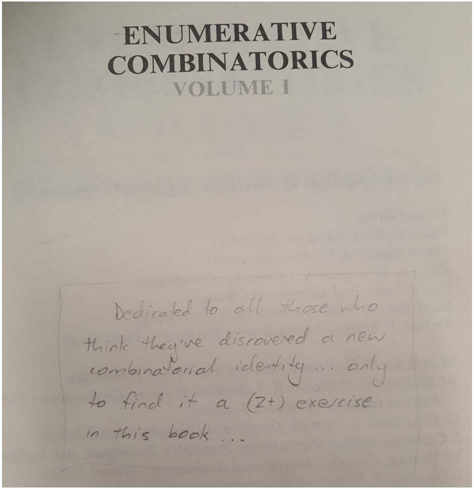
Table of Contents

Overview

- The On-Line Encyclopedia of Integer Sequences® (OEIS®)

  `https://oeis.org/`

- ***Enumerative Combinatorics*** by Richard P. Stanley



Twelvefold Way

Distribute k balls into n urns. $(f : B \to U,\ |B| = k,\ |U| = n)$

Balls (domain)	Urns (codomain)	unrestricted (any function)	≤ 1 (injective)	≥ 1 (surjective)
labeled	labeled	n^k	$n^{\underline{k}}$	$n!\left\{ {k \atop n} \right\}$
unlabeled	labeled	$\left(\!\binom{n}{k}\!\right)$	$\binom{n}{k}$	$\left(\!\binom{n}{k-n}\!\right)$
labeled	unlabeled	$\sum_{i=1}^{n} \left\{ {k \atop i} \right\}$	$[k \leq n]$	$\left\{ {k \atop n} \right\}$
unlabeled	unlabeled	$\sum_{i=1}^{n} p_i(k)$	$[k \leq n]$	$p_n(k)$

- $n^{\underline{k}} = (n)_k = P(n, k) = P_k^n$
- $\binom{n}{k} = C(n, k) = C_k^n$
- $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$
- $\left\{ {k \atop n} \right\} = \#$ partition of $[k]$ into n parts.
- $p_n(k) = \#$ partition of k into n parts.
- $[k \leq n]$: Iverson bracket

Physics Digression

Maxwell-Boltzmann statistics (applicable to no known particles)

- k distinguishable particles, n distinguishable cells.
- Different arrangements with equal probability $1/n^k$.

Bose-Einstein statistics (bosons, e.g., photons, nuclei, atoms, spin-1 particles)

- k indistinguishable particles, n distinguishable cells.
- Different arrangements with equal probability $1/\left(\!\binom{n}{k}\!\right)$.

Fermi-Dirac statistics (fermions, e.g., electrons, neutrons, protons, spin-$\frac{1}{2}$ particles)

- k indistinguishable particles, n distinguishable cells.
- No two or more particles can be in the same cell.
- Different arrangements with equal probability $1/\binom{n}{k}$.

Permutations

k-permutation of n

Number of ways of arranging k elements from a set of size n (order matters) is given by

$$n^{\underline{k}} = P(n,k) = P_k^n = \frac{n!}{(n-k)!}$$
$$= \underbrace{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}_{k \text{ terms}}$$

which is obviously an integer. Note: $0! = 1$.

Combinations

Definition

The number of ways to choose k elements from a set of n (order does NOT matter) is denoted

$$C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{P(n,k)}{k!} = \frac{n^{\underline{k}}}{k!}$$

Reads "n choose k".

Basic Properties

- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{1} = n$

Combinations

Why is $\binom{n}{k}$ an integer?

Method I: Counting Prime Factors.

Note that $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, it is sufficient to show that all factors of the denominator are cancelled by factors in the numerator. Let $\mu_p(x)$ be the the number of the prime factor p in x. According to Legendre's theorem, for $N \in \mathbb{N}$, we have

$$\mu_p(N!) = \sum_{k \geq 1} \left\lfloor \frac{N}{p^k} \right\rfloor$$

We want to show that $\mu_p(n!) \geq \mu_p(k!) + \mu_p((n-k)!)$ for all $p \in \mathbb{P}$. Indeed,

$$\mu_p(n!) - \mu_p(k!) - \mu_p((n-k)!) = \sum_{k \geq 1} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{k}{p^k} \right\rfloor - \left\lfloor \frac{n-k}{p^k} \right\rfloor \right)$$

The rest follows by noticing that for $x, y \in \mathbb{R}$, either $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$, or $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1$. $\square$

Combinations

Method II: Using Lagrange's Theorem.

Consider the symmetric group $G = S_n$, then $|G| = n!$. Next consider the subgroup $H \leq G$ given by

$$H := \left\{ f \in S_n \;\middle|\; \begin{array}{c} f(\{1, \ldots, k\}) = \{1, \ldots, k\} \\ f(\{k+1, \ldots, n\}) = \{k+1, \ldots, n\} \end{array} \right\}$$

then $H \cong S_k \times S_{n-k}$, and $|H| = k!(n-k)!$. It follows by Lagrange's theorem that $|H|$ divides $|G|$. $\square$

Method III: Using Induction.

The induction procedure follows by the recursive identity

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \qquad \square$$

Recursive Identity for Binomial Coefficients

Theorem

For all $n > 0$ and $0 < k < n$, $k, n \in \mathbb{N}$, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Lattice Paths

1	5	15	35	70
1	4	10	20	35
1	3	6	10	15
1	2	3	4	5
1	1	1	1	1

Pascal Triangle

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

$$\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5}$$

Recursive Identity for Binomial Coefficients

$$\sum_{k=0}^{n}\binom{r+k}{k} = \binom{r}{0} + \binom{r+1}{1} + \cdots + \binom{r+n}{n} = \binom{r+n+1}{n}$$

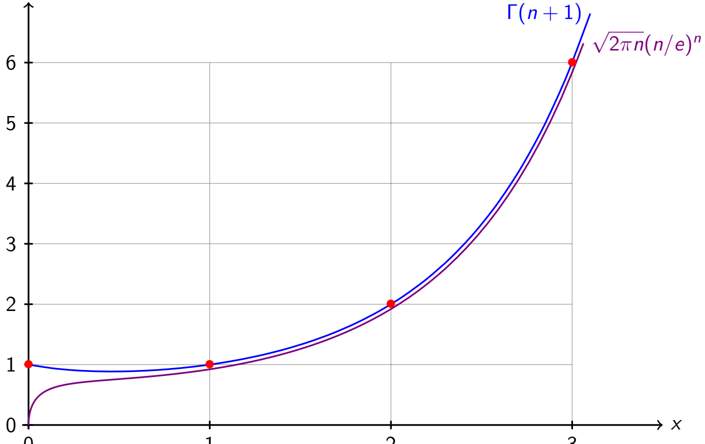
$$\begin{array}{ccccccccccccccccccccc}
&&&&&&&&&& \binom{0}{0} \\
&&&&&&&& \binom{1}{0} &&&& \binom{1}{1} \\
&&&&&&&&& \backslash \\
&&&&&& \binom{2}{0} &&&& \binom{2}{1} &&&& \binom{2}{2} \\
&&&&&&&&&&& \backslash \\
&&&& \binom{3}{0} &&&& \binom{3}{1} &&&& \binom{3}{2} &&&& \binom{3}{3} \\
&&&&& \backslash &&&&&& / &&&& / \\
&& \binom{4}{0} &&&& \binom{4}{1} &&&& \binom{4}{2} &&&& \binom{4}{3} &&&& \binom{4}{4} \\
&&&&& / &&&&&&&&&& \backslash \\
\binom{5}{0} &&&& \binom{5}{1} &&&& \binom{5}{2} &&&& \binom{5}{3} &&&& \binom{5}{4} &&&& \binom{5}{5}
\end{array}$$

Stirling Approximation

How to calculate $\binom{n}{k}$ if n, k are really large?

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

It works extremely good even for small integers.

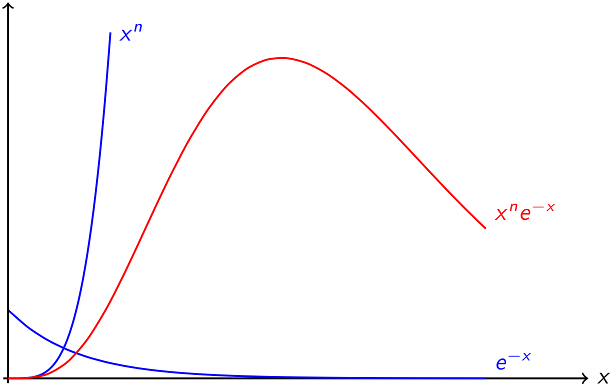


Stirling Approximation

The continuous version of the factorial is given by the Gamma function

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t}\, dt$$

we can approximate the integrand using a bell-shaped curve (Gaussian normal distribution).



Stirling Approximation

Consider the Gamma integral representation of factorial, then

$$n! = \int_0^\infty x^n e^{-x}\, dx = \int_0^\infty e^{-(x-n\ln x)}\, dx$$

Let the exponent be $f(x) \coloneqq x - n\ln x$, which we will approximate using a quadratic function. This is also known as Laplace's method. Since

$$f'(x) = 1 - \frac{n}{x} = 0 \Rightarrow x = n \qquad \text{and} \qquad f''(x) = \frac{n}{x^2}\bigg|_{x=n} = \frac{1}{n}$$

thus $-f$ attains minimum at $x = n$, thus by Taylor expansion, approximately near $x = n$,

$$f(x) \sim n - n\ln n + \frac{1}{2n}(x-n)^2$$

therefore

$$\begin{aligned}\int_0^\infty e^{-(x-n\ln x)}\, dx &\sim \int_0^\infty e^{-(n-n\ln n)} e^{-(x-n)^2/(2n)}\, dx \\ &\sim e^{-(n-n\ln n)} \int_{\mathbb{R}} e^{-(x-n)^2/(2n)}\, dx = n^n e^{-n}\sqrt{2\pi n}\end{aligned}$$

Stirling Approximation

By stirling approximation, we have

$$\binom{n}{k} \sim \sqrt{\frac{n}{2\pi k(n-k)}} \cdot \frac{n^n}{k^k(n-k)^{n-k}}$$

In particular, $\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}}$.

Example

Consider flipping $2n$ fair coins, what is the probability that exactly half are heads and the other half are tails?

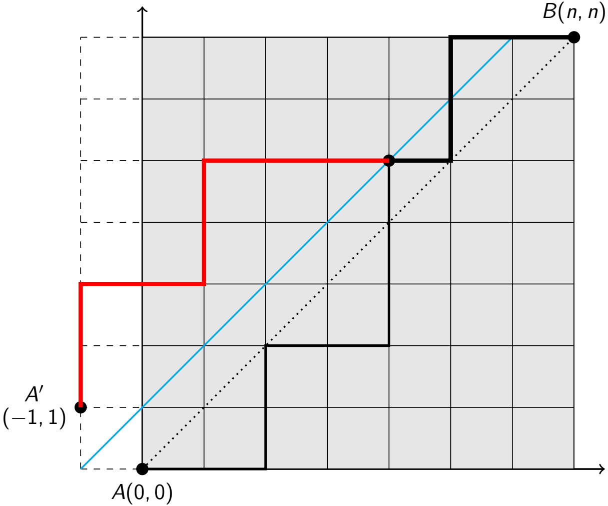
Let X be a random variable following a binomial distribution, i.e., $X \sim \text{Binomial}(2n, \frac{1}{2})$, then

$$\Pr(X = n) = \binom{2n}{n}\left(\frac{1}{2}\right)^n\left(\frac{1}{2}\right)^n \sim \frac{1}{\sqrt{\pi n}}$$

If $2n = 100$, then probability is approximately $\frac{1}{\sqrt{50\pi}} = \frac{1}{5\sqrt{2\pi}} \approx 0.08$. Note that $\sqrt{2\pi} \approx e \approx 2.5$, (recall $1! \sim \sqrt{2\pi \cdot 1}(1/e)^1$).

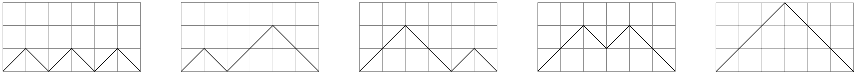
Catalan Numbers

How many lattice paths from $(0, 0)$ to (n, n) that never go above the diagonal? $C_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$.

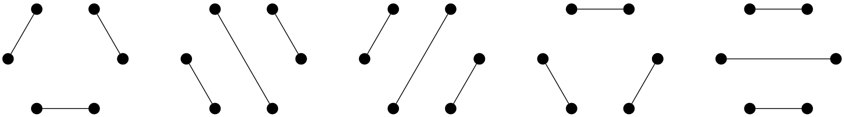


Catalan Numbers

Mountain Range/Dyck Paths



Noncrossing Handshakes

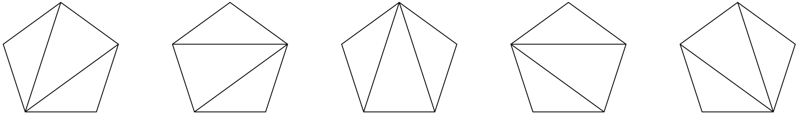


Paired Parentheses

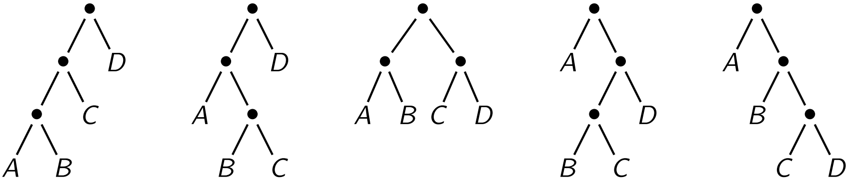
- ()()()
- (())()
- ()(())
- (()())
- ((()))

Catalan Numbers

Polygon Triangulation



Full Binary Trees



Matrix Chain Multiplication

- $((AB)C)D$
- $(A(BC))D$
- $(AB)(CD)$
- $A((BC)D)$
- $A(B(CD))$

Catalan Numbers

Segner's recurrence relation

We can establish the following recurrence relation starting with $C_0 = 1$, and

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k} \text{ for } n \geq 0,$$

We recognize the RHS is a convolution. Now consider the following generating function

$$c(x) \coloneqq \sum_{n=0}^{\infty} C_n x^n$$

then $c(x) = 1 + xc(x)^2$, and

$$c(x) = \frac{1 \pm \sqrt{1-4x}}{2x} = \frac{1 \pm (1 - 2x - 2x^2 + \cdots)}{2x}$$

We want the solution to be a (formal) power series, take the minus sign.

Catalan Numbers

Segner's recurrence relation (Cont.)

Note that

$$c(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

which we expand as

$$\begin{aligned}
c(x) &= \frac{1}{2x}(1 - \sqrt{1-4x}) = \frac{1}{2x} \cdot 2 \sum_{n=1}^{\infty} \frac{(-1)^n}{4^n} \binom{2n-2}{n-1} \frac{(-4x)^n}{n} \\
&= \sum_{n=1}^{\infty} \binom{2n-2}{n-1} \frac{x^{n-1}}{n} \\
&= \sum_{n=0}^{\infty} \binom{2n}{n} \frac{x^n}{n+1} = \sum_{n=0}^{\infty} C_n x^n.
\end{aligned}$$

Top 10 Binomial Coefficient Identities

factorial expansion	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$	integers, $n \geq k \geq 0$.
symmetry	$\binom{n}{k} = \binom{n}{n-k}$	integer $n \geq 0$, integer k.
absorption/extraction	$\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1}$	integer $k \neq 0$.
addition/induction	$\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}$	integer k.
upper negation	$\binom{r}{k} = (-1)^k\binom{k-r-1}{k}$	integer k.

Top 10 Binomial Coefficient Identities (Cont.)

trinomial revision	$\binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}$	integers m, k.
binomial theorem	$\sum_k \binom{r}{k} x^k y^{r-k} = (x+y)^r$	integers $r \geq 0$, or $\lvert x/y \rvert < 1$.
parallel summation	$\sum_{k \leq n} \binom{r+k}{k} = \binom{r+n+1}{n}$	integer n.
upper summation	$\sum_{0 \leq k \leq n} \binom{k}{m} = \binom{n+1}{m+1}$	integers $m, n \geq 0$.
Vandermonde convolution	$\sum_k \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}$	integer n.

Sperner's Theorem

Theorem

The width of the poset $(2^{[n]}, \subset)$, *aka subset/boolean lattice, is* $\binom{n}{\lfloor n/2 \rfloor}$.

Proof (Lubell-Meshalkin-Yamamoto, aka LYM).

First of all, note that as k ranges over 0 to n, the binomial coefficients $\binom{n}{k}$ increase until the middle then decrease by symmetry (recall rows of Pascal's triangle). For example, if n is odd, then

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\frac{n-1}{2}} = \binom{n}{\frac{n+1}{2}} > \cdots > \binom{n}{n-1} > \binom{n}{n}$$

If n is even, then

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\frac{n}{2}} > \cdots > \binom{n}{n-1} > \binom{n}{n}$$

Note that $\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$.

Sperner's Theorem

Proof (Cont.)

We count the number of maximal chains. Note that

- The total number of maximal chain is $n!$.
- If $S \subset [n]$ with $|S| = k$, then the number of maximal chains containing S is $k!(n-k)!$.

Let $\{A_1, A_2, \ldots, A_w\}$ be a maximum antichain. Note that a maximal chain cannot contain A_i and A_j with $i \neq j$, thus

$$\sum_{i=1}^{w} |A_i|!(n - |A_i|!) \leq n!$$

that is

$$\sum_{i=1}^{w} \frac{|A_i|!(n - |A_i|!)}{n!} \leq 1$$

Sperner's Theorem

Proof (Cont.)

which is

$$\sum_{i=1}^{w} \frac{1}{\binom{n}{|A_i|}} \leq 1$$

but $\binom{n}{|A_i|} \leq \binom{n}{\lfloor n/2 \rfloor}$ for all $i \in \{1, \ldots, w\}$, thus we have $w / \binom{n}{\lfloor n/2 \rfloor} \leq 1$, so $w \leq \binom{n}{\lfloor n/2 \rfloor}$. Lastly, note that this upper bound can be achieved by the antichain formed by subset of size $\binom{n}{\lfloor n/2 \rfloor}$ (in the middle). $\square$

Multinomial Coefficients

Multinomial Coefficients

For all $n, m, k_1, \ldots, k_m \in \mathbb{N}$, with $k_1 + \cdots + k_m = n$ and $m \geq 2$, we have the ***multinomial coefficients***

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!k_2!\cdots k_m!} = \frac{\left(\sum_{i=1}^{m} k_i\right)!}{\prod_{i=1}^{k} k_i!}$$

which counts the number of ways of splitting a set of n elements into an ordered sequence of m disjoint subsets. Relating to binomial coefficients

$$\binom{n}{k_1, k_2, \ldots, k_m} = \binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3}\cdots\binom{n-\sum_{i=1}^{m-1} k_i}{k_m}$$

Example

Count distinct permutations of the word MISSISSIPPI.

$$\frac{11!}{1!4!4!2!}$$

Multinomial Formula

Theorem (Gallier, Prop. 4.10, p.216-7)

For all $m, n \in \mathbb{N}$ with $m \geq 2$, for all pairwise commuting variables $a_1, \ldots, a_m$, we have

$$(a_1 + \cdots + a_m)^n = \sum_{\substack{k_1, \ldots, k_m \geq 0 \\ k_1 + \cdots + k_m = n}} \binom{n}{k_1, k_2, \ldots, k_m} a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$$

Question: How many terms occur on the RHS of the multinomial formula?

Table of Contents

Notation

Definition

Let $\left(\!\binom{n}{k}\!\right)$ be the number of k-element multisets on an n-element set. Reads "n multichoose k".

Remark

If $k > n \geq 0$, $n, k \in \mathbb{N}$

- $\binom{n}{k} = 0$. (pigeionhole principle.)
- $\left(\!\binom{n}{k}\!\right) \neq 0$.

Remark

$\left(\!\binom{n}{k}\!\right)$ counts the ways to select k objects from a set of n elements, where order is not important, but repetition is allowed.

Counting Multisets

Proposition

The number of k-element multisets on an n-element set is

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Proof by double counting.

- Definition.
- We want to divide k identical ***stars*** by $n-1$ ***bars***. We arrange everything in $n+k-1$ posititions. Choose k positions for the stars, and the rest for bars, or vice versa. $\square$

Example: 10-element multisets from a 4-element set

$\star$	$\star$	$\star$	$\vert$	$\star$	$\star$	$\vert$	$\vert$	$\star$	$\star$	$\star$	$\star$	$\star$
1	2	3	4	5	6	7	8	9	10	11	12	13

A Multisets Identity

Theorem

Given $n, k \geq 1$, $n, k \in \mathbb{N}$,

$$\left(\!\!\binom{n}{k}\!\!\right) = \left(\!\!\binom{k+1}{n-1}\!\!\right)$$

Proof by double counting.

- Number of ways to arrange k stars and $n-1$ bars.
- Number of ways to arrange $n-1$ stars and k bars.

The above two maps to each other by switching bars and stars. $\square$

$\star$	$\star$	$\star$	$\mid$	$\star$	$\star$	$\mid$	$\mid$	$\star$	$\star$	$\star$	$\star$	$\star$
$\mid$	$\mid$	$\mid$	$\star$	$\mid$	$\mid$	$\star$	$\star$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$

What Multiset Counts

Example

The quantity $\left(\!\binom{n}{k}\!\right)$ counts,

- the number of ways to put k identical balls into urns $B_1, \ldots, B_n$.
- the number of ways to distribute k candy bars to n people.
- the number of ways to buy k drinks from a vending machine with n varieties.
- The number of nonnegative integer solutions to $x_1 + x_2 + \cdots + x_n = k$.
- The number of positive integer sequences $a_1, a_2, ..., a_k$ where $1 \leq a_1 \leq a_2 \leq \cdots \leq a_k \leq n$.

Counting Integer Solutions

Example

Consider

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \leq 538$$

What are the number of integer solutions if

1. $x_i > 0$ and $=$ holds;
2. $x_i \geq 0$ and $=$ holds;
3. $x_i > 0$ and $<$ holds;
4. $x_i \geq 0$ and $<$ holds;
5. $x_i \geq 0$.

Remark

- $x_i > 0 \Rightarrow x_i \geq 1$.

Counting Integer Solutions

Example

How many nonnegative integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 63$$

such that $x_1, x_2 \geq 0$, $2 \leq x_3 \leq 5$, $x_4 > 0$.
Consider the following solution sets, where $A \supset B$. Answer: $|A| - |B|$.

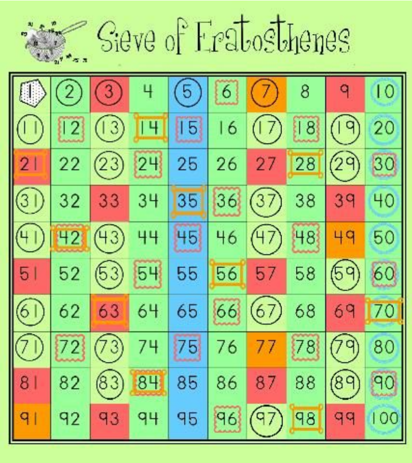
- A: such that $x_1, x_2 \geq 0$, $x_3 \geq 2$, $x_4 > 0$, i.e., $x_3 - 2 \geq 0$, $x_4 - 1 \geq 0$, and
$$x_1 + x_2 + (x_3 - 2) + (x_4 - 1) = 60$$
We have $|A| = \binom{60+3}{3}$.
- B: such that $x_1, x_2 \geq 0$, $x_3 > 5$, $x_4 > 0$, i.e., $x_3 - 6 \geq 0$, $x_4 - 1 \geq 0$, and
$$x_1 + x_2 + (x_3 - 6) + (x_4 - 1) = 56$$
We have $|B| = \binom{56+3}{3}$.

Table of Contents

Inclusion-Exclusion Principle

Example

- 2 sets: $|A \cup B| = |A| + |B| - |A \cap B|$
- 3 sets: $|A \cup B \cup C| = |A| + |B| + |C|$
  $$- |A \cap B| - |B \cap C| - |C \cap A|$$
  $$+ |A \cap B \cap C|$$



Applications

- Sieve of Eratosthenes
- Euler's totient function
- ...

Inclusion-Exclusion Principle

Notation

Given $I \subset \{1, \ldots, n\}$, we let

$$A_I := \bigcap_{i \in I} A_i,$$

where $A_i \subset X$ for all $i \in I$. For example, $A_{\{1,2,4\}} = A_1 \cap A_2 \cap A_4$. In particular, $A_\varnothing = X$.

Theorem (Inclusion-Exclusion Principle)

Let $A_1, \ldots, A_n$ be subsets of X. Then the number of elements of X which lie in none of the subsets A_i is

$$\sum_{I \subset \{1,\ldots,n\}} (-1)^{|I|} |A_I|$$

Inclusion-Exclusion Principle

Proof (Not by induction).

Re-wirte the sum as

$$\sum_{I\subset[n]}(-1)^{|I|}|A_I| = \sum_{I\subset[n]}\sum_{x\in A_I}(-1)^{|I|} = \sum_{x\in X}\sum_{I:x\in A_I}(-1)^{|I|}$$

- If $x \in X - \cup_{i=1}^{n} A_i$, then $J = \{i \in [n] \mid x \in A_i\} = \varnothing$. Since x is fixed, thus $\sum_{I\subset J}(-1)^{|I|} = \sum_{I=\varnothing}(-1)^0 = 1$.
- Otherwise, the set $J = \{i \in [n] \mid x \in A_i\} \neq \varnothing$. Note that $x \in A_I$ iff $I \subset J$, thus

$$\sum_{I\subset J}(-1)^{|I|} = \sum_{i=0}^{|J|}\binom{|J|}{i}(-1)^i = (1-1)^{|J|} = 0$$

Sum the terms and we are done. □

Inclusion-Exclusion Principle

Corollary

Let $A_1, \ldots, A_n$ be a sequence of (not necessarily distinct) sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\varnothing \neq I \subset \{1,\ldots,n\}} (-1)^{|I|+1} |A_I|.$$

Proof.

Take the complement of both sides of previous therem within the set $X = A_\varnothing$, that is,

$$\begin{aligned} |A_1 \cup \cdots \cup A_n| &= |A_\varnothing| - \sum_{I \subset \{1,\ldots,n\}} (-1)^{|I|+1} |A_I| \\ &= \sum_{\varnothing \neq I \subset \{1,\ldots,n\}} (-1)^{|I|+1} |A_I| \end{aligned}$$

□

Inclusion-Exclusion Principle

Special Case

The formula is a lot simpler when

$$|I| = |J| \Rightarrow |A_I| = |A_J|,$$

that is, $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$ depends only on k, where $I = \{i_1, i_2, \ldots, i_k\}$.
Now the formula becomes

$$|A_1 \cup \cdots \cup A_n| = \sum_{|I|=1}^{n} (-1)^{|I|+1} \binom{n}{|I|} |A_I|$$

Derangement

Definition

A permutation $\sigma \in S_n$ over the set $\{1, 2, \ldots, n\}$ is called a derangement if $\sigma(i) \neq i$ for all $i = 1, \ldots, n$.

Theorem

The number of derangements of the set $\{1, 2, \ldots, n\}$ *is given by*

$$d_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)! = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$$

Proof.

Take $A_i := \{\sigma \in S_n \mid \sigma(i) = i\}$, thus $|A_i| = (n-1)!$. Note that for general set $I \subset \{1, 2, \ldots, n\}$, $|A_I| = (n - |I|)!$. The rest follows by inclusion-exclusion principle and

$$\binom{n}{i}(n-i)! = \frac{n!}{i!(n-i)!}(n-i)! = \frac{n!}{i!}$$

□

Derangement

Asymptotics

Assume that each $\sigma \in S_n$ happens equally likely, what is the probability that σ is a derangement?
Note that $|S_n| = n!$, thus

$$\lim_{n\to\infty} \frac{d_n}{n!} = \lim_{n\to\infty} \sum_{i=0}^{n} \frac{(-1)^i}{i!} = e^{-1} = \frac{1}{e} \approx \frac{1}{3}$$

Counting Surjections

Theorem

Let $k \geq n$. The number of surjections $f : \{1, \ldots, k\} \to \{1, \ldots, n\}$ is given by

$$S_{k,n} = \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} (n-i)^k$$

Proof.

Take $A_i = \{f \mid f(j) \neq i \text{ for all } j\} = \{f \mid i \notin \operatorname{im} f\}$. $\square$

Counting Surjections

Example

What is $S_{5,3} = |\{f : \{1,2,3,4,5\} \to \{1,2,3\} \mid f \text{ surjective}\}|$?

Method I.

$$S_{5,3} = \binom{3}{0}(3-0)^5 - \binom{3}{1}(3-1)^5 + \binom{3}{2}(3-2)^5 - \underbrace{\binom{3}{3}(3-3)^5}_{=0} \qquad \square$$

Method II.

We first calculate that

$$\left\{ {5 \atop 3} \right\} = \binom{5}{3} + 3\binom{5}{4} = 25$$

thus $S_{5,3} = 3!\left\{ {5 \atop 3} \right\} = 150$. $\square$

Dimension of Vector Spaces

Given finite dimensional vector spaces U, V, and W, are the following identities correct?

- $\dim(U + V) = \dim U + \dim V - \dim(U \cap V)$.
- $$\begin{aligned}\dim(U + V + W) \\ &= \dim U + \dim V + \dim W \\ &\quad - \dim(U \cap V) - \dim(U \cap W) - \dim(V \cap W) \\ &\quad + \dim(U \cap V \cap W).\end{aligned}$$

Table of Contents

Overview

- Study a way to describe the growth of functions in the limit — asymptotic efficiency
- Focus on what's important (leading factor) by abstracting lower-order terms and constant factors
- Indicate running times of algorithms
- A way to compare "sizes" of functions

$$O \approx \leq$$
$$\Omega \approx \geq$$
$$\Theta \approx =$$

In addition,

$$o \approx <$$
$$\omega \approx >$$

Big "Oh" Notation

Definition

A function $g(n)$ is an ***asymptotic upper bound*** for $f(n)$, denoted by

$$f(n) = O(g(n))$$

if there exist positive constants c and n_0 such that

$$0 \leq f(n) \leq cg(n) \text{ for all } n \geq n_0$$

i.e.,

$$\limsup_{n \to \infty} \frac{f(n)}{g(n)} < \infty$$

Example

Show that $2n + 10 = O(n^2)$.
Proof 1. Since $2n + 10 \leq n^2$ for $n \geq 5$, we can choose $c = 1$ and $n_0 = 5$.
Proof 2. Observe that $2n + 10 \leq 2n^2 + 10n^2 = 12n^2$ for $n \geq 1$, we can choose $c = 12$ and $n_0 = 1$.

Big "Oh" Notation

- $O(g(n))$ is a ***set*** of functions

  $$O(g(n)) = \{f(n) \mid \exists c, n_0 > 0 \text{ s.t. } 0 \leq f(n) \leq cg(n) \text{ for } n \geq n_0\}$$

  We write $f(n) = O(g(n))$ or $f(n) \in O(g(n))$.
- Examples of functions in $O(n^2)$:
  - $n^2 + n$
  - $n^2 + 1000n$
  - $1000n^2 + 1000n$
  - $n/1000$
  - $n^2/\lg n$

Ω Notation

Definition

A function $g(n)$ is an ***asymptotic lower bound*** for $f(n)$, denoted by

$$f(n) = \Omega(g(n))$$

if there exist positive constants c and n_0 such that

$$0 \leq cg(n) \leq f(n) \text{ for all } n \geq n_0$$

i.e.,

$$\liminf_{n\to\infty} \frac{f(n)}{g(n)} > 0$$

Example

$\sqrt{n} = \Omega(\lg n)$. We can choose $c = 1$ and $n_0 = 16$.

Ω Notation

- $\Omega(g(n))$ is a ***set*** of functions

$$\Omega(g(n)) = \{f(n) \mid \exists c, n_0 > 0 \text{ s.t. } 0 \leq cg(n) \leq f(n) \text{ for } n \geq n_0\}$$

- Examples of functions in $O(n^2)$:
  - n^2
  - $n^2 + n$
  - $n^2 - n$
  - $1000n^2 + 1000n$
  - $1000n^2 - 1000n$
  - $n^{2+\varepsilon}$, $\varepsilon > 0$
  - $n^2 \lg n$
  - n^3

Θ Notation

Definition

A function $g(n)$ is an ***asymptotic tight bound*** for $f(n)$, denoted by

$$f(n) = \Theta(g(n))$$

if there exist constants c_1, c_2, and n_0 such that

$$0 \le c_1 g(n) \le f(n) \le c_2 g(n) \text{ for all } n \ge n_0$$

Example

- $\frac{1}{2}n^2 - 2n = \Theta(n^2)$. We can choose $c_1 = \frac{1}{4}$, $c_2 = \frac{1}{2}$, and $n_0 = 8$.
- If $p(n) = \sum_{i=1}^{d} a_i n^i$ and $a_d > 0$, then $p(n) = \Theta(n^d)$.

Θ Notation

- $\Theta(g(n))$ is a ***set*** of functions

$$\Theta(g(n))$$
$$= \{f(n) \mid \exists c_1, c_2, n_0 \text{ s.t. } 0 \leq c_1 g(n) \leq f(n) \leq c_1 g(n) \text{ for } n \geq n_0\}$$

- Examples of functions in $O(n^2)$:
  - n^2
  - $n^2 + n$
  - $n^2 - n$
  - $1000n^2 + 1000n$
  - $1000n^2 - 1000n$

Theorem
$\Theta(g(n)) = O(g(n)) \cap \Omega(g(n))$.

Asymptotic Notation

Example

The function grows faster as the list goes:

- $\log^* n$
- $\log\log\log n$
- $\log\log n$
- $\log n$
- $\sqrt{n}$
- n
- $n\log n$
- $n^{3/2}$
- n^2
- n^3
- $n^{\log\log n}$
- $n^{\log n}$
- 2^n
- $(\log n)^n$
- $n^{n/2}$
- n^n
- 2^{2^n}
- $2^{2^{2^n}}$

Notation

The iterated logarithm, “log star”, is given by

$$\log^* n := \begin{cases} 0, & n \leq 1 \\ 1 + \log^*(\log n), & n > 1 \end{cases}$$

which is well defined if base is $> e^{1/e} \approx 1.444667$. We use $\lg^*$ for binary iterated logarithm.

Using Limits for Comparing Orders of Growth

Let

$$L := \lim_{n\to\infty} \frac{f(n)}{g(n)}$$

We have serval possibilities (given that f and g nonnegative.)

- If $L = 0$, then $f(n) = O(g(n))$;
- If $L = \infty$, then $f(n) = \Omega(g(n))$;
- If $0 < L < \infty$, then $f(n) = \Theta(g(n))$;
- Limit does not exsit: inconclusive.

L'Hôpital's rule

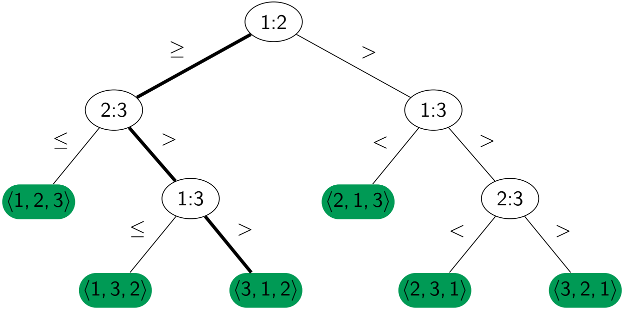
Let f and g be differentiable. If $\lim_{x\to\infty}|f(x)| = \lim_{x\to\infty}|g(x)| = \infty$, and $\lim_{x\to\infty} g'(x) \neq 0$, then

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = \lim_{x\to\infty} \frac{f'(x)}{g'(x)}$$

provided that the limit on the RHS exsits in $\overline{\mathbb{R}}$.

Lower Bound for Sorting

In a ***comparison sort***, we use only comparisons between elements to gain order information about an input sequence $\langle a_1, a_2, \ldots, a_n \rangle$, and the output is given by permutation of the input as $\langle a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)} \rangle$, $\sigma \in S_n$.



Because any correct sorting algorithm must be able to produce each permutation of its input, each of the $n!$ permutations on n elements must appear as one of the leaves of the decision tree for a comparison sort to be correct.

Lower Bound for Sorting

Theorem

Given n elements, any comparison sort algorithm requires $\Omega(n \lg n)$ *comparisons in the worst case.*

Proof.

It suffices to determine the height of a decision tree in which each permutation appears as a reachable leaf. Consider a decision tree of height h with ℓ reachable leaves. Because each of the $n!$ permutations of the input appears as some leaf, we have $n! < \ell$. Since a binary tree of height h has no more than 2^h leaves, we have

$$n! \leq \ell \leq 2^h$$

Take the logarithms, we have

$$h \geq \lg(n!) = \Omega(n \lg n)$$

where the last equality follows from Stirling's approximation formula. □

Table of Contents

Solving Recurrences

Example

$T(n) = 4T(n/2) + n$, which means

$$T(n) = \begin{cases} \Theta(1), & n = 1 \text{ (usually omit this part)} \\ 4(T/2) + n, & n > 1 \end{cases}$$

General Methods

- Substitution Method (guess, say, by trial and error, and prove, say, by induction).
- Recursion-tree Method.
- Master Method.

Solving Recurrences

Example (Factorial)

Let $T(n)$ denote the worst-case running time of **`fact`**, then

$$T(1) = d$$
$$T(n) = T(n-1) + c$$

where c is a constant denoting the work of the comparison–conditional–multiplication–return, and d is a constant denoting the work of the comparison–conditional–return.

```
Function fact(n):
    if n = 1 then
        return 1
    else
        return n · fact(n − 1)
    end
end
```

Solving Recurrences

Example (Merge Sort)

Let $T(n)$ denote the worst-case running time of Merge Sort on an input array containing n elements. Then, for a constant c, we have:

$$T(1) = c$$
$$T(n) = T(\lfloor \tfrac{n}{2} \rfloor) + T(\lceil \tfrac{n}{2} \rceil) + cn$$

which is a typical ***"divide-conquer-combine"*** process.

```
Function mergeSort(A[1 ... n]):
    if n = 1 then
        return A
    else
        L ← mergeSort(1 ... ⌊n/2⌋)
        R ← mergeSort(⌊n/2⌋+1 ... n)
        return merge(L, R)
    end
end
```

Solving Recurrences

Example

Solve $T(n) = 4T(n/2) + n$.

It is sufficient to consider $n = 2^m$, $m \in \mathbb{N}$. Thus $n/2 = 2^{m-1}$, and $m = \log_2 n = \lg n$. Now we have $T(2^m) = 4T(2^{m-1}) + 2^m$. Let $\widetilde{T}(m) := T(2^m)$, then

$$\widetilde{T}(m) = 4\widetilde{T}(m-1) + 2^m$$

whose general solution is given by

$$\widetilde{T}(m) = c \cdot 4^m + d \cdot 2^m, \qquad c, d \text{ constants}$$

thus

$$\begin{aligned} T(n) &= c \cdot 4^{\log_2 n} + d \cdot 2^{\log_2 n} = c \cdot n^{\log_2 4} + d \cdot n^{\log_2 2} \\ &= c \cdot n^2 + d \cdot n = \Theta(n^2) \end{aligned}$$

Master Theorem/Method

Theorem (Master Thoerem, cf., Corman, Leiserson, Rivest, & Stein.)

If $T(n) = aT(n/b) + f(n)$ (for constants $a \geq 1$, $b > 1$, $d \geq 0$), then

1. $T(n) = \Theta(n^{\log_b a})$ *if* $f(n) = O(n^{\log_b a - \varepsilon})$ *for some constant* $\varepsilon > 0$.
2. $T(n) = \Theta(n^{\log_b a} \lg n)$ *if* $f(n) = \Theta(n^{\log_b a})$.
3. $T(n) = \Theta(f(n))$, *if* $f(n) = \Omega(n^{\log_b a + \varepsilon})$ *for some constant* $\varepsilon > 0$, *and if* $af(n/b) \leq cf(n)$ *for some constant* $c < 1$ *and all sufficiently large* n *(regularity condition)*.

Master Theorem/Method

Remark

1. $n^{\log_b a}$ is polynomially larger than $f(n)$, e.g.,

$$T(n) = 7 \cdot T(n/2) + \Theta(n^2)$$

2. $n^{\log_b a}$ and $f(n)$ are on the same order, e.g.,

$$T(n) = 2 \cdot T(n/2) + \Theta(n)$$

3. $f(n)$ is polynomially larger than $n^{\log_b a}$, and satisfies the regularity condition, e.g.,

$$T(n) = 4 \cdot T(n/2) + n^3$$

Note that the master theorem does not cover all possible cases (e.g., quick sort).