Combinatorics

Robin Truax

March 2020

Contents

1 The Basics

Convention: The set of natural numbers is the set $\mathbb{N} = \{0, 1, 2, \dots\}$ (in particular, it includes 0).

In these notes, we will focus on the basics of "combinatorics", the math of counting. We will focus on basic techniques such as double-counting, which is a way to prove that two things are equal by showing that they enumerate the same set. In later sections, we will approach more advanced topics, setting ourselves up to begin studying Algebraic Combinatorics in another set of notes.

Definition 1 (n-sets)**.** Given a natural number n, we say a set S is an n-set if $|S| = n$. The prototypical example of an n-set (for $n \geq 1$) is $\{1, \dots, n\}$, which we denote as $[n]$. Indeed, consideration of any n-set reduces (under relabeling) to consideration of $[n]$.

Definition 2 (Permutation)**.** A *permutation* on an n-set is a bijection from the set to itself, which equates to an "ordering" of the set. We denote the number of permutations of an n-set by $n!$.

Lemma 1. *$0! = 1$ and $n! = n \cdot (n-1) \cdots 2 \cdot 1$ for all $n \geq 1$.*

Proof. Trivial, left as an exercise to the reader. □

Lemma 2 (Rearrangement Inequality)**.** *If $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n\}$ are lists of nonnegative real numbers and σ, τ are permutations of $[n]$, then the quantity*

$$a_{\sigma(1)}b_{\tau(1)} + a_{\sigma(2)}b_{\tau(2)} + \cdots + a_{\sigma(n)}b_{\tau(n)}$$

is maximized when σ and τ are the permutations which put A and B in increasing order.

Proof. Trivial, left as an exercise to the reader. □

Theorem 3 (AM-GM Inequality)**.** *For any set of nonnegative real numbers $\{a_1, \dots, a_n\}$, the arithmetic mean of the set is greater than or equal to the geometric mean of the set. Symbolically,*

$$\frac{a_1 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 \dots a_n}$$

Proof. Assume without loss of generality that $a_1 \leq a_2 \leq \cdots \leq a_n$. Then define the sequence $\{r_{ij}\}_{i=1}^{n}$ as $r_{ij} = \sqrt[n]{a_i}$ for all integers $1 \leq i, j \leq n$.

$$\sum_i a_i = \sum_i \prod_j r_{ij}$$

Since these sequences are sorted in ascending order, by the Rearrangement Inequality,

$$\sum_i \prod_j r_{ij} \geq \sum_i \prod_j r_{i,i+j} = n \sum \sqrt[n]{a_i}$$

with equality precisely when all the r_{ij} and thus all the a_i are equal, whence the result follows. □

Lemma 4. *For all $n > 1$,*

$$\left(\frac{n}{e}\right)^n < n! < e\left(\frac{n}{2}\right)^n$$

Proof. We will first prove that $n! > \left(\frac{n}{e}\right)^n$ for all positive integers n. To do this, notice that in the case $n = 1$, the result is true. Now assume it is true for $n = k$: we will prove it is true for $n = k + 1$. To do this, consider:

$$(k+1)! = (k+1)k! > (k+1)\left(\frac{k}{e}\right)^k = \frac{(k+1)k^k}{e^k}$$

But by the definition of e, $\frac{(k+1)^k}{k^k} = \left(1+\frac{1}{k}\right)^k < e$ for all positive k. This implies that $\frac{(k+1)k^k}{e^k} > \frac{(k+1)^{k+1}}{e^{k+1}} = \left(\frac{k+1}{e}\right)^{k+1}$ so by induction the first inequality follows.

Now notice that the AM-GM inequality on $\{1,\ldots,n\}$ implies that $n! < \left(\frac{n+1}{2}\right)^n = \frac{(n+1)^n}{2^n}$ for $n > 1$. But again notice that $\frac{(n+1)^n}{n^n} = \left(1+\frac{1}{n}\right)^n < e$ for all positive n, which means that $n! < e\left(\frac{n}{2}\right)^n$ and the entire result follows. □

1.1 The Binomial Coefficient

Definition 3 (Binomial Coefficient)**.** For a natural number n and integer k, the *binomial coefficient* $\binom{n}{k}$ is defined to be the number of k-element subsets of an n-set (in particular, if k is negative or larger than n, $\binom{n}{k} = 0$ as there are no such subsets).

Lemma 5. *If n is a natural number and $0 \le k \le n$, then:*

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

Proof. Every permutation π of $[n]$ induces a k-element subset $\{\pi(1), \pi(2), \ldots, \pi(k)\}$. Clearly, this is a surjective map from the set of permutations to the k-element. However, the order of the first k elements does not matter. Similarly, the order of the last $n-k$ elements also does not matter. Thus $k!(n-k)!$ permutations generate the same k-element subset, so the total number of k-element subsets is $\frac{n!}{k!(n-k)!}$, as desired. □

Theorem 6. *Following are some properties of the binomial coefficient for any n, k:*

1. $\binom{n}{k} = \binom{n}{n-k}$
2. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
3. $k\binom{n}{k} = n\binom{n-1}{k-1}$
4. $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
5. $\sum_{k=0}^{n} \binom{n}{k}^2 = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$

Proof. Trivial, left as as an exercise to the reader. Try finding a combinatorial and an algebraic proof for each identity! □

Theorem 7 (Binomial Theorem)**.** *Given an indeterminate t,*

$$(1+t)^n = \sum_{k=0}^{n} \binom{n}{k} t^k$$

More generally, given indeterminates x and y,

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

Proof. Write

$$(1+t)^n = \underbrace{(1+t)(1+t)(1+t)\cdots(1+t)}_{n}.$$

Via the distributive property, we see that for a term t^k, we must choose k of the n terms to contribute a t to the term. Thus, the coefficient of t^k is precisely $\binom{n}{k}$. Extending this to all $0 \le k \le n$, the first result follows. The reader is encouraged to follow the logic through to prove the second formulation and to try to prove both via mathematical induction. □

Corollary 7.1. *The number of even-size subsets of a set of size n is the same as the number of odd-size subsets.*

Proof. By the binomial theorem $0 = (1-1)^n = \sum_{k=0}^{n} \binom{n}{k}(-1)^k$. In other words,

$$\sum_{k \text{ even} \leq n} \binom{n}{k} = \sum_{k \text{ odd} \leq n} \binom{n}{k}$$

which is precisely the result desired. □

1.2 More Basic Counting

Theorem 8. *The various numbers of ways to select k objects from an n-set under certain distinguishability rules are given by the following table:*

	Order significant	*Order not significant*
Repetitions allowed	n^k	$\binom{n+k-1}{k}$
Repetitions not allowed	$\frac{n!}{k!}$	$\binom{n}{k}$

Proof. Trivial, left as an exercise for the reader (except for the case of order doesn't matter with repetitions allowed, which we will now cover). □

Lemma 9. *The number of choices of k objects from an n-set with repetitions allowed and order not significant is equal to the number of ways of choosing n nonnegative integers whose sum is k.*

Proof. Given a choice of k objects from the set $a_1, \ldots, a_n$, let x_i be the number of times that the object a_i gets chosen. This induces a bijective correspondence between n-tuples of nonnegative integers summing to k and such choices, as desired. □

Lemma 10. *The number of n-tuples of nonnegative integers $x_1, \ldots, x_n$ with $x_1 + \cdots + x_n = k$ is*

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

Proof. Put $n+k-1$ and fill $n-1$ of them with markers. Let x_1 be the number of spaces before the first marker, x_2, be the number of spaces between the first and second marker, and so on. This induces a bijective correspondence between the n-tuples that sum to k and the choosing of $n-1$ markers in a set of $n+k-1$ spaces, whence the result follows. □

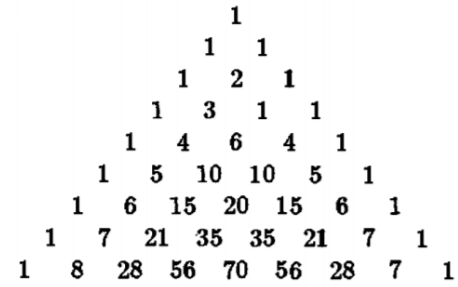
Corollary 10.1. *This implies that the number of ways to select k objects from an n-set with repetitions allowed where order doesn't matter is $\binom{n+k-1}{k}$.*

Theorem 11. *The number of ordered selections without repetition from a set of n objects in $\lfloor e \cdot n! \rfloor$.*

Proof. The number N in question is just $\sum_{k=0}^{n} \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{1}{k!}$. But notice that $e \cdot n! - N < \frac{1}{n} \leq 1$, so $\lfloor e \cdot n! \rfloor = N$, as desired. □

1.3 Pascal's Triangle and Its Properties

Definition 4 (Pascal's Triangle)**.** Pascal's triangle is the standard way to write out the binomial coefficients, as so:



Thus $\binom{n}{k}$ is element k element in row n (if we index from 0).

Theorem 12. *Let p be a prime and let $m = a_0 + a_1 p + \cdots + a_k p^k$, $n = b_0 + b_1 p + \cdots + b_k p^k$ where $0 \leq a_i, b_i < p$ for $i = 0, \ldots, k-1$. Then:*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \mod p$$

Proof. It suffices to prove that if $m = cp + a$ and $n = dp + b$, where $0 \leq a, b < p$, then:

$$\binom{m}{n} \equiv \binom{c}{d}\binom{a}{b} \mod p$$

Since then induction proves the result. Recall that $(1+t)^p \equiv 1 + t^p \mod p$ (as formal polynomials). But then:

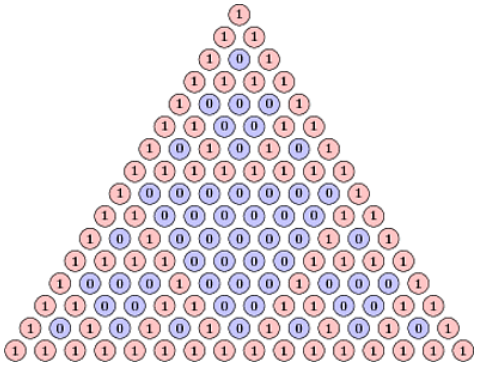
$$\begin{aligned}(1+t)^m &= (1+t)^{cp}(1+t)^a \\ &\equiv (1+t^p)^c(1+t)^a \\ &= \sum_{i=0}^{c} \binom{c}{i} t^{pi} \cdot \sum_{j=0}^{a} \binom{a}{j} t^j\end{aligned}$$

But the only way to get a term $t^n = t^{dp+b}$ is to take the term $i = d$ in the first sum and $j = b$ in the second, whence:

$$\binom{m}{n} \equiv \binom{c}{d}\binom{a}{b} \mod p$$

as required. □

For example, Pascal's Triangle mod 2 has the following structure:



This extends to make the Sierpinski triangle as we add more and more lines to our diagram, a beautiful connection!

1.4 The Principle of Inclusion and Exclusion

Theorem 13 (Principle of Inclusion and Exclusion)**.** *Let $(A_1, \ldots, A_n)$ be a family of subsets of X. Then the number of elements of X which lie in none of the subsets A_i is:*

$$\sum_{I \subseteq [n]} (-1)^{|I|} |A_I|$$

Proof. Trivial, left as an exercise for the reader. If you lack intuition, draw Venn diagrams with progressively more circles and see how to count the space outside all the circles. □

Corollary 13.1. *The number of surjective mappings from an n-set to a k-set is given by:*

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

In particular, since a surjective mapping from an n-set to itself is a permutation,

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

Proof. Take X to be the set of all mappings from $[n]$ to $[k]$, so $|X| = k^n$. For $i = 1, \ldots, k$, let A_i be the set of mappings f for which the point i does not lie in the range of f. Then $|A_i| = (k-1)^n$ and more generally $|A_I| = (k - |I|)^n$. By PIE, we see that the number of surjections is equal to

$$\sum_{I \subseteq [k]} (-1)^{|I|} (k - |I|)^n$$

The result follows from noticing there are $\binom{k}{i}$ sets I of cardinality i and summing 1 to k. □

Definition 5 (Derangement)**.** A *derangement* of $[n]$ is a permutation π of $[n]$ with no fixed point (that is, there is no $i \in [n]$ with $\pi(i) = i$). We denote the number of derangements of n-set by $d(n)$.

Theorem 14. *The number of derangements of $[n]$ is equal to:*

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

Proof. Let X be the set of permutations and A_i the set of permutations fixing the point i. Thus $|A_i| = (n-1)!$ and more generally $|A_I| = (n - |I|)!$. Thus the number of derangements is:

$$\sum_{I \subseteq [n]} (-1)^{|I|} (n - |I|)! = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)! = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}.$$

□

Corollary 14.1. *$d(n)$ is equal to the nearest integer to $n!/e$ for $n \geq 1$.*

Proof. Trivial from using the Taylor series for e^x, left as an exercise for the reader. □

2 Recursion

Definition 6 (Fibonnaci Numbers)**.** The *Fibonacci numbers* is the sequence of natural numbers given by $F_0 = F_1 = 1$ and $F_n = F_{n+1} + F_{n+2}$. The Fibonacci sequence begins $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

The Fibonacci numbers are the classic example of a sequence given first by a "recurrence relation" and only secondly by some closed-form equation.

Definition 7 (Recurrnece Relations)**.** A $(k+1)$-recurrence relation for a sequence g with terms $g_0, g_1, \ldots$ is a relation giving g_n in terms of $g_{n-1}, g_{n-2}, \ldots, g_{n-k}$. Clearly, given such a relation, g is uniquely determined by its first k values – whether that is $G_0, \ldots, G_{k-1}$ or $G_1, \ldots, G_k$.

Thus, the Fibonacci numbers' recurrence relation is a 3-term recurrence relation, since F_n is given in terms of F_{n-1} and F_{n-2}.

2.1 Generating Functions

Definition 8 (Generating Function)**.** Given a sequence $s_0, s_1, \ldots$, we say the formal power series $\phi(t) = \sum_{n \geq 0} s_n t^n$ is the *(standard) generating function* for s.

Definition 9 (Exponential Generating Function)**.** Given a sequence $s_0, s_1, \ldots$, we say the formal power series $\psi(t) = \sum_{n \geq 0} \frac{s_n t^n}{n!}$ is the *exponential generating function* for s. Notice that the formal algebraic derivative $A'(t)$ is the exponential generating function of the new sequence $s' = s_1, s_2, \ldots$.

2.2 The Fibonacci Numbers

We will first document some number of places where the Fibonnaci numbers arise:

Theorem 15. *The number of ways to write $n \in \mathbb{N}$ as the ordered sum of 1s and 2s is F_n.*

Proof. We will denote the number of ways to write a natural number n as the sum of 1s and 2s as $S(n)$. By our note in the last section, it suffices to show that $S(0) = S(1) = 1$ and that $S(n) = S(n-1) + S(n-2)$. Clearly, the initial conditions are the same: the only sum of 1s and 2s equalling 0 is the empty sum, and the only sum of 1s and 2s equalling 1 is 1. There are two cases for ordered sums equalling n:

1. The first number is 1. In this case, there are $S(n-1)$ completions of the rest of the sum.
2. The first number is 2. In this case, there are $S(n-2)$ completions of the rest of the sum.

Thus $S(n) = S(n-1) + S(n-2)$, and the result follows. □

Theorem 16. *The worst-case input (with respect to the size of the inputs) for the Euclidean algorithm is a difference of two Fibonacci numbers.*

Proof. This follows beautifully and simply from induction. Left as an exercise to the reader. □

Theorem 17 (Zeckendorf's Theorem)**.** *Every positive integer can be written in a unique way as the sum of one or more distinct Fibonacci numbers in such a way that the sum does not include any two consecutive Fibonacci numbers.*

Proof. Again, a simple induction proof. Left as an exercise to the reader. □

Theorem 18. *The limit of the terms F_{n+1}/F_n is the golden ratio $\phi = \frac{1+\sqrt{5}}{2}$.*

Proof. Note that clearly $1 < L \leq 2$. Now let $L = \lim_{n\to\infty} F_{n+1}/F_n = \lim_{n\to\infty} 1 + \frac{F_{n-1}}{F_n} = 1 + \frac{1}{L}$. Thus $L^2 - L - 1 = 0$ and by the quadratic formula (and the fact that $L > 0$) $L = \frac{1+\sqrt{5}}{2}$. □

Theorem 19.

$$F_n = \left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Proof. Let $\phi(t)$ be the power series $\phi(t) = \sum_{n\geq 0} F(n)t^n$. Notice that $t\phi(t) = \sum_{n\geq 1} F(n-1)t^n$ and similarly $t^2\phi(t) = \sum_{n\geq 2} F(n-2)t^n$. This, together with comparison of the 1 and t terms, implies:

$$\phi(t) = 1 + (t+t^2)\phi(t) \Rightarrow \phi(t) = \frac{1}{1-t-t^2}$$

Now let $\alpha = \frac{-1+\sqrt{5}}{2}$ and $\beta = \frac{-1-\sqrt{5}}{2}$ be the roots of $1-t-t^2$, so:

$$\phi(t) = \frac{-1}{(\alpha-t)(\beta-t)} = \frac{a}{\alpha-t} + \frac{b}{\beta-t}$$

whence, by multiplying through by $(\alpha-t)(\beta-t)$, we see that:

$$-1 = a(\beta-t) + b(\alpha-t)$$

whence $a+b=0$ and $a\beta+b\alpha=-1$. This implies $a\alpha+b\alpha=0$, whence $a(\alpha-\beta)=1 \Rightarrow a = \frac{1}{\sqrt{5}} \Rightarrow b = \frac{-1}{\sqrt{5}}$. But notice that we can rearrange $\phi(t)$ in the following manner:

$$\phi(t) = \frac{a}{\alpha-t} + \frac{b}{\beta-t} = \frac{a/\alpha}{1-t/\alpha} + \frac{b/\beta}{1-t/\beta} = \frac{a}{\alpha}(t/\alpha)^n + \frac{b}{\beta}(t/\beta)^n$$

Thus $F_n = \frac{a}{\alpha}\left(\frac{1}{\alpha}\right)^n + \frac{b}{\beta}\left(\frac{1}{\beta}\right)^n$. Finally, notice that $\frac{1}{\alpha} = \frac{1+\sqrt{5}}{2}$ and $\frac{1}{\beta} = \frac{1-\sqrt{5}}{2}$, whence:

$$F_n = \left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

□

2.3 Solving Linear k-Recurrence Relations

We now document the general solution of a linear recurrence relation of the form $F(n) = a_1F(n-1) + \ldots a_kF(n-k)$. Start by supposing that $F(n) = \alpha^n$ is a solution to this equation. Then it is not hard to see that α works if and only if it is a root of the characteristic equation $0 = -x^k + a_1x^{k-1} + \cdots + a_k$.

Now we will try to find k "fundamental solutions" $A_1(n), \ldots A_k(n)$. For each root α_i with multiplicity d_i, we take the fundamental solutions $\alpha_i^n, n\alpha_i^n, \ldots, n^{d-1}\alpha_i^n$. By the Fundamental Theorem of Algebra, we end up with k fundamental solutions. Any solution of the general linear recurrence relation will then take the form:

$$b_1A_1(n) + \cdots + b_kA_k(n)$$

for some coefficients $b_1, \ldots, b_k$. It is easy to find these coefficients using the initial conditions for the recurrence relation.

We now offer another proof of the "useless theorem" (the closed-form expression for the Fibonacci numbers).

Theorem 20.

$$F_n = \left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Proof. Our recurrence relation $F_n = F_{n-1} + F_{n-2}$ has characteristic equation $0 = -x^2 + x + 1$ and hence (by the quadratic formula) roots $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$. Thus a closed-form expression has the form:

$$b_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + b_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

From the initial conditions $F_0 = F_1 = 1$, it is trivial to find b_1 and b_2 and verify the result. □

2.4 Derangements and Involutions

We will use recurrence relations to to offer another proof of our formula for the number of derangements of an n-set. Recall that our initial parameters will be $d(0) = 1, d(1) = 0$.

Lemma 21.

$$d(n) = (n-1)(d(n-1) + d(n-2))$$

Proof. Consider an arbitrary permutation π and let $\pi(1) = i$. There are two cases for $\pi(i)$:

1. $\pi(i) = 1$. In this case, there are $d(n-2)$ ways to complete the derangement.
2. $\pi(i) \neq 1$. In this case, there are $d(n-1)$ ways to complete the derangement (essentially, one imagines 1 and i as the same in terms to needing to avoid sending i to 1 under π).

But there were $(n-1)$ choices for $\pi(1)$, so $d(n) = (n-1)(d(n-1) + d(n-2))$, as desired. □

Theorem 22. *The number $d(n)$ of derangements of an n-set is given by*

$$d(n) = n! \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!}\right)$$

Proof. Let $f(n)$ denote the RHS. It is trivial to check that $f(0) = 1, f(1) = 0$ (i.e. $d(n)$ and $f(n)$ satisfy the same initial values). Then all we must do is show that $f(n)$ satisfies the same recursive relation as $d(n)$:

$$(n-1)(f(n-1) + f(n-2)) = (n-1)(n-1)! \left(\sum_{i=0}^{n-1} \frac{(-1)^i}{i!}\right) + (n-1)(n-2)! \left(\sum_{i=0}^{n-2} \frac{(-1)^i}{i!}\right)$$

$$= (n-1)(n-1)! \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!} - \frac{(-1)^n}{n!}\right) + (n-1)! \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!} - \frac{(-1)^{n-1}}{(n-1)!} - \frac{(-1)^n}{n!}\right)$$

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

$$= n! \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!}\right) = f(n)$$

whence by induction $f(n) = d(n)$ for all n. □

Definition 10. A permutation of a set is called an *involution* if it is its own inverse; that is $\pi : S \to S$ is an involution on S if $\pi(\pi(S)) = \mathrm{id}_S$. We denote the number of involutions on an n-set by $s(n)$.

Lemma 23.

$$s(n) = s(n-1) + (n-1)s(n-2)$$

Proof. There are two cases for an involution π on $[n]$:

1. π fixes n. There are $s(n-1)$ such permutations.
2. π does not fix n. That is, it is swapped with some i. There are $n-1$ choices for this i and $s(n-2)$ possible completions, so there are $(n-1)s(n-2)$ such permutations.

The result follows. □

Proposition 24. *For every $n > 1$, $s(n)$ is even.*

Proof. Note that $s(2) = 2$ and $s(3) = s(2) + 2s(1) = 4$. The result follows immediately from induction and the recurrence relation. □

Proposition 25. *$s(n) > \sqrt{n!}$ for all $n > 1$.*

Proof. Notice that $s(2) = 2 > \sqrt{2!}$. Now assume the result holds for all $n > k$; we seek to prove it for $n = k$. To do this, note that by hypothesis and our recurrence relation $s(k) > \sqrt{(k-1)!} + (k-1)\sqrt{(k-2)!}$. This can be simplified to $s(k) > (\sqrt{n-1}+1)\sqrt{(n-1)!} > \sqrt{n}\sqrt{(n-1)!} = \sqrt{n!}$, which proves the result for $n = k$, as desired. □

Definition 11. The double factorial of a positive integer n, denoted $n!!$, is the product of all positive integers less than or equal to n with the same parity as n. For example, $6!! = 6 \cdot 4 \cdot 2 = 48$. Notice that if n is even, then $n!! = n!2^{n/2}$.

Theorem 26. *The number of involutions on an n-set is:*

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (2k-1)!!$$

Proof. Let $\tau \in S_n$ be an involution on $[n]$ and write it as a product of disjoint cycles. Since it has order 1 or 2, it cannot contain any cycles of order 3 or more, so it must be a product of disjoint transpositions. Now suppose that τ is a product of k disjoint transpositions. We must choose the $2k$ permutes elements and then group the $2k$ letters into k pairs. Thus, there are $\binom{n}{2k}(2k-1)!!$ involutions that are products of k disjoint transpositions. Summing from $k = 0$ (the identity) to $\lfloor n/2 \rfloor$ gives the desired result. □

2.5 Quicksort Via Generating Functions

Definition 12 (Quicksort)**.** Suppose one has a list L and seeks to sort it. Then the Quicksort algorithm to sort this list is as follows:

1. Let a be the first item of L.
2. Partition the rest of the list into sublists L^-, L^+ consisting of the elements less than and greater than a respectively.
3. Sort L^- and L^+ (trivial once they are empty) and return (L^- sorted, a, L^+sorted).

Theorem 27. *The average number of comparisons needed to sort a list of length n is $2n\log(n) + O(n)$.*

Proof. Let the average number of comparisons required to sort a list of length n be denoted q_n. Notice that the first step takes $n-1$ comparisons. If a_n is the kth smallest element, the other steps requires an average of $q_{k-1} + q_{n-k}$ comparisons. Thus, the total average other steps required is the average over all k, so:

$$q_n = n - 1 + \frac{1}{n}\sum_{k=1}^{n}(q_{k-1} + q_{n-k}) = n - 1 + \frac{2}{n}\sum_{k=1}^{n} q_k$$

The initial value is clearly $q_0 = 0$. We seek now to solve this recurrence relation by finding a generating function $Q(t) = \sum_{n\geq 0} t^n$. Notice that:

$$\sum_{n\geq 0} nq_n t^n = \sum_{n\geq 0} n(n-1)t^n + 2\sum_{n\geq 0}\left(\sum_{i=0}^{n-1} q_i\right)t^n$$

Notice that the LHS is $tQ'(t)$ and the first term of the RHS is just the Taylor series of $\frac{2t^2}{(1-t)^3}$. The second term of the RHS is difficult, but I claim it is equal to $\frac{2tQ(t)}{1-t}$. This is because:

$$\frac{tQ(t)}{1-t} = (t + t^2 + t^3 + \dots)(q_0 + q_1 t + q_2 t^2 + \dots) = \sum_{n\geq 0}\sum_{i=0}^{n-1} q_i t^n$$

Thus we have the following first-order linear differential equation:

$$Q'(t) = \frac{2t^2}{t(1-t)^3} + \frac{2t}{t(1-t)}Q(t)$$

This is solved by the usual integrating factor method resolving into:

$$Q(t) = \frac{-2(t + \log(1-t))}{(1-t)^2}$$

One can verify that the RHS is equal to:

$$Q(t) = 2\left(\frac{t^2}{2} + \frac{t^3}{3} + \frac{t^4}{4} + \dots\right)(1 + 2t + 3t^2 + \dots)$$

Thus $q_n = 2\sum_{i=2}^{n}\left(\frac{1}{i}\right)(n-i+1) = 2(n+1)\sum_{i=1}^{n}\left(\frac{1}{i}\right) - 4n$. But since $\sum_{i=1}^{n}\left(\frac{1}{i}\right) = \log(n) + O(1)$, whence $q_n = 2n\log(n) + O(n)$. □

3 Special Sequences

Now that we have developed the necessary theory, we will explore some of the special sequences that pop up in combinatorial applications. In particular, we will discuss the famous Catalan numbers.

3.1 Catalan Numbers and Their Many Forms

Definition 13 (Catalan Numbers)**.** The *Catalan number* C_n is the number of lattice paths along the edges of a grid with $n \times n$ square cells, with the following requirements:

1. The path starts at the lower left corner and finishes in the upper right corner.
2. The path can only move upwards or rightwards.
3. The path can't pass above the lower-left-to-upper-right diagonal of the square.

In particular, $C_0 = 1$.

Theorem 28 (Closed-form Catalan)**.** *The nth Catalan number is given by the the equation:*

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$$

Proof. Notice that all paths are enumerated by $\binom{2n}{n}$. Then notice that any path going over the diagonal can have the portion of itself after its first crossing over the diagonal reflected to give a unique path from to the point $(n-1, n+1)$; hence there are $\binom{2n}{n+1}$ such paths. The result follows. □

Lemma 29 (Recurrence Relation for Catalan Numbers)**.** *We define* $C_0 = 1$*. For* $n \geq 0$*,*

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$$

Proof. Given a path P, let i be the last time strictly before the endpoint of P that P touches the diagonal. There are C_i ways to get to P and C_{n-i} ways to complete the path, so there are $C_i C_{n-i}$ total paths with final "touchpoint" i. Summing over all possible values of i (namely $0 \leq i \leq n$) gives us the desired result. □

Theorem 30. *The number of ways a sum of* $n+1$ *terms can be bracketed so that it is calculated just by adding two terms at a time is* C_n*. For example, given the* 4*-term sum* $a+b+c+d$*, we can bracket it in* 5 *ways:*

1. $((a+b)+c)+d$
2. $(a+(b+c))+d$
3. $a+((b+c)+d)$
4. $a+(b+(c+d))$
5. $(a+b)+(c+d)$

Proof. Denote the number of such sums by $s(n)$. It suffices to note that $s(0) = 1$ and that s satisfies the above recurrence relation. This is left as an exercise to the reader. □

Following are a list of places where the Catalan numbers show up as an enumerating sequence. Proving the relations is left as an exercise to the reader, but in some cases, hints are given.

Proposition 31. C_n *is the number of Dyck words of length* $2n$*, where a Dyck word is a string consisting of* n X*'s and* n Y*'s such that no initial segment of the string has more* Y*'s than* X*'s.*

Proof. This is simply another way to imagine the initial definition (X denotes "move right" and Y denotes "move up"). □

Corollary 31.1. C_n *counts the number of expressions containing* n *pairs of parentheses which are correctly matched.*

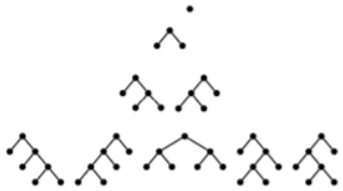
Corollary 31.2. *If one is standing one step from the edge of a cliff,* C_n *enumerates the number of sequences of* $2n$ *left-or-right steps you can take without falling off the cliff. Thus, if a murderer puts you one step from the edge of a cliff and hands you a random sequence of* $2n$ *left-or-right steps that you must perform, you have a* $\frac{1}{n+1}$ *chance of survival.*

Corollary 31.3. C_n *is the number of ways to form a "mountain range" with* n *upstrokes and* n *downstrokes that all stay above a horizontal line, as seen below:*

$n = 0$:	*	1 way
$n = 1$:	/\	1 way
$n = 2$:	/\ /\/\, / \	2 ways
$n = 3$:	/\ /\ /\ /\/\ / \ /\/\/\, /\/ \, / \/\, / \, / \	5 ways

Mountain Ranges

Definition 14 (Rooted Binary Tree)**.** A *rooted binary tree* is an arrangement of nodes and lines connecting them where there is a distinguished special node (the root) and as one descends from the root, there are either two lines going down or zero. *Internal nodes* are those nodes which have two "children".



Proposition 32. *There are C_n rooted binary trees with n internal nodes.*

Proposition 33. *C_n is the number of permutations of $[n]$ that avoid sending $1, 2, 3$ to $i, i+1, i+2$ (thus avoiding the sequence 123 in the resultant string).*

Proposition 34. *C_n is the number of ways a regular $n+2$-gon can be divided into n triangles if different orientations are counted separately.*

Proposition 35. *C_n is the number of ways for $2n$ people sitting around a circular table to all be simultaneously shaking hands in such a way that none of the arms cross each other.*

3.2 Bell Numbers

Definition 15. The *Bell number* B_n is the number of partitions of an n-set. For example, $B_0 = 1, B_1 = 1, B_2 = 2$.

Lemma 36. *For $n \geq 1$,*

$$B_n = \sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k}$$

Proof. Take $X = [n]$ and consider a partition of X. It has a unique part containing n, say $\{n\} \cup Y$ (where Y is a subset of $[n-1]$). If $|Y| = k-1$, then there are $\binom{n-1}{k-1}$ choices of Y and B_{n-k} choices of a partition of the remaining points, so there are $\binom{n-1}{k-1} B_{n-k}$ such partitions. We then sum over all possible values of k (namely 1 to n), and the result follows. □

Proposition 37. *If a natural number N is the product of n distinct primes, then B_n gives the number of distinct factorizations of N.*

Theorem 38 (The Exponential Generating Function of the Bell Numbers)**.** *The exponential generating function of the Bell numbers is given by the following equation:*

$$\sum_{n \geq 0} \frac{B_n t^n}{n!} = e^{e^t - 1}$$

Proof. Let $F(t) = \sum_{n \geq 1} B_n t^n / n!$ be the exponential generating function of B_n. Notice that:

$$\frac{d}{dt} F(t) = \sum_{n \geq 1} \frac{B_n t^{n-1}}{(n-1)!}$$

By substituting the recurrence relation and simplifying:

$$\frac{d}{dt} F(t) = \left(\sum_{j \geq 0} \frac{t^j}{j!} \right) \cdot \left(\sum_{k \geq 0} \frac{B_k t^k}{k!} \right) = e^t F(t)$$

By solving this separable differential equation and plugging in the initial condition that $F(0) = 1$, we obvtain the desired result. □

3.3 Stirling Numbers

Definition 16 (Stirling Numbers)**.** Let n and k be positive integers. The *Stirling number of the first kind* $s(n,k)$ is defined by the rule that $(-1)^{n-k}s(n,k)$ is the number of permutations of $\{1,\ldots,n\}$ with k cycles.

The *Stirling number of the second kind* $S(n,k)$ is the number of partitions of $\{1,\ldots,n\}$ with k nonempty parts. In particular, if $k \leq 0$ or $k > 0$, both $s(n,k)$ and $S(n,k)$ are 0.

Proposition 39 (Properties of Stirling Numbers)**.** *Following are some basic properties of Stirling numbers:*

1. $\sum_{k=1}^{n}(-1)^{n-k}s(n,k) = \sum_{k=1}^{n}|s(n,k)| = n!$
2. $\sum_{k=1}^{n} S(n,k) = B_n$
3. $s(n,n) = S(n,n) = 1$
4. $s(n+1,k) = -ns(n,k) = s(n,k-1)$
5. $S(n+1,k) = kS(n,k) + S(n,k-1)$
6. *Define* $(t)_n := t(t-1)\ldots(t_n+1)$. *Then* $(t)_n = \sum_{k=1}^{n} s(n,k)t^k$ *and* $t^n = \sum_{k=1}^{n} S(n,k)(t)_k$.

Proof. Trivial (except for 6, which follows by induction) and thus left as exercises for the reader. □

Proposition 40.

$$S(n,k) = \frac{1}{k!}\sum_{j=1}^{k}(-1)^{k-j}\binom{k}{j}j^n$$

Proof. This is $\frac{1}{k!}$ times the number of surjections $[n] \to [k]$. Thus it suffices to prove that the number of such surjections is $k!S(n,k)$. Notice that each partition of $[n]$ with k non-empty parts $A_1,\ldots,A_k$ defines a surjection from $[n] \to [k]$: namely the function given by mapping $i \in A_j$ to j. However, under reordering of our k non-empty parts, we can create $k!$ such surjections from each partition, whence the result follows. □

4 Geometry

This section is a brief look at some interesting definitions from "geometric" combinatorics.

4.1 Extremal Set Theory

Definition 17 (Intersecting Families)**.** A family $\mathcal{F}$ of subsets of X is *intersecting* if any $A, B \in \mathcal{F}$ have nonempty intersection.

Proposition 41. *An intersecting family* $\mathcal{F}$ *of subsets of* $[n]$ *satisfies* $|\mathcal{F}| \leq 2^{n-1}$. *This is the best possible bound, as it is realized for all* n.

Proof. The 2^n subsets of $[n]$ can be partitioned into 2^{n-1} pair of the form $\{A, [n] \setminus A\}$. Clearly, only one set can be taken from each pair, whence the inequality follows. The bound is realized precisely when one set is taken from each pair. □

Definition 18 (Sperner Families)**.** A family $\mathcal{F}$ of sets is called a *Sperner family* if no member of $\mathcal{F}$ properly contains any other.

Proposition 42. *Let* $\mathcal{F}$ *be a sperner family of subsets of the* n*-element set* $X = \{1,\ldots,n\}$. *Then* $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$. *If equality holds, then* $\mathcal{F}$ *consists of all subsets of* X *of size* $\lfloor n/2 \rfloor$ *or all subsets of size* $\lceil n/2 \rceil$.

Proof. Consider a chain of subsets $\varnothing = A_0 \subset A_1 \subset \cdots \subset A_n = X$. Notice that there is a bijective correspondence between chains (of this length) and permutations, given by:

$$\pi \mapsto \varnothing = \{\} \subset \{\pi(1)\} \subset \{\pi(1), \pi(2)\} \subset \cdots \subset \{\pi(1), \ldots, \pi(n)\} = X$$

Thus there are $n!$ chains, each with a $1/\binom{n}{k}$ chance to contain a subset A (with $|A| = k$). By assumption, any chain contains at most one member of $\mathcal{F}$, so:

$$\sum_{A \in \mathcal{F}} |A|!(n - |A|!) = n! \left(\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \right)$$

But since there are only $n!$ chains, we see that:

$$\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \leq 1$$

The middle binomial coefficients are the largest, so if $m = \lfloor n/2 \rfloor$, we see that $\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{m}} \leq 1$ whence $|\mathcal{F}| \leq \binom{n}{m}$, as desired. Furthermore, this bound is only met when all the sets are of size m or $n - m = \lceil n/2 \rceil$. We are done if n is even: if not, then we must prove that either all of the sets in $\mathcal{F}$ have size m or all of them have size $m + 1$. To do this, note that every chain must contain precisely one element of $\mathcal{F}$ to meet the bound, and then consider the sequence:

$$A_0 \subset B_0 \supset A_1 \subset \ldots$$

where the A_i are all the sets of size m and the B_i are all the sets of size $m + 1$. Now notice that if there is one A_0 in $\mathcal{F}$, then B_0 cannot be in there, hence A_1 is, hence B_1 is not, etc. Similarly, if there is one $B_0 \in \mathcal{F}$, A_0 cannot be in there, A_1 cannot be in there, but B_1 must be, etc. Thus the result follows. □

Theorem 43 (The de Bruijin-Erdös Theorem)**.** *Let $\mathcal{F}$ be a family of subsets of the set $X = \{1, \ldots, n\}$ and suppose that any two sets of $\mathcal{F}$ have exactly one point in common. Then $|\mathcal{F}| \leq n$ with equality only when one of the following situations occurs:*

1. *Up to renumeration, we have $\mathcal{F} = \{A_1, \ldots, A_n\}$ where $A_i = \{i, n\}$ for $i = 1, \ldots, n$.*
2. *Up to renumeration, we have $\mathcal{F} = \{A_1, \ldots, A_n\}$ where $A_n = \{1, 2 \ldots, n-1\}$ are $A_i = \{i, n\}$ for $1 \leq i \leq n - 1$.*
3. *For some positive integer q, we have $n = q^2 + q + 1$, each set in $\mathcal{F}$ has size $q + 1$, and each point lies in $q + 1$ members of $\mathcal{F}$.*

We will not offer a proof here, but encourage you to research it on your own.

4.2 Packings, Coverings, and Steiner Triple Systems

Consider the following problem:

Problem 1. Given integers l, m, n with $l < m < n$, what is the greatest number of m-element subsets of an n-element set with the property that any l-element subset lies in at most one of the chosen sets?

Proposition 44. *Let $\mathcal{B}$ be a family of m-subsets of an n-set such that any l-set lies in at most one member of $\mathcal{B}$. Then $|\mathcal{B}| \leq \binom{n}{l}/\binom{m}{l}$ with equality if and only if any l-subset lies in exactly one member of $\mathcal{B}$.*

Proof. Count pairs of l-sets and elements in $\mathcal{B}$, (L, B). There are $\binom{m}{l}$ subsets of size l in each B, so there are $|B| \cdot \binom{m}{l}$ such pairs. On the other hand, there are $\binom{n}{l}$ subsets of size l, each in at most one $B \in \mathcal{B}$, so the number of such pairs is bounded above by $\binom{n}{l}$, with equality if every l-set lies in a unique member of $\mathcal{B}$, whence the result follows. □

Definition 19. A pair $(X, \mathcal{B})$ where X is an n set and $\mathcal{B}$ a family of m-subsets satisfying the hypotheses of the proposition and attaining the bound is called a *Steiner system* $S(l, m, n)$.

Problem 2. For which values of l, m, n does a Steiner system $S(l, m, n)$ exist?

Definition 20. A Steiner system $S(2, 3, n)$ is called a *Steiner triple system* (with order n) and denoted STS(n). Explicitly, it is a set X of points and a set $\mathcal{B}$ of 3-element subsets of X such that any two points of X lie in a unique triple.

Theorem 45. *If there exists a Steiner triple system of order n, then $n = 0$ or $n \equiv 1, 3 \mod 6$.*

Proof. Suppose that $(X, \mathcal{B})$ is an STS of order $n > 0$. We claim the following results:

Lemma 46. *Any point lies in $(n-1)/2$ triples.*

This follows from noticing that there are $n-1$ two-element subsets containing a point x and that the fact that any 3-subset containing x contains *two* such subsets, so $\frac{n-1}{2}$ subsets contain x.

Lemma 47. *There are $n(n-1)/6$ triples.*

This follows from noticing that there are $n(n-1)/2$ pairs (x, B) (where x is a point and B a triple containing x). But then there are three choices of x for each B, so there are $n(n-1)/6$ triples in all.

This immediately demonstrates the result: both $(n-1)/2$ and $n(n-1)/6$ must be integers, which implies that n is $1, 3 \mod 6$, as desired. □

Theorem 48. *If $n \equiv 3 \mod 6$, then there exists a Steiner triple system of order n.*

Proof. Suppose that $n \equiv 3 \mod 6$, so $n = 3m$ where m is an odd positive integer. Then let $X = \{a_i, b_i, c_i \mid i \in \mathbb{Z}/(m)\}$ and let the blocks come in the following two types:

1. Triples of the form $a_i a_j b_k$, $b_i b_j c_k$ or $c_i c_j a_k$ where $i, j, k \in \mathbb{Z}/(m)$, $i \neq j$ and $i + j = 2k$ in $\mathbb{Z}/(m)$.
2. Triples of the form $a_i b_i c_i$ for $i \in \mathbb{Z}/(m)$

One can verify that this gives a Steiner triple system by checking that any pair of points lies in a unique triple of the above form. □

Theorem 49. *If $n \equiv 1 \mod 6$, then there exists a Steiner triple system of order n.*

The proof is not offered here, but we encourage you to research the various ways of constructing such a Steiner triple system.

Definition 21 (Packings and Coverings)**.** Let X be a set with n elements. A $(2, 3)$-*packing* is a set $\mathcal{B}$ of triples such that any two points of X are contained in *at most* one member of $\mathcal{B}$, and a $(2, 3)$-*covering* is a set $\mathcal{B}$ are contained in *at least* one member of $\mathcal{B}$. The size of the largest $(2, 3)$-packing is denoted $p(n)$ and the size of the smallest $(2, 3)$-covering is denoted $c(n)$.

Proposition 50. *For all n, $p(n) \leq n(n-1)/6$ and $c(n) \geq n(n-1)/6$, with equality in either bound if and only if there exists a STS of order n.*

4.3 Finite Geometry

Definition 22 (Gaussian Coefficients)**.** The *Gaussian coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is defined to be the number of k-dimensional subspaces of $V(n, q)$ (the vector space of dimension n over over the finite field of size q).

Theorem 51 (Formula for the Gaussian Coefficient)**.**

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}$$

Proof. First notice that the number of linearly independent k-tuples in an n-dimensional space is $(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$. A k-dimensional subspace is spanned by k-linearly independent vectors, which we have counted: but a given subspace will have many different bases.

However, each subspace will have exactly as many bases as the number of linearly independent k-tuples in a k-dimensional space, so we can just use our earlier formula substituting k for n. Dividing the two gets the number of k-dimensional subspaces and our desired formula. □

Proposition 52.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q \tag{1}$$

4.4 Projective Geometry

Definition 23 (Projective Plane)**.** The real projective plane $\mathbb{P}_2(\mathbb{R})$ is the set of lines through the origin (1-dimensional subspaces) of 3-dimensional space $\mathbb{R}^3$.

Notice that by choosing a plane Π not through the origin, we can identify each line with a point on Π (namely the point it passes through) except all lines that are parallel to Π (which become "points at infinity"). Also notice that a line in the projective plane Π is swept out by a 2-dimensional subspace in $\mathbb{R}^3$, and the entire plane is swept out by the entire 3-dimensional space of $\mathbb{R}^3$.

Definition 24 (n-dimensional Projective Space)**.** The n-dimensional *projective space* over a field F, denoted $\mathbb{P}_n(F)$ is composed of a $(n+1)$-dimensional vector space V over F, where the points of $\mathbb{P}_n(F)$ are the 1-dimensional subspaces of V, the lines are the 2-dimensional subspaces, the planes are the 3-dimensional subspaces, and so on.

Definition 25 (k-flat)**.** We use the term k-flat for an object in projective geometry represented by a $(k+1)$-dimensional vector subspace. For example, a line in projective geometry is a 1-flat.

Proposition 53 (Properties of Projective Space)**.** *Following are some elementary properties of projective space and brief proofs of them using linear algebra.*

1. *Two points lie in a unique line (since two points are* 1*-dimensional subspaces and their span is* 2*-dimensional).*
2. *Two intersecting lines lie in a unique plane (since the lines are* 2*-dimensional with a* 1*-dimensional intersection, so their span is* 3*-dimensional).*
3. *Two coplanar lines intersect (two* 2*-dimensional subspaces with a* 3*-dimensional span must intersect* 1*-dimensionally).*

Proposition 54. *$\mathbb{P}_n(\mathbb{F}_q)$ has $\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = (q^{n+1}-1)/(q-1)$ points. It has $\binom{n+1}{k+1}_q$ k-flats, each of which contains $(q^{k+1}-1)/(q-1)$ points.*

An interesting "reverse characterization" was given by Veblen and Young, demonstrating why we would care about projective geometry in combinatorics:

Theorem 55 (Veblen-Young Theorem)**.** *Let $\mathcal{L}$ be a family of subsets (called lines) of the set X. Suppose that the following conditions hold:*

1. *Every line contains at least three points,*
2. *Two points of X lie in a unique line,*
3. *There exist two disjoint lines,*
4. *If a line meets two sides of a triangle, not at their intersection, then it meets the third side also.*

Then X and $\mathcal{L}$ can be identified with the points and lines of the projective space $\mathbb{P}_n(\mathbb{F}_q)$ for some prime power q and $n \geq 3$.

Definition 26 (Projective Planes)**.** A *projective plane* of order q consists of a set X of $q^2 + q + 1$ elements called points, and a set $\mathcal{B}$ of $(q+1)$-element subsets of $\mathcal{B}$ called lines having the property that any two points lie on a unique line.

Proposition 56 (Properties of Projective Planes)**.** *Following are some basic properties of a projective plane with order q:*

1. *any point lies on $q+1$ lines,*
2. *two lines meet in a unique point,*
3. *and there are $q^2 + q + 1$ lines.*

Theorem 57 (Duality Principle)**.** *Let $(X, \mathcal{B})$ be a projective plane of order q. Further let $X' = \mathcal{B}$ and $\mathcal{B}' = \{\beta_x \mid x \in X\}$, where $\beta_x = \{L \in \mathcal{B} \mid x \in L\}$. Then $(X', \mathcal{B}')$ is also a projective plane of order q, swapping the lines and points of the original plane.*

Definition 27 (Affine Planes)**.** An *affine plane* of order q consists of a set X of q^2 points and a set $\mathcal{B}$ of q-element subsets of X called lines such that two points lie on a unique line. We call two lines in an affine plane *parallel* if they are equal or disjoint.

Proposition 58 (Properties of Affine Planes)**.** *Following are some basic properties of a affine plane with order q:*

1. *Any point lies on $q+1$ lines.*
2. *There are $q(q+1)$ lines.*
3. *If p is a point and L a line, there is a unique line L' through p parallel to L.*
4. *Parallelism is an equivalence relation. Furthermore, parallel class contains q lines which partition the point set.*

Theorem 59. *A projective plane of order q exists if and only if an affine plane of order q exists.*

Proof. Removing a line (and all its points) from a projective plane creates an affine plane. Conversely, let X be the set of points in an affine plane and Y be the set of parallel classes of lines in said affine plane. Then if we add each element in Y to X, let Y be a new line, and replace each line L with a new line $L* = L \cup \{C\}$ (where C is the parallel class containing L), then the result can be seen to be a projective plane. □

In this case, we call the line Y the *line at infinity*, for obvious reasons.

4.5 Lattices

Definition 28 (Lattices)**.** A *lattice* is a set X with two binary operations $\wedge$ (called the greatest lower bound) and $\vee$ (called the least upper bound) defined on X, as well as two distinguished elements 0 and 1 that satisfy the following axioms:

1. $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$ (associativity)
2. $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ (commutativity)
3. $x \wedge x = x \vee x = x$, $x \wedge (x \vee y) = x = x \vee (x \wedge y)$, and $x \wedge 0 = 0$ and $x \vee 1 = 1$ (idempotent laws)

Proposition 60. *An equivalent definition for a lattice is that it is a poset X with a unique minimal element 0 and a unique maximal element 1 such that any pair of elements in X have a greatest lower bound and least upper bound.*

Proof. Trivial, left as an exercise for the reader. □

Definition 29. A lattice L is *distributive* if it satisfies the two distributive laws:

1. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
2. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Recall, as we discussed in set theory, that a subset Y of a set X is said to be *closed downward* or a *down-set* if $y \in Y, z \leq y \Rightarrow z \in Y$. Notice that the union or intersection of two down-sets is a down-set.

Definition 30. The set of all down-sets of a poset P with the operations of union and intersection, is a distributive lattice with $0 = \varnothing$ and $1 = P$, denoted $L(P)$.

Theorem 61. *Let L be a finite distributive lattice. Then there is a finite poset P (uniquely determined by L) such that L is isomorphic to $L(P)$.*

5 A Hint of Algebraic Combinatorics

The most basic link between algebra and combinatorics is given by Cayley's Theorem:

Definition 31. A *permutation group* on a set X is a subgroup of the symmetric group S_X of all permutations of X. Every permutation group can be viewed as the set of automorphisms of some structure on X.

Theorem 62 (Cayley's Theorem)**.** *Any group G is isomorphic to a permutation group.*

Proof. Let X be the underlying set of G. Then each element g in G acts as a permutation on X by taking x to xg (where xg is defined as $x, g \in G$). In particular, this induces an injective homomorphism $\phi : G \to S_X$ given by $g \mapsto (x \mapsto gx)$, whence $G \cong \operatorname{im} \phi \leq S_X$. We call $\operatorname{im} \phi$ the *standard permutation representation* of G. □

5.1 Group Actions

Definition 32 (Group Actions)**.** The *action* of a group G on a set X is a homomorphism $\phi : G \to S_X$. Given such a homomorphism, we say that G acts on X. We abbreviate $\phi(g)(x)$ by $g \cdot x$.

Definition 33 (Orbits)**.** Suppose G is a group acting on X. Then define an equivalence relation $\equiv$ on X by the rule $x \equiv y$ if and only if $xg = y$ for some $g \in G$. The equivalence classes of this relation are called the *orbits* of the group G. The orbit containing an element x is denoted $G \cdot x$. If there is only one orbit, the action of G is called *transitive*.

Definition 34 (Coset Space)**.** The *coset space* $(G : H)$ is the set of right cosets of H in G. The coset *action* of G on $(G : H)$ is the natural one, given by the rule $(Hk)g = H(kg)$.

Proposition 63. *Any transitive action of G is equivalent to a coset action.*

Proof. Let G act transitively on the set X. Choose an arbitrary point $x \in X$ and let $H = \{g \in G \mid xg = x\}$ be the *stabilizer* of x, G_x. Then H is a subgroup of G and there is a natural bijection between X and $(G : H)$, namely:

$$\text{For each } y \in X \text{ let } S(y) = \{g \in G \mid xg = y\}. \text{ In particular, this is equal to } Hy.$$

This defines an equivalence of the actions of G, as if $yg = z$, $S(y)g = S(z)$. □

Proposition 64. *Two coset actions on $(G : H)$ and $G : K)$ are equivalent if and only if the subgroups H and K are conjugate.*

Theorem 65. *The number of inequivalent actions of the symmetric group S_3 on $\{1, \ldots, n\}$ is the same as the number of ways to express n as the sum of ones, twos, threes, and sixes.*

Proof. We will first consider the transitive actions. To do this, notice that up to conjugation, there are unique subgroups of order $1, 2, 3, 6$ in S_3 (and these are all subgroups of S_3). Thus, there is a unique transitive action on a set of size $1, 2, 3$, or 6.

Since an arbitrary action is made up of a disjoint union of these, the number f_n of different actions on $\{1, \ldots, n\}$ is equal to the number of ways of expressing n as a sum of ones, twos, threes, and sixes. □

5.2 Burnside's Lemma

Definition 35 (Stabilizer)**.** For any group G acting on a finite set X, the stabilizer of x (denoted G_x) is the set of elements in G fixing x, that is

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Proposition 66. *For any group G acting on a finite set X, G_x is a subgroup of G for any $x \in X$.*

Theorem 67 (Orbit-Stabilizer Theorem)**.** *Let G be a group which acts on a finite set X. Then, for any $x \in X$, the size of the orbit $G \cdot x$ of x is equal to the index of the stabilizer G_x.*

$$|G \cdot x| = [G : G_x]$$

Proof. Notice that $g, h \in G$ satisfy $g \cdot x = h \cdot x$ if and only if $gh^{-1} \in G_x$. Therefore, $g \cdot x = h \cdot x$ if and only if g and h are in the same left coset of G_x. Now, notice that each $y \in G \cdot x$ corresponds to the set of elements $g' \in G$ with $g' \cdot x = y$. Also, our above work shows that each of these sets correspond to a unique left coset of G_x. Therefore, each $y \in G \cdot x$ corresponds to a unique coset of G_x. □

Theorem 68 (Burnside's Lemma)**.** *Let G be a finite permutation group on a set X. For each element $g \in G$, we let X^g denote the set of elements in X fixed by g. Furthermore, we let X/G denote the set of orbits of G. Then,*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Proof. Notice that $\sum_{g \in G} |X^g| = |\{(x, g) \in X \times G \mid g \cdot x = x\} = \sum_{x \in X} |G_x|$. We use the orbit-stabilizer theorem to show that $\frac{|G|}{|G \cdot x|} = |G_x|$, whence our sum becomes:

$$\sum_{g \in G} |X^g| = |G| \sum_{x \in X} \frac{1}{|G \cdot x|}$$

But notice that the sum $\sum_{x \in X} \frac{1}{|G \cdot x|}$ is precisely the number of orbits of G, so indeed it is equal to $|X/G|$. Substituting this in and dividing both sides by G, we find the desired result:

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = |X/G|$$

□

Theorem 69. *There are $\frac{r^6 + 3r^4 + 12r^3 + 8r^2}{24}$ ways to color a cube with r colors if two colored cubes which differ by a rotation are considered identical.*

Proof. The symmetry group of rotations of the cube, C, is isomorphic to S_4. Its elements can be described by the following table:

Type	Axis	Order of Rotation	No. of elements
1	None	1	1
2	Face	2	3
3	Face	4	6
4	Edge	2	6
5	Vertex	3	8

For any $g \in C$, a coloring $x \in X$ is fixed by g if and only if all faces in the same cycle of g have the same color. Thus, if $c(g)$ is the number of cycles of an element g, the number of fixed colorings is $r^{c(g)}$. We use this to create the next table:

Type	$c(g)$	$\lvert X^g \rvert$	No. of elements	Part of Sum
1	6	r^6	1	r^6
2	4	r^4	3	$3r^4$
3	3	r^3	6	$6r^3$
4	3	r^3	6	$6r^3$
5	2	r^2	8	$8r^2$

Thus, by summing everything and dividing by 24 (the order of C), we get the desired polynomial $\frac{r^6+3r^4+12r^3+8r^2}{24}$. □

5.3 Cycle Indices

Definition 36 (Cycle Index)**.** Suppose we have an element g of a permutation group G acting on a set X with $|X| = n$. Further suppose the cycle decomposition of g has c_1 cycles of length 1 (fixed elements), c_2 cycles of length 2, and so on. Then the *cycle index* of g is the monomial:

$$z(g; s_1, \dots, s_n) = s_1^{c_1} s_2^{c_2} \dots s_n^{c_n}$$

Furthermore, the *cycle index* of the group G is the average of the cycle indices on its elements:

$$Z(G; s_1, \dots, s_n) = \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} s_i^{c_i(g)}$$

Now take a collection of 'figures' $\Phi = \{\phi_1, \phi_2, \dots\}$ with a natural number 'weight' function $w(\phi_i)$ such that there are only finitely many figures of any given weight. This gives us a figure-counting series

$$a(t) = \sum_{n \geq 0} a_n t^n$$

where a_n is the number of ϕ_i with $w(\phi_i) = n$. Next, we are given a permutation group G on X and we want to count the number of ways of associating a figure with each point of X in such a way that two configurations are identical if some element of G takes one to the other. For example, we could have the object being acted on being X and the figures being colors.

Precisely, an attachment of figures to points of X is a function $f : X \to \Phi$, with a total weight $w(f) = \sum_{x \in X} w(f(x))$. Now G acts on the set of functions by the rule $(fg)(x) = f(xg^{-1})$. We want to count the orbits of G on functions, which we do by means of the *function-counting series* $b(t) = \sum_{n \geq 0} b_n t^n$ where b_n is the number of orbits of G on functions of total weight n (as the action of G doesn't change the weights of the functions).

Theorem 70 (Cycle Index Theorem)**.**

$$b(t) = Z(G; a(t), a(t^2), \dots, a(t^n))$$

Lemma 71. *The cycle index of S_4 is $\frac{1}{24}(s_1^6 + 3s_1^2s_2^2 + 6s_1^2s_4 + 6s_2^3 + 8s_3^2)$.*

Lemma 72. *The cycle index of C_n is $\frac{1}{n}\sum_{d|n}\phi(d)s_d^{n/d}$.*

Theorem 73. *Thus there are $N_k = \frac{1}{n}\sum_{d|n}\phi(d)k^{n/d}$ necklaces of length n with k types of gems if two necklaces that can be rotated into each other are considered equivalent.*

6 Extras

6.1 Roots of Unity Filter

There is an extremely interesting problem-solving application called the *roots of unity filter*. We can use it (and the Binomial Theorem) to find the numbers of subsets whose size satisfies a certain size requirement. We saw a brief hint of this in the section on subsets of even and odd size, but we will further explore it here.

Proposition 74. *If n is a multiple of 8, then the number of sets of size divisible by 4 is $2^{n-2}+2^{(n-2)/2}$.*

Proof. Let A be the desired number and B be the number of sets whose size is congruent to 2 mod 4. Notice that $A + B$ is the number of all sets of even size, so $A + B = 2^{n-1}$.

Now substitute $t = i$ in the Binomial Theorem:

$$(1+i)^n = (\sqrt{2}e^{i\pi 4})^n = 2^{n/2} = \sum_{k=0}^{n}\binom{n}{k}i^k$$

By taking the real part of the right-hand side, we obtain that $A - B = 2^{n/2}$. This demonstrates that $A = 2^{n-2} + 2^{(n-2)/2}$ and $B = 2^{n-2} - 2^{(n-2)/2}$. Also, by noting that the imaginary part of the above sum is 0, we see that the number of subsets of size congruent to 1 mod 4 is equal to the number of subsets of size congruent to 3 mod 4 is equal to 2^{n-2}. □

Theorem 75 (The Roots of Unity Filter)**.** *If ζ is a primitive kth root of unity and $p(x)$ is a polynomial of the form $a_nx^n + a_{n-1} + \ldots a_1x + a_0$ (where n is a multiple of k), then:*

$$\frac{p(1) + p(\zeta) + \cdots + p(\zeta^{n-1})}{k} = a_0 + a_k + a_{2k} + \cdots + a_n$$

Consider the following practice problems:

Problem 3. The above theorem filters 0 mod k. Thus, consider how one can generalize our result to filter a mod k.

Problem 4. Use the roots of unity filter to come up with other estimates of the number of subsets of size congruent to 0 mod k for various k given that the whole set has size congruent to 0 mod $2k$.

6.2 Stirling's Formula

Theorem 76 (A Weaker Estimate for $n!$)**.** *As $n \to \infty$, $\log(n!) \sim n\log(n)$ (that is, their ratio approaches 1).*

Proof. Clearly $\log(n!) < n\log(n) = \log(n^n)$. Then consider the power series expansion of e^n, $\sum_{k\geq 0}\frac{n^k}{k!}$. Comparing e^n to the nth term in said series shows that $e^n > n^n/n!$, whence $n! > n^n/e^n$. Thus $\log(n!) > n\log(n) - n$, so we have the inequality:

$$n\log(n) - n < \log(n!) < n\log(n)$$

From here, a fairly obvious application of the squeeze theorem derives the desired result. □

Theorem 77 (Stirling's Formula)**.**

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

Proof. The full proof takes some pages, and is documented here. □

6.3 Error-Correcting Codes

Definition 37 (Hamming Space)**.** *Hamming Space* $H(n, q)$ is the set of all words of length n over the fixed alphabet Q of size q. We give $H(n, q)$ a metric, called *Hamming distance* between words v, w to be the smallest number of errors which could change v and w (that is, $d(v, w) = |\{i \mid v_i \neq w_i\}|$).

Proposition 78. *$H(n, q)$ is a metric space under Hamming distance: that is, $d(v, w) \geq 0$ with equality if and only if $v = w$, $d(v, w) = d(w, v)$, and $d(u, v) + d(v, w) \geq d(u, w)$.*

Definition 38 (Codes)**.** A *code* of length n over the alphabet Q is just a subset C of Hamming space $H(n, q)$ which contains at least two words. The elements of the code are called *codewords*.

Our idea is to perform error correction by restricting our transmissions to be members of the code C, rather than arbitrary words. If the members of C are sufficiently distinguishable, then, given just a few errors, we can recover the transmitted word.

Definition 39 (Nearest-Neighbor Decoding)**.** Nearest-neighbor decoding is done as so: if the word $w \in H(n, q)$ is received, we find the codeword $c \in C$ for which $d(w, c)$ is as small as possible. We assume that the transmitted word was c.

Definition 40 (Error-Correcting)**.** For a positive integer e, we say that the code C is *e-error-correcting* if, given any word w, there is at most one codeword c such that $d(w, c) \leq e$. In other words, the code $C \subseteq H(n.q)$ is e-error-correcting if and only if the balls of radius e with centres at the codewords are pairwise disjoint.

Proposition 79. *A code with minimum distance d (that is the smallest distance between two distinct codewords) is e-error-correcting if and if only $d \geq 2e + 1$.*

Proof. Trivial, left as an exercise for the reader. □

Definition 41 (Binary Symmetric Channel)**.** A *binary symmetric channel* is a channel using only the *binary alphabet* $\mathbb{F}_2 = \{0, 1\}$, with the following conditions:

1. For each digit, there is a probability $p < \frac{1}{2}$ that said digit is swapped to the other value.
2. This probability is equal for all digits and independent of the swapping of any other digits.

Definition 42 (Rate of a Code)**.** The *rate* of a code C of length n over an alphabet of size q is defined by be $\log_q(|C|)/n$. This is because if $|C| = q^k$ for some k, then k-tuples of information become n-tuples, so information is sent k/n times as fast as it would be otherwise.

Theorem 80 (Shannon's Theorem)**.** *Suppose we have a binary symmetric channel with error probability p for a single digit. Then:*

1. *If $R < 1 + p\log_2 p + (1 - p)\log_2(1 - p)$ and $\epsilon > 0$, there is a code with rate at least R such that the probability of error decoding a codeword by nearest-neighbour decoding is less than ϵ.*
2. *This is the best possible bound for R. Specifically, if R is larger than the bound, there is some $\epsilon > 0$ such that we can't find a code with rate at least R with failure rate less than ϵ.*

The proof is not offered here, but we encourage you to research it on your own.