Concrete Mathematics

Dr. Patrick White

Concrete Mathematics Class Spring 2019

Contents

Content By Lecture

0 Introduction

This is an archive of student notes from the Concrete Mathematics class from Spring 2019 at TJHSST, taught by Dr. Patrick White. Concrete Mathematics loosely takes from the textbook of the same name written by Donald Knuth, and teaches basic combinatorial techniques and constructions with the aid of calculus. Here, “concrete” is meant as a portmanteau of “discrete” and “continuous,” since we use both techniques to develop the theory (but obviously with a focus on solving discrete problems). The year I took the class Dr. White also covered some group theory and its application in combinatorics, which may or may not be the norm for this class.
This class doesn’t really exist anymore, but here’s hoping that this semi-static reference can serve as a historical marker as to what this class was like. It would be nice to see current students lobbying to bring it back, given that there is a staff member at TJ willing to teach this course again. Personally, this class was the class I credit for inspiring my current interest in combinatorics. Yes, enumerative combinatorics can seem like a grab-bag of tricks and little facts to know, and people from the math team will have a much easier time with the lines of thinking employed in this class. However, I think there is a rich theory here that is never really explored in competitive math or in the standard calculus pipeline in school, and this course offers a unique opportunity to get a glimpse into what combinatorics is like at an undergraduate level. As a bonus for the future CS majors, you’ll have to take a discrete math class anyway, and it’s likely more fun here in this setting than at wherever you end up. Regardless, this class was a great experience and I hope that this class returns someday.

0.1 Editing Notes

These notes were written by the class, with a rotating scribing system to record what happened in lectures every week, and were either transcribed or copied by me from the original saved tex/pdf sources. The previous page gives credit to the people who scribed for the class on which days. Here are my notes on editing:

- I tried to be faithful as possible to the source – either by essentially including the tex source as input or by transcribing the pdf as best as I could (while also potentially fixing some errors along the way).
- If two sets of notes existed on a day, contributions from both authors are kept in the repository, but the one in this main document is the one that I found to be more coherent/more thorough than the other.

All authors are still credited for every day, regardless if their words are the ones that are in the main document.

- There are some jumps in the dates listed on the previous page – Mondays sometimes don't exist? I don't really remember why to be honest... maybe no lectures happened those days because of quizzes or some other reason? Anyways, the dates are fairly arbitrary and can be safely ignored if you wish.
- Some contributors' graduation years/personal information may be wrong – I tried to put people's current preferred names and graduation years as I remembered them, but I'm not sure I got everyone right.

Errors, corrections, etc. are welcome and you can email me or submit a pull request if you like.

Part I
Enumerations

Consider the following common variety of counting problem:

Classic Problem. Suppose you have b balls and u urns. How many ways are there to put the balls into the urns, if:

the balls are:

1. labeled
2. unlabeled

the urns are:

1. labeled
2. unlabeled

and there can be:

1. **no** restrictions on the balls in the urns
2. **at most** one ball per urn
3. **at least** one ball per urn

This problem comes in 12 possible varieties! What happens when we have:

- 7 balls and 3 urns?
- 4 balls and 8 urns?

In time, we will be able to answer all 12 variants of each of these questions.

Remark. *This series of twelve problems for any b and u is called the* ***twelvefold way****, posed by Gian-Carlo Rota.*

1 Basic Notation

If A is a set, then we define:

$\lvert A\rvert$ or $\#\{A\}$	represents the (finite) number of elements in the set, known as the *magnitdue*, *length*, *size*, or *cardinality* of that set
$A \cap B$	*intersection* (command in LaTeX is \cap)
$A \cup B$	*union* (command in LaTeX is \cup)
$\overline{A}$	*complement*, given by $\{x \mid x \notin A\}$
$A \setminus B$	*minus*, given by $\{x \mid x \in A, x \notin B\}$; sometimes written as $A - B$
$x \in A$	set inclusion (x is an *element* of A)
$A \subseteq B$	A is a *subset* of B ($x \in A \implies x \in B$)
$A \subsetneq B$	A is a *proper subset* of B ($A \subseteq B, A \neq B$)
$\varnothing$	empty set
2^A or $\mathcal{P}(A)$	*power set* of A: set of all subsets of A, including A and $\varnothing$

2 Counting Strategies

2.1 Basic Combinatorics

Theorem 2.1. $|2^A| = 2^{|A|}$

Proof. We begin with an example.

$$\mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Notice that the number of subsets is indeed $2^3 = 8$.

Many problems in combinatorics are best solved by isomorphic counting; we rephrase the problem into something easier to count. Let us consider the binary functions on A, $f : A \to \{0,1\}$. Notice that each f can be uniquely represented with a binary string, which in turn represents a way to make a subset of A

$$\begin{aligned} 001 &\to f(1) = 0,\ f(2) = 0,\ f(3) = 1 \to \{3\} \\ 110 &\to f(1) = 1,\ f(2) = 1,\ f(3) = 0 \to \{1,2\} \end{aligned}$$

Thus, $|2^A|$ is equinumerous to the number of binary numbers of length $|A|$, or $2^{|A|}$.

■

Theorem 2.2. *If $A \subseteq B$ and $B \subseteq A$, then $A = B$*

Theorem 2.3 (Principle of Inclusion-Exclusion). $|A \cup B| = |A| + |B| - |A \cap B|$

The Principle of Inclusion-Exclusion may be applied repeated to count the cardinality of unions of more than two sets:

$$|A \cup B \cup C| = |A| + |B| + |C| - |AB| - |BC| - |AC| + |ABC|$$

Note that when it's clear what we're talking about, we can abbreviate $A \cap B$ as AB.

Problem. Prove that, for $m, n \in \mathbb{N}$ selected uniformly at random

$$P(\gcd(m, n) = 1) = \frac{6}{\pi^2}$$

Theorem 2.4 (Multiplication Theorem). *Given sets $A_1, A_2, \ldots A_n$, the number of ways to select an element from each set is $|A_1||A_2| \ldots |A_n|$.*

> *Proof.* Draw a multitree with root nodes in A_1 and let each node $x \in A_i$ have as its children A_{i+1}. As you traverse from root to leaf, each decision you make corresponds to a selection from that set, and the number of paths from root to leaf is $|A_1||A_2| \ldots |A_n|$.
>
> ■

Corollary. If $|A| = n$, we can select k of these elements, with repetition, in n^k ways.

Corollary. If $|A| = n$, we can select k of these elements, without repetition, in $n(n-1)(n-2)\ldots(n-k+1)$ ways.

We will notate the above expression as

$$n(n-1)(n-2)\ldots(n-k+1) = {}_nP_k = {}^nP_k = n^{\underline{k}}$$

The final notation will be the most commonly used in this class. This is called the "falling factorial". Similar, we can define a "rising factorial":

$$n^{\overline{k}} = (n)(n+1)\ldots(n+r-1)$$

Problem 1. How many passwords with only capital letters or digits contain 8, 9, 10 characters, barring repeated characters?
Answer: $36^{\underline{8}} + 36^{\underline{9}} + 36^{\underline{10}}$

Problem 2. How many passwords with only capital letters or digits containing at least 1 digit and 1 letter contain 8, 9, or 10 characters, barring repeated characters?
Answer: $(36^{\underline{8}} + 36^{\underline{9}} + 36^{\underline{10}}) - (26^{\underline{8}} + 26^{\underline{9}} + 26^{\underline{10}}) - (10^{\underline{8}} + 10^{\underline{9}} + 10^{\underline{10}})$

Problem 3. How many passwords with only capital letters or digits contain 8 characters and have capital letters in even-numbered spaces (the 0th position, the 2nd position, and so on), allowing for repitition of characters? *Answer:* $5^4 * 36^4$

Problem 4. How many divisors does the number 496 have? What about the number 360?

Solution Consider the prime factorizations of these numbers:

$$496 = 31 \cdot 2^4 \qquad 360 = 5 \cdot 3^2 \cdot 2^3$$

A divisor of these numbers is created by choosing a possible number of prime factors that divide the original number. For example, a divisor of 496 can have either 0 or 1 factors of 31, and anywhere from 0 to 4 factors of 2. Then the number of divisors of 496 is $(1 + 1)(4 + 1) = 10$, and similarly, the number of divisors of 360 is $(1 + 1)(2 + 1)(3 + 1) = 24$, following from the Multiplication Theorem. ■

Problem 5. What are the sum of the divisors of 496 and 360? The "sum of all divisors" function is denoted $\sigma(n)$.

Solution Using a modification of the Multiplication Theorem, note that the multiplication operation encodes the idea of "all possible ways of combining two things." As such, if we consider the sum of all of the different prime powers that can appear in any divisor and multiply them together, we will create a term with every divisor, added together. For instance, the sum of the divisors of 496 is:

$$\sigma(496) = (1 + 31)(1 + 2 + 4 + 8 + 16) = 32\dot{3}1 = 992$$

and similarly

$$\sigma(360) = (1 + 5)(1 + 3 + 9)(1 + 2 + 4 + 8) = 6 \cdot 13 \cdot 15 = 1170.$$

■

Remark. *If we consider the sum of all proper divisors of a positive integer n ($\sigma(n) - n$), we can classify integers into three categories based on how $\sigma(n) - n$ compares to n:*

- *If $\sigma(n) - n < n$, then n is deficient.*
- *If $\sigma(n) - n > n$, then n is abundant.*

- *If $\sigma(n) - n = n$, then n is perfect.*

In the example above, note that 360 is abundant and 496 is perfect.
Finding perfect numbers is actually an incredibly difficult problem in number theory – in fact, nobody even knows if there exists perfect numbers that are odd! In the even case, though, Euler showed that perfect numbers are of the form $2^{p-1}(2^p - 1)$ if $2^p - 1$ is prime (which requires p itself to be prime also). Primes of the form $2^p - 1$ are called ***Mersenne primes****, and it is not even known if there are infinitely many of these primes! Only 51 Mersenne primes are known to exist as of 2023, so we only know of 51 perfect numbers.*

2.2 Quotient Sets

Problem. Let us count the number of permutations of "ABCD". There are 24 permutations of this string of length 4 (e.g. ABCD, ABDC, ...). There are also 24 permutations of length 3 (e.g. ABC, ABD, ...) Let define equivalence relationship $p_1 \cong p_2$ if they contain the same letters (e.g. ACB $\cong$ ABC). Define an *equivalence class* C to be such that $p_1, p_2 \in C \implies p_1 \cong p_2$. How many equivalence classes are there out of the 24 permutations of length 3?

Solution There are 4 equivalence classes. Note the following:

1. All equivalence classes are of the size same size, 3!
2. Different equivalence classes are disjoint
3. The set of all equivalence classes forms a partition of the set of all $4^{\underline{3}}$ permutations of length 3.

Thus, there are $4^{\underline{3}}/3!$ equivalence classes. ■

By noticing that equivalence classes are of size $r!$, we can now count *combinations.*

$$_nC_r = \frac{_nP_r}{r!}$$

2.3 Partitions

A *partition* of a set S is a subset of $S_1, ...S_k$ such that

(i) $\bigcup_{i=1}^{k} S_i$. The subsets 'cover' the set S

(ii) $S_i \cap S_j = \varnothing$. The subsets are pairwise disjoint.

(iii) $S_i \neq \varnothing$

Problem 1. Let S be the set of all integers composed of digits in $\{1, 3, 5, 7\}$ at most one.

(i) Find $|S|$

(ii) $\sum\limits_{x \in S} x$

Solution

(i) Let $S = S_1 \cup S_2 \cup S_3 \cup S_4$ where S_1 is the number of one digit numbers, S_2 is the number of two-digit numbers, and so on.

$$\begin{aligned} |S_1| &= {}^4P_1 = 4 \\ |S_2| &= {}^4P_2 = 12 \\ |S_3| &= {}^4P_3 = 24 \\ |S_4| &= {}^4P_4 = 24 \\ |S| = |S_1| + |S_2| + |S_3| + |S_4| &= \boxed{64} \end{aligned}$$

(ii) Let $\alpha = \alpha_1 + 10\alpha_2 + 100\alpha_3 + 1000\alpha_4$ where α_1 is the sum of all units digits of all numbers in S, α_2 is the sum of all the tens digits of all the numbers, and so on. We will find the value of α_1 using the following:

$$\begin{array}{l} S_1 \to s_1 = (1+3+5+7) \\ S_2 \to s_2 = (1+3+5+7) \times (3) \\ S_3 \to s_3 = (1+3+5+7) \times (3 \times 2) \\ S_4 \to s_4 = (1+3+5+7) \times (3 \times 2 \times 1) \\ \hline \alpha_1 = 16 \times (1+3+6+6) = 256 \end{array}$$

Note that α_2 is the sum of the same values, excluding s_1 as S_1 is the set of only one digit numbers. α_3 is the sum of the same values as α_2, excluding s_2 as S_2 is the set of only two digit numbers, and so on.

$$\begin{aligned} \alpha_2 &= \alpha_1 - s_1 = 240 \\ \alpha_3 &= \alpha_2 - s_2 = 192 \\ \alpha_4 &= \alpha_3 - s_3 = 96 \end{aligned}$$

Thus, $\alpha = \alpha_1 + 10\alpha_2 + 100\alpha_3 + 1000\alpha_4 = \boxed{117,856}$

An easier solution is the following:

$$1+3+5+7=(1+7)+(3+5)=8(\frac{4}{2})=16$$
$$13+...+75=(13+75)+...+(35+53)=88(\frac{12}{2})=528$$
etc

Since each $x \in S_i$ pairs with $\bar{x} \in S_i$ to sum to $88...8$. We find $\alpha = 8\frac{|S_1|}{2}+88\frac{|S_2|}{2}+888\frac{|S_3|}{2}+8888\frac{|S_4|}{2} = \boxed{117,856}$

■

2.4 Cyclic Permutation

Consider the set T of 3 permutations of (s_1, s_2, s_3, s_4) or $(1,2,3,4)$. We know that $T = \{123, 132, 234, 214, ...\}$ and $|T| = P(4,3) = 24$.

We define $x \cong y \iff x+y$ are cyclically equivalently

Problem 1. Given 123 $\cong x$, how many solutions are there for $x \in T$?

Solution The x values are 123, 231, 312, so there are $\boxed{3}$ solutions. Thus, we see any sequence of length $n \cong n$ sequences ■

Theorem 2.5. *If $Q(n,r)$ is the number of cyclic permutations of length r from a set of n elements, $Q(n,r) = \frac{P(n,r)}{r}$.*

Theorem 2.6. *There are (n-1)! ways to seat n people around a round table.*

Proof. Each ordering $\cong n$ orderings. Thus, $\frac{n!}{n} = (n-1)!$

■

Problem 2. There are 5 boys and 3 girls seated around a round table.

(i) There are no restrictions.

(ii) B_1 and G_1 are not adjacent

(iii) No girls are adjacent to other girls

Solution

(i) Using theorem 2.1, there are $\boxed{7!}$ ways.

(ii) We first place B_1 in any of the 7 seats and set B_1 as our reference point. There are then 5 places for G_1 to sit not adjacent to B_1 and 6! ways for the remaining 6 people to sit. The total number of ways if $\boxed{6! \cdot 5}$. We can also consider the number of ways for B_1 and G_1 to sit next to each other, which is $2 \cdot 6!$. Subtracting that from arranging without restrictions, the total number of ways is $\boxed{7! - 2 \cdot 6!}$

(iii) We first arrange all the 5 boys, which is $4!$ ways. There are 5 spaces between each boy, so we can choose 3 of the seats and then arrange the 3 girls, $\binom{5}{3} \cdot 3!$. The total number of ways is $\boxed{4! \cdot \binom{5}{3} \cdot 3!}$

■

One possible "bogus solution" to this last problem:
Solution Arrange the boys in a line in 5! ways, choose three of the boys to put girls to the left of, and arrange the girls in 3! ways. *We then divide by 8 in order to account for the cyclicity of the table.* ■
Recall, however, the **reason** we divided by 8 to begin with is to divide by the size of each of the equivalence groups in the original problem when arranging people around the table. There are **not** 8 elements in each of these equivalence groups - cyclical arrangements with a girl on the very right is not part of set that we counted. In fact, there are only 5.

2.5 Recursion

Another way to count a set is to recursively generate it from smaller cases. This is a very useful general strategy to compute a quantity.

Exercise 1. Find the recursive definition of $P(n, r)$.

Solution We know that the closed form of $P(n, r) = \frac{n!}{(n-r)!}$. Our goal is to define $P(n, r) = f(P(< n, < r))$.
Let $S = \{s_1, ..., s_n\}$, r be given $0 \leq r \leq n$, and T be the set of all r-permutations of S. We can partition T into $T = T_1 \cup T_2$ where

$$t = T_1 \Leftrightarrow s_1 \notin t \text{ (no } s_1)$$
$$t = T_2 \Leftrightarrow s_1 \in t \text{ (yes } s_1)$$

We can find the $|T_1|$ in terms of $P(\leq n, \leq r)$

$$|T_1| = P(n-1, r)$$
$$|T_2| = r \cdot P(n-1, r-1)$$

For $|T_2|$, we can order $r-1$ elements from $\{s_2, ..., s_n\}$ and place s_1 in any of the r locations. Thus, $\boxed{P(n, r) = P(n-1, r) + r \cdot P(n-1, r-1)}$ ■

Exercise 2. Find a recursive definition of $C(n, r)$

Solution Again, let T be the subset of $S = \{s_1, ..., s_n\}$ of size r.
To find $|T|$, let $T = T_1 \cup T_2$ where T_1 has no set containing s_1 and T_2 has every set containing s_1.

$|T_1| = C(n-1, r)$ we can choose r from $s_2, ...s_n$

$|T_2| = C(n-1, r-1)$ we choose $r-1$ from $s_2, ...s_n$ and add in s_1

Thus, $\boxed{C(n, r) = C(n-1, r) + C(n-1, r-1)}$ ■

Problem 1. Given $2n$ tennis players. How many ways are there to arrange n games/pairings?

Solution There are several solutions to this problem:

1. We can match P_1 with another $2n-1$ players. For the next player P_2 who hasn't been matched, we can choose $2n-3$ players, and so on. The solution is just $(2n-1)(2n-3)...(1) = \boxed{(2n-1)!!}$
2. We can choose each pair and divide by $n!$ to remove the ordering of the pairs. There are $\boxed{\frac{\binom{2n}{n}\binom{2n-2}{2}...\binom{2}{2}}{n!}}$ ways.
3. We can permute all $2n$ players and divide by $n!$ (the number of ways to order the game doesn't matter) and 2^n (the order of the partners doesn't matter). There are $\boxed{\frac{(2n)!}{n!2^n}}$

■

2.6 Interlude: Points in the Plane

Here is a difficult but interesting problem from the International Mathematical Olympiad that uses the counting techniques we have encountered thus far, but in a creative manner:

Problem 1. (IMO 1989/3) Given $n, k \in \mathbb{Z}^+$, let S be a set of n points in the plane such that no three points of S are collinear, and for any point P of S there are at least k points of S equidistant from P. Prove that

$$k < \frac{1}{2} + \sqrt{2n}$$

Proof. Draw an edge between points P and Q if P and Q are one of the k points that are equidistant from another point O. We will count all such edges between all pairs of points. One way to do so is simply choose any two of the points as an upper bound, which can be done in $\binom{n}{2}$ ways.
The other way we can do so is by counting edges among the points equidistant from a point P. We can compute all pairs of edges between these equidistant points, which gives at least $\binom{k}{2}$ edges. Across all points, this gives at least $n\binom{k}{2}$. However, we have overcounted - notice that at a maximum, each edge can represent an intersection between two circles representing equidistant sets of points around each point. If this edge was the intersection of three or more of these circles, this would give at least three points in S as collinear, which is forbidden. This means that we have overcounted by at most $\binom{n}{2}$. This method of counting may not have accounted for all the edges (i.e. it's a lower bound). Combining these two gives the inequality

$$\binom{n}{2} \geq n\binom{k}{2} - \binom{n}{2}$$

Expanding, we have:

$$\begin{gathered}2 \cdot \frac{n(n-1)}{2} \geq \frac{nk(k-1)}{2} \\ n-1 \geq \frac{k^2-k}{2} \\ n \geq 1 + \frac{4k^2-4k}{8} > \frac{4k^2-4k+1}{8} \\ 8n > (2k-1)^2 \\ 2\sqrt{2n} > 2k-1 \\ k < \frac{1}{2} + \sqrt{2n}\end{gathered}$$

as desired.

■

3 Combinatorial Sequences

3.1 Binomial Coefficients

Recall we derived a recursive definition of combinations (ie. binomial coefficients) in the last lecture:

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

This is also known as **Pascal's Identity**.
We now prove the famed **Binomial Theorem**:

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

While proving this fact, we will extend the definition of the combination (or binomial coefficient) as follows:

$$\binom{n}{k} = \begin{cases} \frac{n^{\underline{k}}}{k!} & 0 \le k \le n \\ 0 & k > n, k < 0 \end{cases}$$

We will prove this in two ways - first by induction and then by a simple combinatorial argument.

Proof 1. First, let us consider the trivial base case for $n = 0$, for which $(x+y)^0 = 1$ which is easily true, as $\binom{0}{0} = 1$.
For the inductive step, we can consider $(x+y)^{n+1}$ as $(x+y)(x+y)^n$, and apply the Binomial Theorem to the $(x+y)^n$ term. We expand:

$$\begin{aligned}(x+y)(x+y)^n &= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k} \\ &= \sum_{k=1}^{n+1}\binom{n}{k-1}x^k y^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}\end{aligned}$$

where we shift the indices of the first sum back so the exponents of the x and y terms match up. We will now extend the bounds of each of the sums by one in order to combine them together into one sum - this is legal, as the terms that we are adding are zero by our extended definition of the binomial coefficient.

$$\sum_{k=0}^{n+1}\binom{n}{k-1}x^k y^{n+1-k} + \sum_{k=0}^{n+1}\binom{n}{k}x^k y^{n+1-k}$$

Now we finish using Pascal's Identity:

$$\sum_{k=0}^{n+1}\left(\binom{n}{k-1}+\binom{n}{k}\right)x^k y^{n-k} = \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n-k}$$

■

Proof 2. We can write the product $(x+y)^n$ out explicitly:

$$(x+y)^n = \overbrace{(x+y)(x+y)\dots(x+y)}^{n}$$

Notice that the term $x^k y^{n-k}$ appears $\binom{n}{k}$ times, which immediately implies the desired as we sum over all possible k.

■

Reflection A. Notice how much cleaner the combinatorial argument was! We will appeal to such arguments again and again as the course progresses.

What if we want to expand something like $(1-x)^{\frac{1}{2}}$ binomially? This forces us to define binomial coefficients when the top argument is a real α - and furthermore, we have to define them in such a way so that it doesn't involve factorials of α (which aren't well defined). We can define as follows for $\binom{\alpha}{n}$ if n is an integer, but α can be any real:

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-n+1)}{n!} = \frac{\alpha^{\underline{n}}}{n!}$$

Once this is done, we can simply apply the Binomial Theorem, which turns out still to be true with this definition, except the sum does not terminate (left to the reader as an exercise):

$$\begin{aligned}(1-x)^{\frac{1}{2}} &= \sum_{k=0}^{\infty}\binom{\frac{1}{2}}{k}(-x)^k \\ &= 1 + \frac{\frac{1}{2}}{1!}(-x)^1 + \frac{\frac{1}{2}\left(-\frac{1}{2}\right)}{2!}(-x)^2 + \frac{\frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)}{3!}(-x)^3 + \dots \\ \implies (1-x)^{\frac{1}{2}} &= 1 - \sum_{n=0}^{\infty}\frac{(2n-1)!!}{(n+1)!2^{n+1}}x^{n+1}\end{aligned}$$

where we define $(-1)!! = 1$.

Recall we had this double factorial last class, and in fact we showed that $(2n-1)!! = \frac{(2n)!}{2^n n!}$ by solving the same combinatorial problem of creating games in a tournament. Applying this, we obtain

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

Remark. *The term $\binom{2n}{n}\frac{1}{n+1}$ is the nth **Catalan number**. We will see these numbers again in the near future.*

3.2 Multisets and Problems with Repetition

We will now start to look at problems where we can have repetition of elements. Consider the following problems:

Problem 2. Given the elements of the set $\{a, b, c, d\}$, how many ways are there to construct a sequence of length 7 with repetition allowed?

Solution. For each element in the sequence, we can choose any element in the set, giving $\boxed{4^7}$ possibilities.

■

Problem 3. Given the multiset $\{3 \cdot a, 2 \cdot b, 5 \cdot c\}$, how many unique sequences are there that use all the letters once?

Solution. If we first label the as, bs, and cs so that they are distinguishable, we can arrange all the letters in $10!$ ways to begin with. However, since all of the as are indistinguishable, permuting the order of the labeled as produces an equivalent arrangement - so we must divide by a factor of $3!$. We must do the same thing for the bs and cs, giving $\boxed{\dfrac{10!}{3!2!5!}}$ sequences.

■

Problem 4. Given the multiset $\{\infty \cdot a, \infty \cdot b, \infty \cdot c, \infty \cdot d\}$, how many ways can one choose a sub-multiset of size 7?

Solution. Notice that we only care about the quantities of each of the letters a, b, c, d, so we can consider the equivalent problem of finding the number of positive-integer solutions to the equation $w + x + y + z = 7$. This can be counted by considering the isomorphic problem of counting binary strings of length 10 with three 1s. To see why this problem is the same as counting solutions to the equation, notice that for every such binary string, we can let the number of 0s to the left of the first 1 be the value of w, the number of 0s between the first and second 1s be the value of x, etc. This uniquely maps this binary string to a solution to this Diophantine equation, and similarly every solution to the equation gives a binary string. We can count the strings easily - there are $\boxed{\binom{10}{3}}$ of these strings, which is the answer to the original problem as well.

■

We can generalize this last problem: with the same reasoning, we find the number of ways to build a size-r multiset from n possible elements is $\binom{n-1+r}{n-1} = \binom{n-1+r}{r}$.
We now define some additional notation for these kinds of problems:

- We denote the number of multisets into a sequence as a *multinomial coefficient*:
$$\binom{n}{r_1, r_2, \ldots r_k} = \frac{n!}{r_1!r_2!\ldots r_k!}$$
where $n = \sum_i r_i$.

- The number of multisets of length r constructed from n possible elements (colloquially known as the *stars and bars* problem) is denoted as
$$\left(\!\!\binom{n}{r}\!\!\right) = \binom{n-1+r}{n-1} = \binom{n-1+r}{r}$$
For example, $\left(\!\binom{3}{7}\!\right) = \binom{3-1+7}{2} = \binom{9}{2} = 36$. Note that unlike binomial coeffients, n need not be less than r!

3.3 Partitions and Stirling Numbers

Problem 1. How many ways can a set of 4 elements be partitioned into 2 non-empty sets?

Solution: We perform casework. Here are the ways:

$$1\,|\,2\,3\,4 \quad 2\,|\,1\,3\,4 \quad 3\,|\,1\,2\,4 \quad 4\,|\,1\,2\,3$$

$$1\,2\,|\,3\,4 \quad 1\,3\,|\,2\,4 \quad 1\,4\,|\,2\,3$$

■

Definition. *The number of ways to partition a set of n elements into k non-empty subsets is the **Stirling Number of the second kind** $S(n,k)$ or $\left\{ n \atop k \right\}$.*

Let's construct a few base cases:

$$\begin{aligned}
&S(1,1) = 1\\
&S(n,1) = 1\\
&S(n,n) = 1\\
&S(0,0) = 1 \quad \text{(defined as such)}\\
&S(n,2) = 2^{n-1} - 1\\
&S(n,n-1) = \binom{n}{2}
\end{aligned}$$

The first four of these are fairly trivial to see, but the last two are not.

Proposition A. $S(n,2) = 2^{n-1} - 1$

Proof. Consider $A = \{0,1\}^n$. This will be the characteristic function of membership in the two sets S_0, S_1. Note that $|A| = 2^n$, but 1^n and 0^n are not valid partitions (since they have an empty set). So we have $|A| = 2^n - 2$ valid mappings. However, since we are double counting because the identity of the subsets are irrelevant, we divide by 2 to yield $2^{n-1} - 1$. ■

Proposition B. $S(n,n-1) = \binom{n}{2}$.

Proof. Choose two elements from the n that will be in the same set, and each of the rest of the elements must be in its own set. ■

With these base cases in mind, we can look at constructing a recursive formula for $S(n,k)$. We can start by looking at the partitions of an $n-1$-element set into $k-1$ elements - and the nth element must go into a new set by itself. Alternatively, we can consider $S(n-1,k)$, or the partitions of an $n-1$-element set into k-elements, and we must pick which one of the sets the last element must go into in k ways. This gives us the recursive formula

$$S(n,k) = S(n-1,k-1) + kS(n-1,k)$$

We can now begin computing values of the Stirling numbers of the second kind:

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	1	1	0	0	0	0
3	1	3	1	0	0	0
4	1	7	6	1	0	0
5	1	15	25	10	1	0
6	1	31	90	65	15	1

3.4 Revisiting Balls and Urns

We actually now have most of the information we need to understand the twelvefold way! If we have b balls and u urns, here are the number of ways to put the balls in the urns (subject to either no restrictions, or putting at least 1 in each/at most 1 in each):

B	U	$\varnothing$	≤ 1 per	≥ 1 per
labeled	labeled	u^b	$u^{\underline{b}}$	$u!\left\{ {b \atop u} \right\}$
unlabeled	labeled	$\left(\!\!\binom{u}{b}\!\!\right)$	$\binom{u}{b}$	$\left(\!\!\binom{u}{b-u}\!\!\right)$
labeled	unlabeled	$\sum_{n=1}^{u} \left\{ {b \atop n} \right\}$	$[b \leq u]$	$\left\{ {b \atop u} \right\}$
unlabeled	unlabeled	?	$[b \leq u]$	?

A few notes on some of these cases:

- unlabeled balls into labeled urns, ≥ 1 per: fill the urns with at least one ball each first, then do the multisets. This also has the name of a "composition of b into u parts."
- $[P]$ means 1 if P is true, and 0 otherwise. This appears for labeled balls unto unlabeled urns, ≤ 1 per urn – either we can do it, or there are no ways to do it. Same with unlabeled balls into unlabeled urns.

3.5 More on Stirling Numbers of the Second Kind

Recall one of the problems from the first day involving putting labeled balls into labeled urns, with the condition that there is at least one ball in each urn (but for consistency, we will use n nuggets and k kettles). For n nuggets and k kettles, we partitioned the n nuggets into k sets in $S(n,k)$ ways, and then labeling the sets in $k!$ ways, giving a total of $k! \cdot S(n,k)$, where $S(n,k)$ is a *Stirling number of the second kind*.

We can actually solve this problem in an alternative method is by using the Principle of Inclusion-Exclusion. We can first count the total number of ways we can place the nuggets into the kettles with no restrictions, and then remove the possibilities that have various numbers of empty kettles.

Specifically, we subtract off the possibilities of placing n nuggets into (at most) $k-1$ kettles, and then adding back possibilities of placing n nuggets into $k-2$ kettles, as they have been subtracted off one extra time, etc. We can continue in this manner until we have added/subtracted back the possibility of n nuggets into zero kettles, which concludes all the possible cases. Let's construct a specific expression for each of these cases. Notice that if we limit ourselves to j kettles to put the nuggets into, we only have j options for each nugget, so we only have j^n possibilities. We also have to account for the number of ways we can choose these kettles, which can be done in $\binom{k}{j}$ ways.
This argument leads to the following equivalent expression for the number of ways we can place these nuggets in the kettles:

$$k^n - \binom{k}{k-1}(k-1)^n + \binom{k}{k-2}(k-2)^n - \ldots + (-1)^k\binom{k}{0}0^n = k!S(n,k)$$

or more compactly,

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n = k!S(n,k).$$

This gives us the following closed form for the Stirling numbers of the second kind:

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n$$

3.6 Stirling Numbers of the First Kind

With this (or the recurrence relation from last class) we can fill in the following table of Stirling numbers of the second kind (with blank entries taken to be 0). Notice how we can run the recurrence relation backwards to get the entries in the top left:

n, k	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
-7	1														
-6	21	1													
-5	175	15	1												
-4	735	85	10	1											
-3	1624	225	35	6	1										
-2	1764	274	50	11	3	1									
-1	720	120	24	6	2	1	1								
0								1							
1									1						
2									1	1					
3									1	3	1				
4									1	7	6	1			
5									1	15	25	10	1		
6									1	31	90	65	15	1	
7									1	63	301	350	140	21	1

The numbers in the upper triangle are the **unsigned Stirling numbers of the first kind**, denoted $\left[{n \atop k}\right]$. Some authors may or may not multiply these numbers in the top left triangle by $(-1)^{n+k}$, giving the **signed Stirling numbers of the first kind** $s(n, k)$. We will use the following theorem (that we will prove later) as a "definition" for the unsigned Stirling numbers of the first kind:

Theorem 3.1 (Stirling Numbers of the First Kind). *For $n, k \in \mathbb{Z}$, we have:*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{Bmatrix} -k \\ -n \end{Bmatrix}$$

This follows straight from the table that we developed, but we will develop these numbers more rigorously from a recursion relation and then prove this identity later. For now, we will investigate some interesting properties relating the Stirling numbers of the first and second kinds.
To begin, consider the expansions of the falling factorials:

$$\begin{aligned}
x^{\underline{1}} &= 1x \\
x^{\underline{2}} &= x(x-1) = 1x^2 - 1x \\
x^{\underline{3}} &= x(x-1)(x-2) = 1x^3 - 3x^2 + 2x \\
x^{\underline{4}} &= x(x-1)(x-2)(x-3) = 1x^4 - 6x^3 + 11x^2 - 6x \\
&\vdots
\end{aligned}$$

Notice that the coefficients of the polynomials are the (signed) Stirling numbers of the first kind! To be explicit, $(-1)^{n+k}\left[{n \atop k}\right]$ or $s(n, k)$ is the coefficient of the x^k term in the expansion of the falling factorial. We can also express polynomial terms x^n in terms of the falling factorials:

$$\begin{aligned}
x &= 1x^{\underline{1}}\\
x^2 &= 1x^{\underline{2}} + 1x^{\underline{1}}\\
x^3 &= 1x^{\underline{3}} + 3x^{\underline{2}} + 1x^{\underline{1}}\\
x^4 &= 1x^{\underline{4}} + 6x^{\underline{3}} + 7x^{\underline{2}} + 1x^{\underline{1}}\\
&\vdots
\end{aligned}$$

From this we see that the coefficient of $x^{\underline{k}}$ in the falling-factorial expansion of x^n is $S(n,k)$.

On a seemingly unrelated note, we can consider lower triangular $n \times n$ matrices built from these numbers, $S_1(n)$ and $S_2(n)$, such that for each entry in these matrices, $S_1(n)_{ij} = s(i,j)$ and $S_2(n)_{ij} = S(i,j)$. Below are $S_1(4)$ and $S_2(4)$:

$$S_1(4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 2 & -3 & 1 & 0 \\ -6 & 11 & -6 & 1 \end{bmatrix} \quad S_2(4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 3 & 1 & 0 \\ 1 & 7 & 6 & 1 \end{bmatrix}$$

Consider what happens when we take $S_1(4)S_2(4)$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 2 & -3 & 1 & 0 \\ -6 & 11 & -6 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 3 & 1 & 0 \\ 1 & 7 & 6 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4$$

In general, the matrices $S_1(n)$ and $S_2(n)$ multiply to I_n, meaning that $S_1(n)$ and $S_2(n)$ are inverses of each other.

What do these two facts have to do with each other? At a deeper level, the Stirling numbers are the coefficients of the coordinate transformations between the basis of polynomial terms and basis of falling factorials. That is, we can use the Stirling numbers of the first kind to transform ”polynomials” expressed in terms of the falling factorials into polynomials in the normal sense, and similarly we can use the Stirling numbers of the second kind to transform polynomials into corresponding ”polynomials” in terms of falling factorials. The matrix discussion above reflects this property of the Stirling numbers - the triangular matrices $S_1(n)$ and $S_2(n)$ being inverses is no coincidence, as it shows how these transformations are inverses of each other.

This discussion gives us three identities involving S and s:

1. $$x^n = \sum_{k=1}^{n} {n \brace k} x^{\underline{k}}$$

2. $$x^{\underline{n}} = \sum_{k=1}^{n} (-1)^{n+k} {n \brack k} x^k$$

3. $$\sum_{k=1}^{\max(n,m)} S(n,k)s(k,m) = \delta_{mn}$$

.

where δ_{mn} is the *Kronecker delta*, defined as follows:

$$\delta_{mn} = \begin{cases} 0 & m \neq n \\ 1 & m = n \end{cases}$$

Problem 1. Prove $\sum_{j=0}^{n} {n \brace k} {j \brack k} = \delta(n,k)$

Solution We are given:
1. $x^n = \sum_{j=0}^{n} {n \brace j} x^{\underline{j}}$
2. $x^{\underline{j}} = \sum_{k=0}^{j} {j \brack k} x^k = \sum_{k=0}^{n} {j \brack k} x^k$
For this second part, we can increase the upper bound because all values for which $n > j$ are just equal to 0.
Plugging Equation 2 into Equation 1, we get...
$x^n = \sum_{j=0}^{n} {n \brace j} \sum_{k=0}^{n} {j \brack k} x^k$
Because j is independent of the inner sum, we can actually switch the order and move both sums to encapsulate the entire expression.
$x^n = \sum_{j=0}^{n} \sum_{k=0}^{n} {n \brace j} {j \brack k} x^k$
The sum basically represents adding the rows of a matrix vs adding the columns of a matrix, which basically proves the statement and we get... $\sum_{j=0}^{n} {n \brace k} {j \brack k} = \delta(n,k)$ ■

3.7 Combinatorics of the Stirling Numbers of the First Kind

Let's look back at our recurrence relation for the Stirling numbers of the second kind:

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}$$

Note the similarity between this and the other two recurrence relations we have seen thus far for permutations and combinations:

$$\text{Permutations: } P(n,k) = kP(n-1,k-1) + P(n-1,k)$$
$$\text{Combinations: } \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Let us construct another recurrence relation in a similar form to $f(n,k) = af(n-1,k-1) + b(n-1,k)$, and see what the function counts. Consider the recurrence relation

$$f(n,k) = f(n-1,k-1) + (n-1)f(n-1,k).$$

Proposition 1. The number of ways $f(n,k)$ that a set of n elements be arranged into k cyclic permutations follows the above recurrence relation.

Proof. Suppose we attempt to add an nth element to some set of cyclic permutations of $n-1$ elements. If this element forms its own cyclic permutation, this can be accomplished if the other elements are divided in $f(n-1,k-1)$ ways into these cyclic permutations. Otherwise, the nth element must go into an already-existing cyclic permutation, and we can arrange the $n-1$ elements into k cyclic permutations in $f(n-1,k)$ ways. We can insert the nth element directly after any of the existing $n-1$ elements in their cyclic permutations, for a total of $(n-1)f(n-1,k-1)$ ways. Since we are counting the same quantity, we must have $f(n-1,k-1) + (n-1)f(n-1,k) = f(n,k)$.

■

Remark. *We can write a permutation π in the following way (for 7 elements, for example)*

$$(14)(256)(37)$$

where (256) denotes a cyclic permutation that sends 2 to 5, 5 to 6, and 6 to 2. Similarly, we can see this permutation swaps 1 and 4, etc. In general, the following is true regarding ***any*** *permutation:*

Theorem 3.2. *Any permutation can be written as a product of cyclic permutations.*

We will not prove this rigorously, but we can sketch out a constructive proof by considering a permutation π of the set $\{1,2,3,\ldots n\}$ as a one-to-one mapping of this set of n elements to itself. We can construct the cyclic permutations that comprise this permutation by "following the mapping for each element." To be clear, we can begin by considering $\pi(1) = c$, and then look for $\pi(c)$, etc. and at every step, we find the element that the previous element we found maps to. If this *ever maps back to* 1*, we have a cyclic permutation - and if there are elements in the permutation that we haven't visited, we can repeat the process on the remaining elements starting at the lowest unvisited element. This is by no means a rigorous proof of the result, but it should give you an intuitive feel for why this is true.*

We can now construct a few easy base cases for the function f:

$$f(1,1) = 1$$
$$f(n,1) = (n-1)!$$

The last is a problem that we've already encountered before, and the first is pretty easy to see. Here is a table of small values of $f(n,k)$:

n,k	1	2	3	4	5
1	1				
2	1	1			
3	2	3	1		
4	6	11	6	1	
5	24	50	35	10	1

Notice that $f(n,k)$ are the Stirling numbers of the first kind! In particular, this means that the Stirling numbers of the first kind count the number of ways a set of n elements can be arranged into k cyclic permutations.

Armed with this recursive definition (and the ability to run it backwards in a similar fashion), we can now show the theorem that we took to be as a definition, that is, $\left[{n \atop k}\right] = \left\{{-k \atop -n}\right\}$:

Proof. The statement is true whenever $k = 0$ or $n = 0$ - it can be easily shown that these are all 0, except when both are, in which case $\left[{0 \atop 0}\right] = \left\{{0 \atop 0}\right\} = 1$. Note that if we assume the statement is true for all $\left[{x \atop y}\right]$ such that $0 \le x < n$ (employing the principle of strong induction), we have:

$$\begin{aligned}
\begin{bmatrix} n \\ k \end{bmatrix} &= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix} \\
&= \begin{Bmatrix} 1-k \\ 1-n \end{Bmatrix} + (n-1)\begin{Bmatrix} -k \\ 1-n \end{Bmatrix} \\
&= \begin{Bmatrix} -k \\ -n \end{Bmatrix} + (1-n)\begin{Bmatrix} -k \\ 1-n \end{Bmatrix} + (n-1)\begin{Bmatrix} -k \\ 1-n \end{Bmatrix} = \begin{Bmatrix} -k \\ -n \end{Bmatrix}
\end{aligned}$$

where the last step follows from the recurrence relation for the Stirling numbers of the second kind. With a similar argument for the negative integers, by induction, the statement is therefore true for all $n, k \in \mathbb{Z}$.

■

With the remark above, we can also show the identity:

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!$$

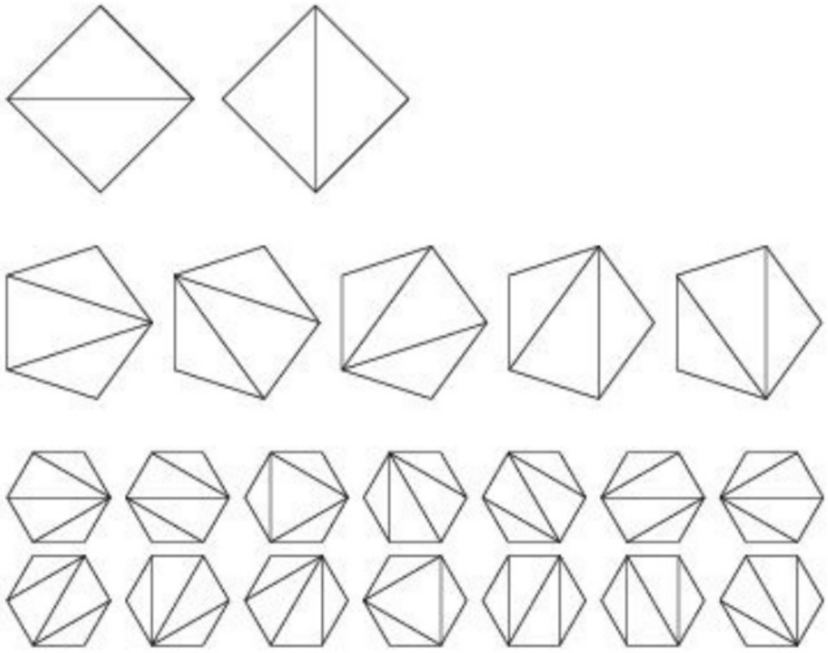


Figure 1: Triangulations for 4, 5, and 6 sided polygons.

Proof. The left hand side is adding up all the possible ways we can split a set of n elements into k cyclic permutations. From the remark, since every permutation can be written as one and only one product of some number of cyclic permutations from 0 to n, we have that this sum must be equal to the total number of permutations of n elements, or $n!$. ■

3.8 Triangulations (Catalan Numbers I)

Q: How many triangulations are there of a labeled hexagon? (This means that although two triangulations may be the same under rotation, which vertices they are attached to matter).
Let us first examine the general case of an n-gon and look at the behavior of the first few [1].

The rules for triangulation are only such that there are no crossings between the lines. Note: a triangulation of an n-gon uses n-3 line segments and results in n-2 interior triangles.

[1] http://mathworld.wolfram.com/CatalanNumber.html

As we can see from Figure 1, the answer to our original question is 14, but let us instead try to come up with a general formula for T_n = number of ways to △ a n-gon.

Note: The following graphics will be done in Microsoft Paint. I'm sorry in advance.

Theorem 3.3.

$$T_n = \sum_{k=2}^{n-1} T_{n-(k-1)} \cdot T_{k-1}$$

Proof. WARNING: THIS WAS THE PROOF THAT WAS SHOWN IN CLASS THAT HAD AN ERROR IN IT. I still think it is worth to look it over and see why it doesn't work. Just to clarify, although this proof does give the correct recursion, it is not correct. To my knowledge, it is nothing short of a miracle that this method accidentally over-counts and under-counts solutions in such a way to produce a correct recursion.
This hexagon could be broken up into 3 different shapes like this, which would result in $T_6 = T_3 \cdot T_5 + T_4 \cdot T_4 + T_5 \cdot T_3$. This obviously satisfies our original theorem, and all n-gons could be split like this, but this does over-count, because it does not account for when splitting up the remaining polygons you end up with the same triangulation. That is the reason why this proof does not work well for formulating the Catalan numbers. ■

Proof. Instead of splitting the polygon with a line, which allows for over-counting, if it is instead split with a triangle, we are guaranteed that each solution found is unique, and from looking at the diagram below, we see that the sum of each of these will give us the correct number.

■

3.9 Triangulating Polygons (Review of Catalan Number Proof)

Proof. The number of ways to triangulate a hexagon, T_6, can be found by recursion through dividing the interior of the hexagon with a triangle. After picking the triangle in one of 4 ways, the number of ways to triangulate the remaining area is either T_5T_2 or T_4T_3, depending on the triangle picked. This means we can say $T_6 = T_5T_2 + T_4T_3 + T_3T_4 + T_2T_5$. We can shift the indices here to get the recursive definition of Catalan numbers using the following:

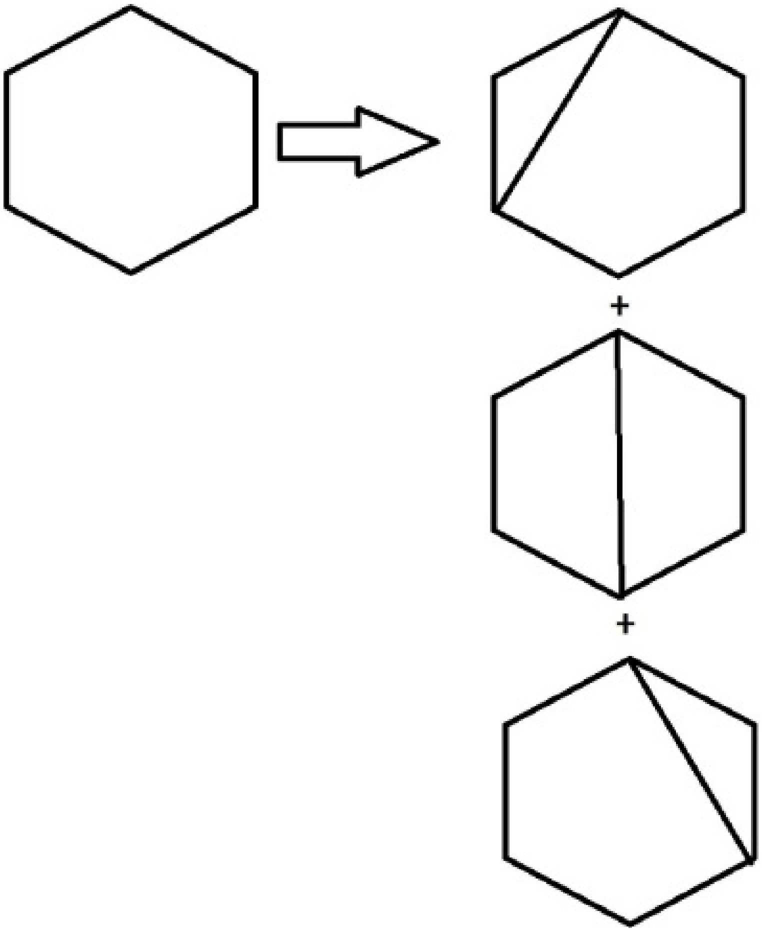


Figure 2: (Incorrect) recursion for a hexagon.

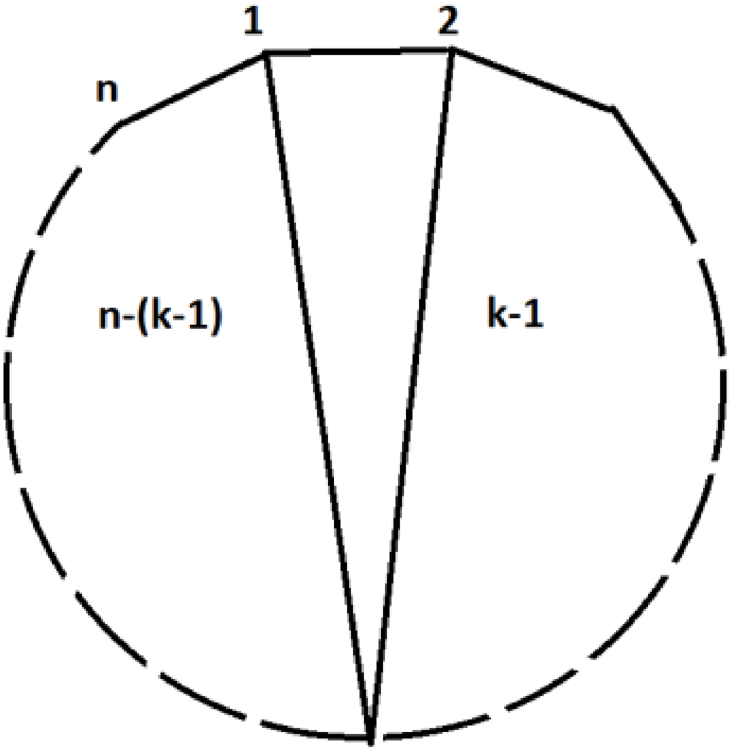


Figure 3: Correct recursion for a hexagon.

$T_{n+1} = T_2T_n + T_3T_{n-1} + ...T_nT_2$
$T_{n+1} = \sum_{j=2}^{n} T_jT_{n+2-j}$
Let $T_{n+1} = C_n$
$T_{n+2} = \sum_{j=2}^{n+1} T_jT_{n+3-j}$
$C_n = \sum_{j=2}^{n+1} C_{j-2}C_{n+1-j}$
$C_{n+1} = \sum_{j=2}^{n+1} C_{j-2}C_{n+2-j}$
$C_{n+1} = \sum_{j=1}^{n} C_jC_{n-j}$ This is the recursive definition of Catalan numbers, so we can conclude that there are C_n ways to triangulate an n+2-gon.

■

3.10 Paths (Catalan Numbers II)

Q: How many paths are there between the points (0, 0) and (2n, 0), only moving with steps of either northeast (up one right one) or southeast (down one right one).
(Note: This is analogous to the question of paths between (0, 0) and (n, n) with only vertical and horizontal steps except the algebra works better in this one. However, the pictures I can find are using this interpretation of the problem, so unless we want more Microsoft Paint pictures, these will do. If at any point you get confused between what we did in class and the pictures I'm showing, turn your head $45°$ to the left and it will make sense again.)
A: $\binom{2n}{n}$.

Proof. There are 2n moves, n of them must be up, n must be down, so choose which n will go southeast and we are done.

■

Now we want to count all of the paths that do not cross the x-axis, as the one in Figure 4 does. I'm going to have to use paint for this as I cannot find pictures. Sorry again.
In order to do this, we first notice that all bad paths (ones that cross the x axis), touch the line y = -1 at least once. To count them, we will reflect everything BEFORE the first y = -1 touch along the line y = -1, and leave everything after it the same. (This is why we do it this way instead of diagonally because the reflection is much easier to visualize). This creates a mapping of all bad paths to something else. This is a one to one mapping, every bad path has a reflection, and every reflection has only 1 bad path associated with it. Now, by counting the reflections we also count bad paths. Since the bad paths start at y = -2, and need to reach (2n, 0), we have to choose n+1 up moves (note that this is because this will also result in one less down move, leaving us two above our initial position).
So bad paths = $\binom{2n}{n-1}$

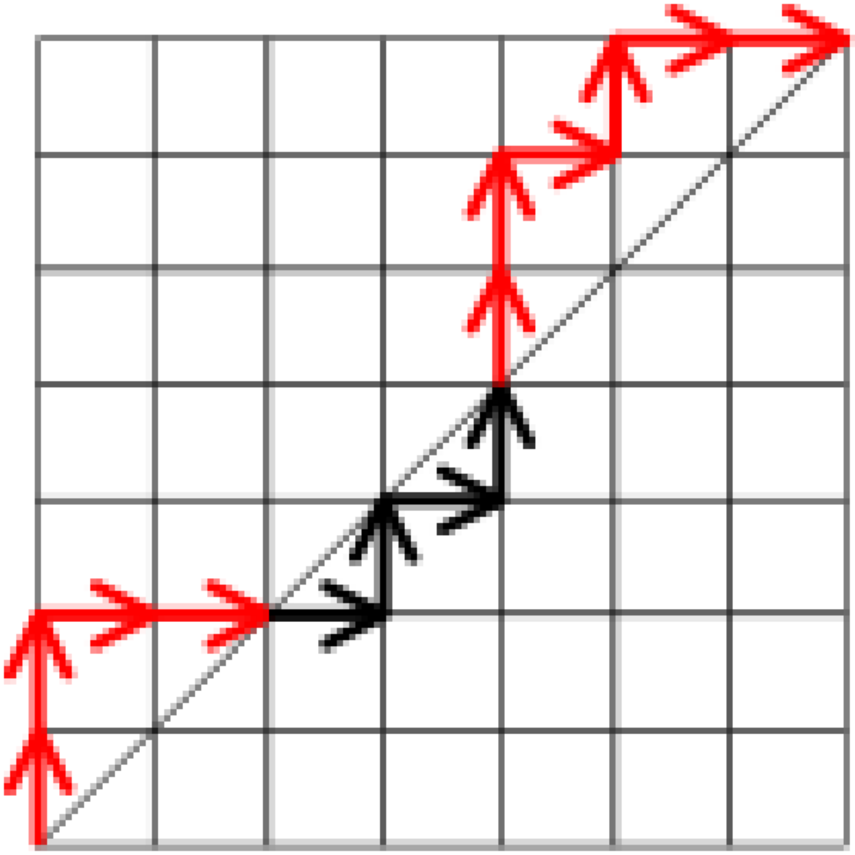


Figure 4: An example of a path.

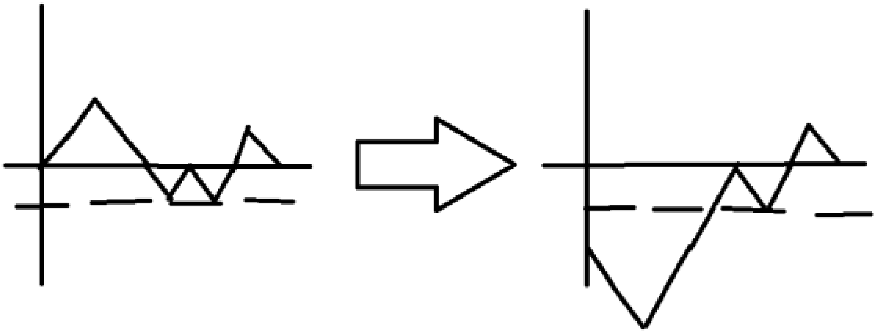


Figure 5: The transformation applied to all bad paths

This gives our total amount of good paths to be the following

$$P = \binom{2n}{n} - \binom{2n}{n+1}$$

$$\frac{(2n)!}{n! \cdot n!} - \frac{(2n)!}{(n-1)!(n+1)!} = \frac{(2n)!}{n! \cdot n!} \cdot (1 - \frac{n}{n+1})$$

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

Which is the Catalan numbers (note how by splitting up the original path problem into two smaller ones, we can also achieve the recursion relation for the Catalan numbers, like we did with the hexagons).

4 Interlude: Stirling's Approximation

We intend to examine different ways that we may approximate the value of $n!$. The first of these methods is Stirling's Approximation.

Theorem 4.1. *(Stirling's Approximation)* $\lim_{n\to\infty} \frac{n!}{(\frac{n}{e})^n * \sqrt{2\pi n}} = 1$

This is the formal definition of Stirling's Approximation. The actual approximation that we are observing, would be the denominator of this fraction. Stirling's thinking behind this, is that as n increases in size, the ratio should eventually become equal to 1.

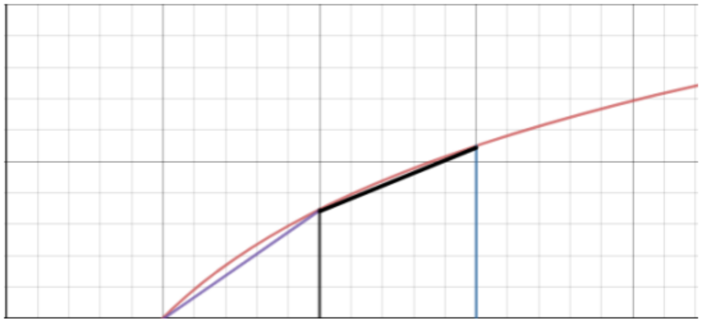
We won't however, be proving the formal definition of Stirling's Approximation. Instead, we want to find some sort of upper and lower bound for the value of $n!$. To do this, we will first create an informal definition for $n!$.

Informally speaking, $n! \sim \frac{n}{e}^n * \sqrt{2\pi n}$
We intend to prove that $n! = \frac{n}{e}^n * \delta\sqrt{n}$, where $\delta \cong \sqrt{2\pi}$

To do this proof, we also want to make note of an important summation remark:

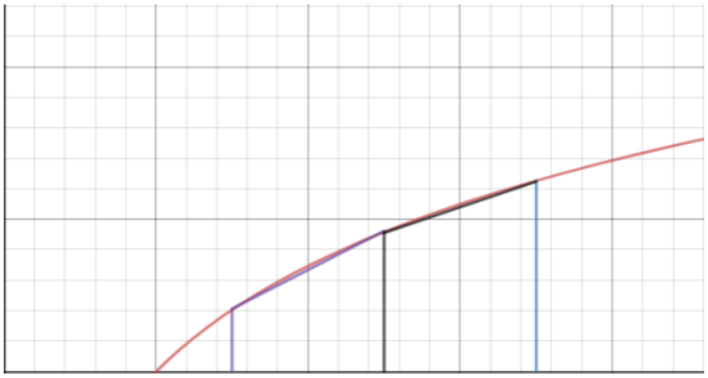
Remark. $log(n!) = \sum_{i=1}^{n} log(i)$

Proof. To do the actual proof, we will consider the function $y = ln(x)$. From here we intend to make two Riemann-style approximations for the integral $\int_i^n ln(x)dx$. For our proof, both approximations will be trapezoidal approximations.



Approach one is two use a trapezoid whose bases are at the integers themselves.

Area of the trapezoids is $\frac{1}{2}\sum_{i=1}^{n-1} [ln(i) + ln(i+1)]$
$= \frac{1}{2}ln(1) + \sum_{i=2}^{n-1} [ln(i) + ln(i+1)] + \frac{1}{2}ln(n)$
$= ln(n!) - \frac{1}{2}ln(n)$



Approach two is two use a trapezoid whose bases are at the midpoints between integers. Notice that we don't care about the area before $x = \frac{1}{2}$ in our calculations.

Area = $ln(2) + ln(3) + ln(4) \cdots + ln(n-1) + \frac{1}{2}ln(n)$, which comes out to be the same as above. Notice that this is an overestimate however, and the previous approach was an underestimate.
$\therefore \int_{\frac{3}{2}}^{n} ln(x)dx + \frac{1}{2}ln(n) < ln(n!) < \int_{1}^{n} ln(x)dx + \frac{1}{2}ln(n)$

Given $\int ln(x)dx = xln(x) - x + C$

We get:
$(nln(n) - n) - (\frac{3}{2}ln(\frac{3}{2}) - \frac{3}{2}) + \frac{1}{2}ln(n) < ln(n!) < (nln(n) - n) - (ln(1) - 1) + \frac{1}{2}ln(n)$
$= (n + \frac{1}{2})ln(n) - n - \frac{3}{2}(ln(\frac{3}{2}) - 1) < ln(n!) < (n + \frac{1}{2})ln(n) - n + 1$

At this point, we have a range of error for $ln(n!)$.

We can define $ln(n!) = [(n+\frac{1}{2})ln(n) - n] + \delta_n$, where $\frac{3}{2}(1 - ln(\frac{3}{2})) < \delta_n < 1 \longrightarrow 0.891802 < \delta_n < 1$

Since $ln(n!) = (n + \frac{1}{2})ln(n) - n + \delta_n$,
$e^{ln(n!)} = e^{nln(n)}e^{\frac{1}{2}ln(n)}e^{-n}e^{\delta_n}$
$n! = n^n\sqrt(n)e^{-n}e^{\delta_n}$
$= (\frac{n}{e})^n\sqrt(n) * e^{\delta_n}$, where $e^{\delta_n} \in [2.439, 2.718]$. The value for $\sqrt{2\pi n} = 2.506$, which falls within our expected range of values.

■

Now that we have an approximation for $n!$, we can look to write an expression that will give us the n^{th} Catalan number. The n^{th} Catalan number is given by the expression $\binom{2n}{n} * \frac{1}{n+1}$
$\binom{2n}{n} * \frac{1}{n+1} = \frac{(2n)!}{n!n!} = \frac{(2n)!}{[(\frac{n}{e})^n * \sqrt{2\pi n}]^2}$

$$= \frac{\frac{2n}{e}^{2n}}{\frac{n}{e}^{2n}} * \frac{\sqrt{4\pi n}}{2\pi n*(n+1)} = \frac{2^{2n}*\sqrt{\pi n}}{\pi n(n+1)} = \frac{4^n}{\sqrt{\pi n}(n+1)}$$

4.1 Gamma Function

Gamma functions are an extension of factorials, such that the arguments are shifted down by one. In other words, $\Gamma(2) = 1!$, $\Gamma(3) = 2!$, etc. We intend to prove that $\Gamma(n+1) = n!$. To do this, we first begin by defining our gamma function.

Definition. $\Gamma(z+1) = \int_0^\infty x^z e^{-x}$

Now that we have defined our gamma function, we will attempt to prove that $\Gamma(n+1) = n!$.

Proof. First, we will integrate this function by parts:

- $u = x^7$, $du = zx^{z-1}$
- $v = -e^{-x}$, $dv = e^{-x}$

$\therefore \int_0^\infty x^z e^{-x} dx = [x^z(-e^{-x})]_0^\infty + \int_0^\infty zx^{z-1}e^{-x}dx$

Notice how when we evaluate the expression $\int_0^\infty x^z e^{-x} dx = [x^z(-e^{-x})]_0^\infty$, x^z becomes 0 when evaluated at $x = 0$, and $(-e^{-x})$ becomes zero when evaluated at $x = \infty$, meaning that this expression evaluates to just 0.

Therefore, we are left with just $\int_0^\infty zx^{z-1}e^{-x}dx$. We can redefine this as $z\int_0^\infty x^{z-1}e^{-x}dx = z\Gamma(z)$.

At this point, we have something that is similar to a factorial, but we can't consider our proof complete until we establish some base cases. We can begin by testing with $z = 1$. $\Gamma(1) = \int_0^\infty x^0 e^{-x}dx = \int_0^\infty e^{-x}dx = 1$
$\therefore \Gamma(1) = 1$
$\Gamma(2) = 1 * \Gamma(1) = 1$
$\Gamma(3) = 2 * \Gamma(2) = 3$
$\Gamma(4) = 3 * \Gamma(3) = 6$
$\therefore \Gamma(n+1) = n!$

■ As we intended, we have now found a function that is similar to a factorial, withe the arguments shifted by one. However, we also want to observe how fractional factorials work. In our case, we'll observe $\Gamma(\frac{1}{2})$.

Proof. $\Gamma(\frac{1}{2}) = \int_0^\infty x^{\frac{-1}{2}} e^{-x}dx = \int_0^\infty \frac{e^{-x}}{\sqrt{x}}$
Let $u = \sqrt{x}$, $u^2 = x$, and $du * 2u = dx$
Substituting u into the equation, we get $\Gamma(\frac{1}{2}) = 2\int_0^\infty e^{-u^2}du$

Now suppose we define a variables v and K, such that
$K = \int_0^\infty e^{-u^2} du = \int_0^\infty e^{-v^2} dv$
$K^2 = \int_0^\infty e^{-u^2} du \int_0^\infty e^{-v^2} dv$
$= \int_0^\infty \int_0^\infty e^{-u^2} e^{-v^2} dudv = \int_0^\infty \int_0^\infty e^{-(u^2+v^2)} dudv$
In Cartesian coordinates, this integral would be difficult to solve. However, we can convert to polar coordinates to solve this equation. Notice that because we are only using positive integers, θ is bounded within the first quadrant
$K^2 = \int_0^{\frac{\pi}{2}} \int_0^\infty e^{-r^2} * rdrd\theta = \frac{\pi}{2} \int_0^\infty e^{-r^2} * rdr$
$= \frac{\pi}{2} * (\frac{-e^{-r^2}}{2})_0^\infty = \frac{\pi}{2}(\frac{1}{2} - 0) = \frac{\pi}{4}$
$\therefore K = \frac{\sqrt{\pi}}{2}$
$\therefore \Gamma(\frac{1}{2}) = 2K = 2\frac{\sqrt{\pi}}{2} = \sqrt{\pi}$

■

5 Problems and Examples

5.1 Remark: Unlabeled Probability

Problem 1. You throw two marbles into two buckets. Find the probability that they both land in the same bucket:

- Unlabeled into unlabeled: 1/2 (2 scenarios: marbles in separate buckets or together)
- Labeled into unlabeled: 1/2 (2 scenarios: marbles in separate buckets or together)
- Labeled into labeled: 1/2 (4 scenarios - 2 of which include both marbles in the same bucket)
- Unlabeled into labeled:

  Let's label buckets A and B. You have two indistinguishable marbles, and so there are three scenarios: marbles are in separate buckets, both marbles are in A, and both marbles in B. Therefore, you may incorrectly conclude that the probability is 2/3, when in reality it remains 1/2. The probability of marbles being in separate buckets is twice the odds that both marbles are in A.

  This is because **probability problems are ALWAYS labeled.**

  If you label the marbles 1 and 2, there are two ways for the marbles to be in separate buckets, each as probable as any of the other scenarios: 1-A and 2-B or 1-B and 2-A.

When you are asked for the probability, always treat both the balls and urns, or marbles and buckets, as labeled into labeled.

5.2 Homework Problems (Problem Set 2)

Problem 1. In how many ways may we write n as a sum of an ordered list of k positive numbers? Such a list is called a composition of n into k parts.

Solution We can split n into n identical 1's. Then the problem becomes about dividing identical objects into k distinguishable piles with at least one in each pile to form ordered pairs of numbers which sum to n. That makes this stars and bars where we have k-1 bars (to divide the set into k-1 groups) and n-1 possible spaces (we want at least one 1 in each group). There are $\binom{n-1}{k-1}$ ways to do this. ■

Problem 2. What is the total number of compositions of n (into any number of parts).

Solution In this question, we have n-1 spaces between each 1 that we can make a "bar" that creates a new group. We have two groups that n-1 things can fall in, so our total number of ways to do that is 2^{n-1}. Alternatively, we could recognize that the total number of ways to do this is the sum of our answer from question one where k goes from 1 to n-1 ($\sum_{k=1}^{n-1}\binom{n-1}{k}$) matches the form of the sum in the binomial theorem ($(a+b)^j = \sum_{k=0}^{j}\binom{j}{k}a^{j-k}b^k$). In this case, a and b would both be 1 and j would be n-1, which would give us 2^{n-1}. ■

Problem 3. A Grey Code is an ordering of n-digit binary strings such that each string differs from the previous in precisely one digit.

Problem 3.1. Write one Grey Code for n=4.

1111, 1110, 1100, 1000, 0000, 0001, 0011, 0111, 0101, 1101, 1001, 1011, 1010, 0010, 0110, 0100.

Problem 3.2. Prove by induction that Grey Codes exist for all $n \geq 4$.

Let n=4 be the base case. Starting with a Grey Code for n=4, to create one for n=5, we can duplicate all the numbers in the Grey Code while keeping the same order and alternate between adding 1's and 0's in the front using the following pattern: 1, 0, 0, 1, 1, 0... This maintains the one-digit difference while listing all the 5-digit binary numbers (because each number listed is unique, since the list of 4-digit numbers was unique and either 0 or 1 is added only once to each number, and there are twice as many numbers in the list, just like there are twice as many 5 digit binary numbers as 4-digit ones). For example, using the earlier Grey Code, we get (11111, 01111, 01110, 11110...). This procedure can be repeated for 6-digit numbers, 7-digit numbers, and so on.

Problem 3.3. Prove that the number of even-sized subsets of an n-element set equals the number of odd-sized subsets of an n-element set.

The subsets of an n-element set can be mapped one-to-one to the strings in a Grey Code for n=n by having the 0's and 1's indicate whether or not to include each element of the original set. Since each string in a Grey Code differs from the previous string by exactly 1 digit, the strings must alternate between having even and odd numbers of 1's, indicating even or odd sized subsets. Since there are 2^n binary strings of length n, there are an even number of strings in each Grey Code, so the alternation between odd and even sized subsets must produce equal numbers of both.

Problem 4. A list of parentheses is said to be balanced if there are the same number of left parentheses as right, and as we count from left to right we always find at least as many left parentheses as right parentheses. For example, (((()()))()) is balanced and ((()) and (()()))(() are not. How many balanced lists of n left and n right parentheses are there?

This is equivalent to the problem of counting the number of paths from (0, 0) to (2n, 0) using only northeast (1, 1) and southeast (1, -1) steps without crossing the x-axis. Adding left parentheses translates to moving northeast, and adding right parentheses translates to moving southeast. Their numbers must be equal in the end, and not crossing the x-axis ensures that the number of left parentheses is always at least as many as the number of right parentheses. To count the number of paths, we use complementary counting: there are $\binom{2n}{n}$ paths altogether, and $\binom{2n}{n+1}$ paths that cross the x-axis (which we can count by reflecting them across the line y=-1 to form paths from (0, -2) to (2n, 0)). This results in $\frac{\binom{2n}{n}}{n+1}$ acceptable paths and acceptable lists.

Problem 5. A tennis club has 4n members. To specify a doubles match, we choose two teams of two people. In how many ways may we arrange the members into doubles matches so that each player is in one doubles match? In how many ways may we do it if we specify in addition who serves first on each team?

We can start by arranging the 4n people into a line, which can be done in (4n)! ways. We can then assign them to courts by taking the first 4 people for the first court, the next 4 for the second, and so on. Since the order of the courts doesn't matter, we must divide by n!. Then, we must account for another overcounting issue: we have 8 different ways to specify the same set of 2 teams for each court. To account for this issue, we must divide by $2^{(3n)}$, since there are n courts. Altogether, this gives us $\frac{(4n)!}{n! \times 2^{3n}}$ ways.

Problem 6. A town has n streetlights running along the north side of main street. The poles on which they are mounted need to be painted so that they do not rust. In how many ways may they be painted with red, white, blue, and green if an even number of them are to be painted green?

We can start by picking an even number of the n poles to be green: there are $\binom{n}{2k}$ ways to do this, where k ranges from 0 to $\lfloor n/2 \rfloor$ There are 3 ways to color each of the remaining n-2k poles, meaning 3^{n-2k} ways altogether. This means the total number of ways to color these streetlights is $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} * 3^{n-2k}$. We can get the closed form of this by adding the binomial expansions of $(3{+}1)^n$ and $(3{-}1)^n$ and dividing by 2 to get the sum. This gives $2^{2n-1}{+}2^{n-1}$.
Alternatively...
Preview of formulation 3:
Let E_n=number of ways to color n poles with an even number of greens, and O_n=number of ways to color n poles with an odd number of greens, so that E_n+O_n=the total number of ways to color n poles.$E_{n+1} = 3E_n + O_n$: Adding one more pole to a set of n poles such that we end up with an even number of green poles can be done in only one way if there are an odd number of green poles in the first set of n poles (the pole must be green) and can be done in 3 ways if there are an even number of green poles in the first n poles (the pole can be any color but green).

Problem 7. We have n identical ping pong balls. In how many ways may we paint them red, white, blue, and green if we use green paint on an even number of them?

There must be 2k balls painted green, where k ranges from 0 to $\lfloor n/2 \rfloor$ in order to ensure that the number of green balls is even. There are 3 ways to color each of the remaining n-2k balls. We can imagine this as a multiset problem, where there are n copies of each of the 3 colors. This means there are $\sum_{k=0}^{\lfloor n/2 \rfloor} \left(\!\binom{3}{n-2k}\!\right)$ ways to color the balls altogether.

Problem 8. A boolean function $f : (0,1)^n \rightarrow$0, 1 is self-dual if replacing all 0s with 1s and 1s with 0s yields the same function. How many self-dual boolean functions are there as a function of n?

We can regard the function's inputs to be in pairs, where switching the 0s and 1s of one member of the pair results in the other member. To ensure that the function is self-dual, both members of a pair must give the same result when inputted into f, meaning that there are $2^n/2$ distinct inputs. Since each input can be mapped to 0 or 1, this means the number of possible functions is $2^{2^{n-1}}$.

Problem 9. A boolean function $f : (0,1)^n \rightarrow$0, 1 is symmetric if any permutation applied to the digits in the domain yields the same function. e.g. f(001)=f(010)=f(100). How many symmetric boolean functions are there as a function of n?

Again, we can group the function inputs based on which must give the same output. There will now be n input groups based on how many 1s are in the input, since inputs with the same number of 1s are just permutations of each other. This means there are n+1 distinct inputs which can each be mapped to 0 or 1, so the number of possible functions is 2^{n+1}.

Problem 10. Prove x^n= $\sum_{k=0}^{n} S(n,k)x^{\underline{k}}$.

The number of ways to assign n labeled balls to k labeled urns is k!S(n, k) if we want at least one ball in each urn. To assign n balls to k urns out of x potential urns, we must assign at least one ball to k urns and no balls to the other x-k. There are k!S(n, k)*$\binom{x}{k}$, or $S(n,k)x^{\underline{k}}$ ways to do this. k ranges from 0 to n, since we wanted at least one of the n balls in each of the urns. Summing all the possible values of k up, we get $\sum_{k=0}^{n} S(n,k)x^{\underline{k}}$. This is equivalent to the left side of the equation, which corresponds to assigning n labeled balls to x labeled urns with no restrictions.

Problem 11. Prove that $(1+x)^\alpha$=$\sum_{k=0}^{\infty} \alpha^{\underline{k}} x^k/k!$ for any real α.

The Taylor series for 1+x centered around 0 is $(1+x)^\alpha + \alpha * x/1! + \alpha * (\alpha - 1) * x^2/2!$...which is equivalent to $\sum_{k=0}^{\infty} \alpha^{\underline{k}} x^k/k!$

5.3 Equivalence Relations (Bell Numbers)

A relation on set A is a subset of AxA=(a, a), (a, b)...(b, a)...(d, d). An equivalence relation is defined as any relation that is symmetric, reflexive, and transitive.
Definitions:
Reflexive - a relates to a, or must relate to itself (e.g., greater than is not a reflexive relationship because a number cannot be greater than itself).
Transitive - if a relates to b and b relates to c, then a relates to c (e.g., greater

than is symmetric because if a $>$ b and b $>$ c, then a $>$ c).
Symmetric - if a relates to b, then b relates to a (e.g., greater than is not symmetric because if a $>$ b, b cannot be greater than a).
Cayely tables represent relations as a table. An example can be found below:

	A	B	C	D
A	X			
B	X	X		
C				
D				X

This table says that a relates to a, b relates to a, b relates to b, and d relates to d. As an example, this table isn't reflexive, symmetric, or transitive. The following revised table makes the relation symmetric.

	A	B	C	D
A	X			
B	X	X		
C			X	
D				X

The table still isn't transitive or symmetric, though. The next table is symmetric and reflexive, but not transitive.

	A	B	C	D
A	X	X		
B	X	X	X	
C		X	X	
D				X

The following table is all three:

	A	B	C	D
A	X	X	X	
B	X	X	X	
C	X	X	X	
D				X

How can we count how many possible relations are reflexive; reflexive and symmetric; and reflexive, symmetric, and transitive (given n rows and columns)?

Problem 1. How can we count the number of reflexive relations?

All reflexive relations must have the diagonal filled in. Without the diagonal, there are $n^2 - n$ spaces that can be filled in or left empty. Because each space can go two ways, our final answer is 2^{n^2-n}.

Problem 2. How can we count the number of reflexive and symmetric relations?

We have to start with the diagonal we had last time in order to find this next answer. For the relation to be symmetric, if a box on one side of the diagonal is filled in, then the reflection of that box over the diagonal must be filled on. That means that we have the freedom to fill in boxes on only one side of the diagonal, or $\frac{n^2-n}{2}$ boxes. Incidentally, $\frac{n^2-n}{2}$ is also $\binom{n}{2}$, which makes our final answer either $2^{\frac{n^2-n}{2}}$ or $2^{\binom{n}{2}}$.

Problem 3. How can we count the number of true equivalence relations?

We can no longer consider the diagonal method we considered earlier. Now, we must realize that to be transitive, we must create subsets of elements that all relate to each other. For instance, if we had elements a, b, c, d, e, and f, we could separate the group into two subsets: b, c, e, f and a, d. If every element in that set related to every other element in that set (including itself), we would have a true equivalence relation. This example is shown in a Cayley table below.

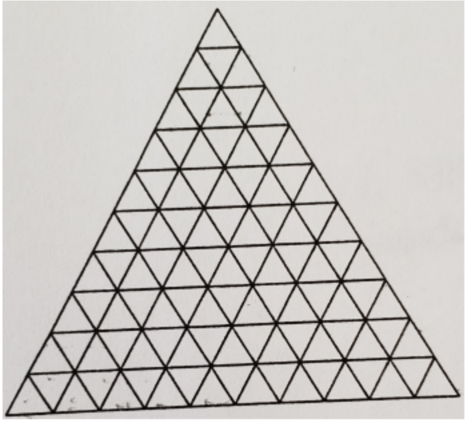
	A	B	C	D	E	F
A	X			X		
B		X	X		X	X
C		X	X		X	X
D	X			X		
E		X	X		X	X
F		X	X		X	X

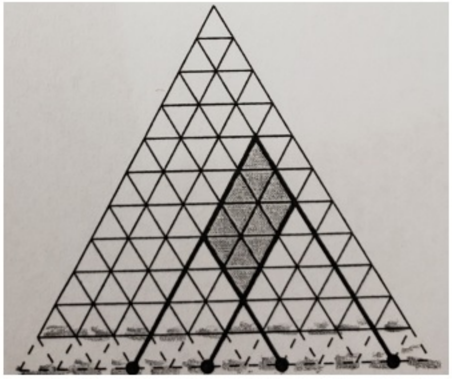
This is an example of a true equivalence relation. But how can we count that? We need to find the total number of ways to partition n elements, which is $\sum_{k=1}^{n} S(n,k)$ or a set of numbers we call the Bell numbers (B_n).

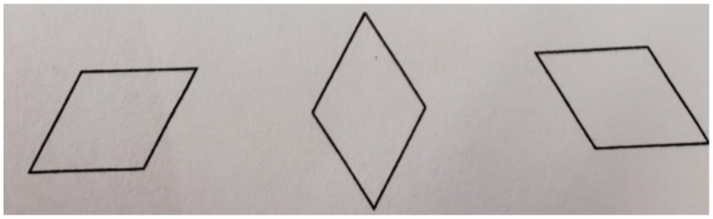
5.4 Parallelogram Problem

Problem 1. We have n rows of triangles as shown below. How many parallelograms can be formed in this figure?

Solution There can be three orientations of parallelograms, shown below, which by symmetry must have the same number of parallelograms. Thus, we can count one and multiply that number by three.





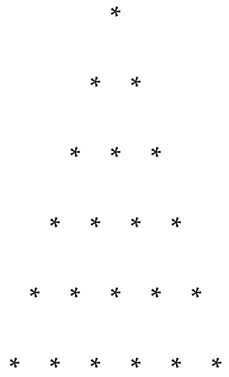


We can observe that a parallelograms has four lines that can be extended out. If we extend them out to one layer lower than the triangle, we can notice that the lines intersect with the bottom layer to find four points. Each one of the parallelograms corresponds to a unique selection of the four points, and vice versa. Thus, for each of the $n+2$ points on the level below the last one, we can choose four of them to get a unique parallelogram. Thus, in conclusion, the solution is

$$3\binom{n+2}{4}$$

■

5.5 Parallelogram Problem (Alternate Solution)



Example 1. We want to find a different way of counting the number of parallelograms that can be made by connecting the stars in the arrangement above.

Solution One method to do this would be to pick a diagonal. We can say that picking the diagonal is unique because only one parallelogram will have the certain segment as its longest diagonal. To determine the number of diagonals, we need to pick the number of line segments we can make using the points.

This can be done by taking the total number of points and choosing 2.
For a triangle of n rows, the number of points is $\frac{(n)(n+1)}{2}$ or $\binom{n+1}{2}$
To choose two dots we do $\binom{\binom{n+1}{2}}{2}$

However, we have to remember that if two dots are on the same line, then they won't be able to form the longest diagonal of a parallelogram, and if both are on an edge, it wouldn't be relevant. Therefore, we have to subtract for the times when the two dots chosen are collinear.

So the subtracted values would be $3 * somevalue$ because we have three orientations of the triangle to account for. (Another way of looking at this would be to say that we have 3 sides of the triangle to account for).
Now, to determine "some value". We realize that some value in one orientation is actually just the same as counting for each row, how many ways they can pick two points.

This can actually be written as a summation: $\sum_{i=2}^{n} \binom{i}{2}$
To explain, the sum. We know we must start at i=2, because a row with one dot cannot pick two dots that are collinear. We use the summation because

in the i-th row there are i dots and we need to pick 2 of them.

This therefore results in a final solution of $\binom{\binom{n+1}{2}}{2} - 3 * \sum_{i=2}^{n} \binom{i}{2}$

After some algebra, our final answer is $\boxed{3\binom{n+1}{4}}$ ■

5.6 Hat Problem

Problem 2. n mathematicians walk into a bar. They each remove their hat and toss it in a pile as they arrive. Several hours later, they leave one by one, grabbing a hat at random to face the brutal March wind. What is the probability that none of the mathematicians receive their own hat?

Solution This problem is equivalent to finding the number of **Derangement** of a set of size n, up to a factor of $n!$. The derangement number is notated as D_n, or $!n$.
We can approach this by counting the number of ways to get the desired outcome via complementary counting, and then to divide it through by the total number of arrangements to get the probability, as each configuration is equally likely. First, to count the number of ways in total that there can be reordered. This is just n!. However, in this, we have counted the number of ways that at least 0 mathematicians receive their hat. Next, we must subtract out the cases that have at least 1 mathematician getting back his or her hat. We can count this by choosing which mathematician gets his or her hat back, and then ordering the rest. Thus, the term is $\binom{n}{1}(n-1)!$. However, this overcounts those configurations for which more than one mathematician receives their hat back; we can fix this problem by using the principle of inclusion/exclusion, to get that the total number of derangements is

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! + \cdots + (-1)^n \binom{n}{n}(n-n)!.$$

This approaches $\frac{n!}{e}$ for sufficiently large n, as $e^x = 1 + x + x^2/2! + \cdots$. Thus, by dividing the nth derangement number by $n!$, we get the probability to be

$$1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{(-1)^n}{n!} \approx e^{-1}$$

for sufficiently large n. ■

5.7 "Coupon Collector"-esqe Problem

Problem 3. You have a bag containing x numbered marbles. Draw n marbles with replacement, where $n \leq x$. What is the probability that you drew exactly k distinct marbles?

Solution To solve this, we can consider sequences of draws. First, we must determine the total number of "events" or valid sequences. There are x^n such sequences. Next, we must pick k of the x distinct marbles to be seen, introducing a factor of $\binom{x}{k}$. Next, we must partition the sequence of n draws into k subsets, each subset representing the draws that got one distinct value of the marble, introducing a factor of $S(n, k)$. And finally, we must assign each marble to a subset, introducing a factor of $k!$. Thus, the probability is

$$\frac{k!\binom{x}{k}S(n,k)}{x^n}.$$

Example I. f there are 10 distinct marbles, we Draw 6, and see 3, one possible outcome is, if the number j represent the jth draw,

$$C : \{1, 4\}, A : \{2, 3, 5\}, B : \{6\}$$

Simplifying the probability a small amount, we get it to be

$$\frac{x^{\underline{k}}S(n,k)}{x^n}.$$

This also turns out to be a way to prove that $x^n = \sum_{k=1}^{n} x^{\underline{k}}S(n, k)$, as the sum of the probabilities of all valid outcomes must be one. ■

Part II
Generating Functions and Recurrences

6 Ordinary Generating Functions

6.1 Intro to Generating Functions

Problem 1. Find the nth term in the sequence if the the first term corresponds with $n = 0$:

$$1, 2, 4, 8, 16, ...$$

Solution $a_0 = 1$, $a_1 = 2$, $a_2 = 4$. It is clear from this pattern that $a_n = 2^n$. ■

Problem 2. Find the generating function for:

$$1, 2, 4, 8, 16, ...$$

Solution In a generating function, the coefficients of each power correspond to each of the terms in the sequence. This sequence can thus be represented as $g(x) = 1 * x^0 + 2 * x^1 + 4 * x^2 + 8 * x^3 + 16 * x^4 + 32 * x^5 + ... = (2x)^0 + (2x)^1 + (2x)^2 + (2x)^3 + (2x)^4 + (2x)^5 + ...$ This resembles the the Taylor power series. Using 'reverse'-Taylor, we find that $g(x) = \frac{1}{1-2x}$. ■

From this example, we can see that $\frac{1}{1-ax}$ is the generating function for the sequence $1, a, a^2, a^3, ... = \{a^k\}_{k=0}$. Generally, from the generating function, to obtain the nth value of the sequence, take the nth derivative of the function evaluated at 0.

Problem 3. For the following sequence, find the generating function:

$$2, 5, 13, 35, 97, ...$$

Solution The nth term of the sequence is $a_n = 2^n + 3^n$. From above, we know that $\frac{1}{1-2x}$ generates $\{2^n\}$ and $\frac{1}{1-3x}$ generates $\{3^n\}$. Since **we can add generating functions**, $\frac{1}{1-2x} + \frac{1}{1-3x}$ generates $\{2^n + 3^n\}$. If we simplify, we get the generating function $g(x) = \frac{2-5x}{1-5x+6x^2}$. ■

Problem 4. Given the Fibonacci sequence, find the generating function. Then find the non-recursive definition of the nth term:

$$f_0 = 0, f_1 = 1, f_n = f_{n-1} + f_{n-2}$$

$$0, 1, 1, 2, 3, 5, 8, 13, 21, ...$$

Solution
Finding the generating function:
To find the function $F(x)$, we need to reduce the number of terms we are dealing with. $F(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + ...$ We can see that the coefficient of the x^3 term is the sum of the coefficients of the x^2 and x terms, as per the definition of the sequence. To cancel out the terms, let's shift the the function by x and x^2.
$F(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + ...$
$x * F(x) = x^2 + x^3 + 2x^4 + 3x^5 + ...$
$x^2 * F(x) = x^3 + x^4 + 2x^5 + ...$
By subtracting, we get $(1 - x - x^2) * F(x) = x$, or $F(x) = \frac{x}{1-x-x^2}$.

Finding the non-recursive definition:
By partial fraction decomposition, we can break down $F(x)$ into the form of $\frac{A}{1-\alpha x} + \frac{b}{1-\beta x}$. This corresponds with the form $F_n = A * \alpha^n + B * \beta^n$. After solving for A, B, α, and β, we find that $F_n = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]$. ■

6.2 Applications of Ordinary Generating Functions

Example 1. Given $\{a, b, c, d, e\}$ pick a multiset of size 3 where no item may appear > 2 times.

Solution Simply count all possible ways, $\left(\!\binom{5}{3}\!\right)$, and subtract out the invalid ones, which is just the sets that have three of the same letter, thus there are 5 invalid sets. Evaluate to get 30 ways. ■

Example 2. 18 items, between 3 and 5 each, select a total of 79 items.

Definition. *Ordinary generating function of a sequence is $a_0, a_1, a_2, \ldots$ is*

$$A(x) = \sum_{k=0}^{\infty} a_k x^k$$

Remember this is just a series with the coefficients of the k'th power of x being the k'th element in the series.

Consider:

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2$$

Evaluate two ways.

1. Expand $(1+x)^n\left(1+\frac{1}{x}\right)^n$ (Note: This is not an obvious way to achieve this result, and to know to expand this to get the answer requires a lot of familiarity with the subject)

$$\begin{aligned}(1+x)^n\left(1+\frac{1}{x}\right)^n &= \sum_{k=0}^{n}\binom{n}{k}x^k\cdot\sum_{j=0}^{n}\binom{n}{j}x^{-j}\\ &= \sum_{k=0}^{n}\sum_{j=0}^{n}\binom{n}{k}\binom{n}{j}x^{k-j}\\ &= \sum_{k=0}^{n}\binom{n}{k}^2+\sum C_kx^k\end{aligned}$$

Rewrite $(1+x)^n\left(1+\frac{1}{x}\right)^n$ as $(1+x)^n(1+x)^nx^{-n}$

$$\begin{aligned}(1+x)^n(1+x)^nx^{-n} &= (1+x)^{2n}x^{-n}\\ &= x^{-n}\sum_{k=0}^{2n}\binom{2n}{k}x^k\\ &= \sum_{k=0}^{2n}\binom{2n}{k}x^{k-n}\\ \text{Let } k=n\\ &= \binom{2n}{n}+\sum C_kx^k\end{aligned}$$

Therefore

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$$

This conclusion is reached be equating the powers of x (in this case x^0) in both expansions. This technique is incredibly useful and will likely be leveraged in the future as well.

2. We have n blue marbles and n green marbles. Choose n total marbles.

$$\begin{aligned}\binom{2n}{n} &= \overset{G}{\binom{n}{0}}\overset{B}{\binom{n}{n}}+\overset{G}{\binom{n}{1}}\overset{B}{\binom{n}{n-1}}+\overset{G}{\binom{n}{2}}\overset{B}{\binom{n}{n-2}}+\dots\\ &= \sum_{k=0}^{n}\binom{n}{k}^2 \text{ because } \binom{n}{r}=\binom{n}{n-r}\end{aligned}$$

■

Consider.

$$(1+ax)(1+bx)(1+cx) = 1 + (a+b+c)x + (ab+bc+ac)x^2 + (abc)x^3$$

This is called the enumerator for subsets of $\{a, b, c\}$.

As you can see, the k'th power of x has all of the possible k length subsets of a, b, c in it.

By letting $a = b = c = 1$, then $\left(1+x^3\right) = 1+3x+3x^2+x^3 = \sum C_k x^k$ where C_k is the number of subsets of size k.

So $(1+x)^n = \sum \binom{n}{k} x^k$ is the Ordinary Generating Function (OGF) for binomial coefficients.
This is the same as choosing k items from a set of n where each item is chosen ≤ 1 times.

Equivalences

Given $(1+x)^n = \sum \binom{n}{k} x^k$
Plug in $x = 1$ to get

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Plug in $x = -1$ to get

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

$$\sum_{\substack{k=0 \\ k \text{ evens}}}^{n} \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ odds}}}^{n} \binom{n}{k}$$

Note that the above relationship was also something we proved on the second pset theoretically using Grey Codes.

Take the derivative

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

$$n \cdot 2^{n-1} = \sum_{k=0}^{n} k \binom{n}{k}$$

Now, let's select k items from n, each ≤ 2 times.

$$\left(1+ax+a^2x^2\right)(1+bx)(1+cx)$$

By expanding this out, we would receive all possible subsets of $\{a,a,b,c\}$ (I suppose subsets isn't the correct word as sets are often thought to not have duplicates but I hope you get what we mean). Having an a^2 means that a was chosen twice. Having no a' s in a term would mean that a was never chosen out of the objects. The power of x the combination accompanies is how many items we chose.

Mathematica will even expand this for us and we can see all of the combinations:

$a^2bcx^4+a^2bx^3+a^2cx^3+a^2x^2+abcx^3+abx^2+acx^2+ax+bcx^2+bx+cx+1$

With this knowledge, just like earlier, we will take a,b, and c equal to 1 in the expression

$$\left(1+ax+a^2x^2\right)\left(1+bx+b^2x^2\right)\left(1+cx+c^2x^2\right)$$
$$C_kx^k=\left(1+x+x^2\right)^n=\left(1+x+x^2\right)\left(1+x+x^2\right)\left(1+x+x^2\right)\dots$$

$$\left(1+x+x^2\right)^n=\sum_{i+j+k=n}1^ix^j\left(x^2\right)^k\left(\begin{array}{c}n\\i,j,k\end{array}\right)$$

Recall.

$$\left(\begin{array}{c}n\\i,j,k\end{array}\right)=\frac{n!}{i!\cdot j!\cdot k!}$$

So

$$\left(1+x+x^2\right)^n=\sum_{r=0}^{n}C_rx^r$$

where the coefficient of x^{j+2k} is $\binom{n}{i,j,k}$

Let us now solve the first example problem with this knowledge. In order to be able to choose ≤ 2 of each object, we would represent that with $\left(1+ax+a^2x^2\right)$ or just $\left(1+x+x^2\right)$ after taking a=1. Since each object can be chosen like this, and there are n objects, we receive $\left(1+x+x^2\right)^n$. Since we are only choosing 3 objects, we want the power of x to equal 3.

Example . Let $n=5,k=3$, each ≤ 2 times. (Note: k refers to the overall power of x, not the actual k we are iterating over in the sum).

Solution Find the coefficient of x^3 in $\left(1+x+x^2\right)^n$

$$\begin{aligned} x^3 &= x^{3+2\cdot 0} \to j=3, k=0, i=2 \\ x^3 &= x^{1+2\cdot 1} \to j=1, n=1, i=3 \\ \text{so the coefficient of } x^3 &= \binom{5}{3,0,2} + \binom{5}{1,1,3} \\ &= \frac{5!}{3!\cdot 2!} + \frac{5!}{3!} \\ &= \frac{120}{12} + \frac{120}{6} = \boxed{30} \end{aligned}$$

■

Going back to **Example 2**, where $n=18, k=79$, each between 3 and 5 times.

Solution Find the coefficient of x^{79} in $\left(x^3+x^4+x^5\right)^{18} = \sum_{k=0}^{n} C_k x^k$ Using Mathematica, we get 5895396. ■

Problem . Given a set of n elements, choose a multiset of size r.

Solution We have a notation for this: $\left(\!\binom{n}{r}\!\right)$ ■

Solution As an alternate solution, expand out $(1+x+\ldots+x^r)^n$ and look for the coefficient of x^r. However, what happens if we don't stop at the x^r term in our initial expression, which although it has no meaning in the context of the problem (it would be like choosing $r+1$ of one item when we only want r total).

$$(1+x+\ldots+x^r+\ldots)^n = \left(\frac{1}{1-x}\right)^n$$

This just comes from the Taylor series expansion of $\frac{1}{1-x}$.

$$(1-x)^{-n} = \sum_{k=0}^{\infty} \frac{(-n)^{\underline{k}}}{k!}(-x)^k$$

Negatives cancel out in each term and by simplifying to a choose statement:

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

This would make the coefficient of x^r equal to $\left(\!\binom{n}{r}\!\right)$, which agrees with our previous answer.

■

Problem . Given a set of n elements choose a multiset of size r, every element must be chosen at least once.

Solution

$$\left(x + x^2 + \dots\right)^n = x^n \cdot \frac{1}{(1-x)^n}$$
$$\sum_{k=0}^{\infty} \frac{(n)^{\underline{k}}}{k!}(x)^{k+n} = \sum_{k=0}^{\infty} \left(\!\binom{n}{r}\!\right) (x)^{k+n}$$

For the exponent to equal r, k must equal $r - n$. Evaluating $\left(\!\binom{n}{r-n}\!\right)$ gives $\binom{r-1}{r-n}$ ■

Problem . Find C_k for $\left(1 + x^5 + x^9\right)^1 00$ for $k = 23$

Solution

$$\sum_{i+j+k=100} (1)^i \cdot x^{5j+9k} \cdot \binom{n}{i, j, k}$$

The only combination of j and k that gives 23 is $j = 1$ and $k = 2$ giving us the answer $\binom{100}{2,1,97}$. ■

6.3 Fundamental Generating Functions

Recall the generating function for a sequence $a_0, a_1, a_2, \dots, a_n, \dots$

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

The goal is to find a formula for an arbitrary a_i.

a. $a_0, a_1, \dots = 1, 1, 1, \dots$ $\qquad f(x) = 1 + x + x^2 + \dots$

Maclaurin series for $\frac{1}{1-x}$. $\qquad = \sum x^i$

$$\begin{aligned} x \cdot f(x) &= x + x^2 + x^3 + \dots \\ f(x) \cdot (1-x) &= 1 \\ f(x) &= \frac{1}{1-x} \end{aligned}$$

b. $a_0, a_1, \cdots = 2, 2, 2, \ldots$

...OR recognize $\dfrac{2}{1-x}$.

$$\begin{aligned} f(x) &= 2 + 2x + 2x^2 + \ldots \\ x \cdot f(x) &= 2x + 2x^2 + 2x^3 + \ldots \\ f(x) \cdot (1-x) &= 2 \\ f(x) &= \frac{2}{1-x} \end{aligned}$$

c. $a_0, a_1, \cdots = 1, -1, 1, -1, \ldots$

i.e. $\dfrac{1}{1-(-x)}$

$$\begin{aligned} f(x) &= 1 - x + x^2 - x^3 + \ldots \\ &= \sum x^i (-1)^{i+1} \\ x \cdot f(x) &= x - x^2 + x^3 - \ldots \\ f(x) + x \cdot f(x) &= 1 \\ f(x)(1+x) &= 1 \\ f(x) &= \frac{1}{1+x} \end{aligned}$$

d. $a_0, a_1, \cdots = 1, 0, 1, 0, \ldots$

$$\begin{aligned} f(x) &= 1 + x^2 + x^4 + \ldots \\ &= \sum x^{2i} \\ x^2 \cdot f(x) &= x^2 + x^4 + x^6 + \ldots \\ f(x) \cdot (1-x^2) &= 1 \\ f(x) &= \frac{1}{1-x^2} \end{aligned}$$

OR you can add parts a. and c. and then divide by 2

e. $a_0, a_1, \cdots = 0, 1, 0, 1, \ldots$

$$\begin{aligned} f(x) &= x + x^3 + x^5 + \ldots \\ &= \sum x^{2i+1} \\ x^2 \cdot f(x) &= x^3 + x^5 + x^7 + \ldots \\ f(x) - x^2 \cdot f(x) &= x \\ f(x) &= \frac{x}{1-x^2} \end{aligned}$$

OR you can subtract part a. by part c. and then divide by 2

f. $a_0, a_1, \dots = 1, 2, 4, 8, 16, \dots$

$$\begin{aligned} f(x) &= 1 + 2x + 4x^2 + 8x^3 + \dots \\ &= \sum (2^i)(x^i) \\ 2x \cdot f(x) &= 2x + 4x^2 + 8x^3 + \dots \\ f(x) \cdot (1-2x) &= 1 \\ f(x) &= \frac{1}{1-2x} \end{aligned}$$

OR recognize similarity to $\frac{1}{1-x}$ Maclaurin series, and simply substitute $2x$ for x.

g. $a_0, a_1, \dots = 1, \frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \dots$

Similar to e^x Maclaurin series.

Account for shift in constant and x.

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \dots \\ &= \sum \frac{x^n}{n!} \\ e^x - 1 &= x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \dots \\ \frac{e^x - 1}{x} &= 1 + \frac{x}{2} + \frac{x^2}{6} + \frac{x^3}{24} + \dots \end{aligned}$$

h. $a_0, a_1, \dots = 1, 2, 3, 4, \dots$

Focus on *powers* of x.

→ Use first derivative!

$$\begin{aligned} f(x) &= 1 + 2x + 3x^2 + \dots \\ \frac{1}{1-x} &= 1 + x + x^2 + \dots \\ \frac{d}{dx}\left(\frac{1}{1-x}\right) &= 1 + 2x + 3x^2 + \dots \\ &= f(x) = \frac{1}{(1-x)^2} \end{aligned}$$

i. $a_0, a_1, \dots = 2, 6, 12, 20, 30, \dots$

$n(n-1)$

→ second derivative!

$$\begin{aligned} \frac{1}{1-x} &= \sum x^k \\ \frac{1}{(1-x)^2} &= \sum_{k=0}^{\infty} kx^{k-1} = \sum_{k=0}^{\infty} (k+1)x^k \\ &= 1 + 2x + 3x^2 + \dots \\ \frac{2}{(1-x)^3} &= \sum_{k=0}^{\infty} k(k-1)x^{k-2} = \sum_{k=0}^{\infty} (k+2)(k+1)x^k \\ &= 2 + 6x + 12x^2 + \dots \end{aligned}$$

j. $a_0, a_1, \dots = 0, 1, 4, 9, 16, \dots$

$$k^2 = \underline{1}(k+2)(k+1) + \underline{-3}(k+1) + \underline{1}$$

$$\sum_{k=0}^{\infty} k^2 x^k = \frac{2}{(1-x)^3} - \frac{3}{(1-x)^2} + \frac{1}{1-x}$$

$$= \frac{x+x^2}{(1-x)^3}$$

Note: the values $(k+2)(k+1)$ refer to the $\left(\binom{2}{k}\right)$ and so on

---

Example. How many ways can you fill a bag with n fruits given the following conditions:

- the number of apples is even
- the number of bananas is a multiple of 5
- the number of oranges is ≤ 4
- the number of pears is ≤ 1

Solution. Use a generating function:

$$f(x) = \underbrace{(1+x^2+x^4+\dots)}_{\text{apples}} + \underbrace{(1+x^5+x^{10}+\dots)}_{\text{bananas}} + \underbrace{(1+x+x^2+x^3+x^4)}_{\text{oranges}} + \underbrace{(1+x)}_{\text{pears}}$$

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

$$= \text{fundamental generating function (h)} = \sum_{k=0}^{\infty}(k+1)x^k$$

$\therefore$ There are $\boxed{\text{n+1}}$ ways to pack n fruits.

6.4 Practice with Generating Functions

Here's some practice turning sequences to generating functions:

a $\langle 1, 1, 1, 1 \dots \rangle = \frac{1}{1-x}$

b $\langle 2, 2, 2, 2 \dots \rangle = \frac{2}{1-x}$ by doubling above equation

c $\langle 1, -1, 1, -1 \dots \rangle = \frac{1}{1+x}$ by noticing the alternation of signs, so we can substitute $-x$ for x

d $\langle 1,0,1,0\ldots\rangle = \frac{1}{1-x^2}$ by noticing we only want the even powers, so we can substitute x^2 for x

e $\langle 0,1,0,1\ldots\rangle = \frac{x}{1-x^2}$ by noticing we can multiply the solution the last problem by x to shift the start of the sum.

f $\langle 1,2,4,8\ldots\rangle = \frac{1}{1-2x}$ by noticing we can get powers of 2 by replacing x with $2x$

g $\langle 1,\frac{1}{2},\frac{1}{6},\frac{1}{24},\ldots\rangle = \frac{e^x-1}{x}$ by noticing the similarity to the expansion of the exponential, but we have to shift it down by killing the first term and lowering the powers.

h $\langle 1,2,3,4,\ldots\rangle = \frac{d}{dx}\frac{1}{1-x} = \frac{1}{(1-x)^2}$ because taking a derivative multiplies each term by its index.

i $\langle 2,6,12,20,30,\ldots\rangle = \frac{d^2}{dx^2}\frac{1}{1-x} = \frac{2}{(1-x)^3}$ by applying the above trick twice.

j $\langle 0,1,4,9,16,\ldots\rangle = ?$
Recall that

$$k^2 = 1(k+2)(k+1) - 3(k+1) + 1$$

where the coefficients are Stirling numbers of the second kind. However, we already have expressions for the generating functions for the falling factorials:

$$\begin{aligned}(k+2)(k+1) &\to \frac{d^2}{dx^2}\frac{1}{1-x} = \frac{2}{(1-x)^3}\\ (k+1) &\to \frac{d}{dx}\frac{1}{1-x} = \frac{1}{(1-x)^2}\\ 1 &\to \frac{1}{1-x}\end{aligned}$$

This gives us our answer $\frac{2}{(1-x)^3} - \frac{3}{(1-x)^2} + \frac{1}{1-x} = \frac{x+x^2}{(1-x)^3}$

6.5 Multiplication of Generating Functions

Let

$$\begin{aligned}A(x) &= a_0x^0 + a_1x^1 + a_2x^2 + \ldots = \sum_{i\geq 0} a_ix_i\\ B(x) &= b_0x^0 + b_1x^1 + b_2x^2 + \ldots = \sum_{i\geq 0} b_ix_i\end{aligned}$$

Let $C(x) = A(x) \cdot B(x)$. What is it's corresponding sequence?
We have to take the *Cauchy product*.

$$C(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \dots$$
$$C_n = \sum_{k=0}^{n} a_k b_{n-k}$$

Consider the two functions

$$A(x) = \text{anything}$$
$$B(x) = 1 + x + x^2 + x^3 + \dots$$
$$C(x) = A(x)B(x) = a_0 + (a_0 + a_1)x + \dots = \sum_{i=0}^{k} a_i x^k$$

Thus we arrive at the following identity:

Theorem 6.1. *If $A(x)$ be the ordinary generating function for $\langle a_0, a_1, a_2 \dots \rangle$. Then, $A(x)/(1-x)$ for $\langle a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots \rangle$*

Let us now consider $A(x) = B(x) = \frac{1}{1-x}$ Recall the following theorem:

$$\sum \frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \left(\!\!\binom{n}{k}\!\!\right) x^k$$

$$C(x) = \langle 1, 2, 3, 4, 5, \dots \rangle$$
$$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} \left(\!\!\binom{2}{k}\!\!\right) x^k$$
$$= \sum \binom{k+1}{k} x^k$$
$$= \sum (k+1)x^k$$

Now let us consider $B(x) \cdot C(x)$

$$\langle 1, 3, 6, \dots \rangle = \frac{1}{(1-x)^3}$$
$$= \sum_{k=0}^{\infty} \left(\!\!\binom{3}{k}\!\!\right) x^k$$
$$= \sum_{k=0}^{\infty} \binom{k+2}{2} x^k$$
$$= \sum_{k=1}^{\infty} \frac{k(k+1)}{2} x^{k-1}$$

This gives us the formula for the triangular numbers. We can go further and get the formula for the tetrahedral numbers.

$$\begin{aligned} D(x) &= \frac{x}{(1-x)^3} = 0 + x + 3x^2 + 6x^3 + 10x^4 + \ldots = \sum_{k=0}^{n} \frac{k(k+1)}{2} x^k \\ E(x) &= D(x) \cdot B(x) = \frac{x}{(1-x)^4} + x \cdot \sum_{k=0}^{\infty} \left(\!\!\binom{4}{k}\!\!\right) x^k \\ &= \sum_{k=0}^{\infty} \binom{k+3}{3} x^{k+1} = \sum_{k=1}^{\infty} \frac{k(k+1)(k+2)}{6} x^k \end{aligned}$$

Now it seems that, by extending this process of computing generating functions for hypertetrahedral numbers and equation coefficients.

$$\sum_{k=1}^{n} k^{\overline{m}} = \frac{n^{\overline{m+1}}}{m+1}$$

This is the power rule for $k^{\overline{m}}$ (finite integrals). For instance, $1^{\overline{4}} + 2^{\overline{4}} + 3^{\overline{4}} + 4^{\overline{4}} + 5^{\overline{4}} + 6^{\overline{4}} = \frac{6^{\overline{5}}}{5}$.

Problem 1. Find $\sum_{i=1}^{n} i^2$

Solution We can write $i^2 = i^{\overline{2}} - i^{\overline{1}}$, and we also know $\sum_{i=1}^{n} i^{\overline{1}} = \frac{n(n+1)}{2}$ and $\sum_{i=1}^{n} i^{\overline{2}} = \frac{n(n+1)(n+2)}{3}$, so we can subtract and simplify, getting $\frac{n(n+1)(2n+1)}{6}$. ■

Problem 2. Find $\sum_{i=1}^{n} i^3$.

Solution Start by expanding the rising factorial in terms of power.

$$\sum i^3 = \sum i^{\overline{3}} - 3\sum i^2 - 2\sum i = \frac{n^{\overline{4}}}{4} - \frac{n(n+1)(2n+1)}{2} - n(n+1)$$

■

6.6 More Applications of Generating Functions

A food counting problem

Problem 1. Fill a bag with n pieces of fruit GIVEN: The number of apples is even, the number of bananas is a multiple of 5, the number of oranges is at most 4, and the number of pears is at most 1. How many ways can I do this?

Solution
To solve this problem, let's find find a generating function that represents the situation. To do so, let's breakdown the function into its apples, bananas, oranges, and pears terms:

Apples: We want 0, 2, 4, ... apples. We can write this as $(x^0 + x^2 + x^4 + x^6 + ...) = (1 + x^2 + x^4 + x^6 + ...)$. This is also equal to $\frac{1}{1-x^2}$.

Bananas: We want 0, 5, 10, ... oranges. We can write this as $(1 + x^5 + x^10 + x^15 + ...)$, or $\frac{1}{1-x^5}$.

Oranges: We want 0, 1, 2, 3, or 4 oranges. We can write this as $(1 + x + x^2 + x^3 + x^4)$. To write this as a fraction, let's make use of the formula for a truncated series: $(1 - x^{n+1}) = (1 - x)(1 + x + x^2 + ... + x^n)$. From this formula, we can see that we can write the number oranges as $\frac{1-x^5}{1-x}$.

Pears: We want either 0 or 1 pear, or $(1 + x)$.

If we multiply all of the components together, we get:

$g(x) = (1+x^2+x^4+x^6+...)(1+x^5+x^10+x^15+...)(1+x+x^2+x^3+x^4)(1+x) = \frac{1}{1-x^2} * \frac{1}{1-x^5} * \frac{1-x^5}{1-x} * (1 + x) = \frac{1}{(1-x)^2}$

$\frac{1}{(1-x)^2}$ has the form of the summation of a multiset: $\sum_{k=0}^{\infty} \left(\!\binom{2}{k}\!\right) x^k = \sum_{k=0}^{\infty}(k+1)x^k$. To find the number of ways to fill the bag with fruit, we simply find the coefficient of x^n in the expansion of the summation. In other words, there are:

$\boxed{(n + 1) \text{ ways}}$.

■

Making Change for $1

Problem 2. Write a generating function for making change given 1¢, 5¢, 10¢, 25¢, and 50¢ coins.

Solution
As with the fruit problem, let's create a generating function for the scenario. We will be working in terms of cents.

1¢: $(1 + x + x^2 + x^3 + ...) = \frac{1}{1-x}$

5¢: $(1 + x^5 + x^10 + ...) = \frac{1}{1-x^5}$

10¢: $(1 + x^10 + x^20 + ...) = \frac{1}{1-x^{10}}$

25¢: $(1 + x^25 + x^50 + ...) = \frac{1}{1-x^{25}}$

50¢: $(1 + x^50 + x^100 + ...) = \frac{1}{1-x^{50}}$

By multiplying all of the terms together, we have the generating function:

$g(x) = \frac{1}{(1-x)(1-x^5)(1-x^{10})(1-x^{25})(1-x^{50})}$

To find the number of ways we can make change for $1, we find the coefficient of x^{100}. This is $\boxed{293}$.
What if there are coins available in every single denomination? Then we have...

1¢: $(1 + x + x^2 + x^3 + ...) = \frac{1}{1-x}$

2¢: $(1 + x^2 + x^4 + ...) = \frac{1}{1-x^2}$

3¢: $(1 + x^3 + x^6 + ...) = \frac{1}{1-x^3}$

4¢: $(1 + x^4 + x^8 + ...) = \frac{1}{1-x^4}$

n¢: $(1 + x^n + x^2n0 + ...) = \frac{1}{1-x^n}$

By multiplying all of the terms together, we have the generating function:

$g(x) = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^n)}$

This is also the generating function for integer partitions.

$g(x) = \prod_{k=0}^{n} \frac{1}{1-x^k} = \sum_{r>0} P(r)x^r$

P(r) is the is the number of integer partitions of r. ■

Theorem 6.2. *The number of partitions of n into distinct parts r is the number of partitions of n into odd parts.*

Distinct parts is when you split the number into parts but the sum doesn't include 2 of the same number. For example, $8 = 1 + 7$ is distinct because 1 and 7 are different. However $8 = 4+2+2$ is not because you have two 2's.

Odd parts are those that are made of a repeated sum of only odd numbers, that can be repeated as many times as one pleases. For example, $8 = 3+3+1+1$ is fine because it contains only odds. However, $8 = 3+3+2$ is not because 2 is an even number.

Generating Functions:

Distinct parts: $g(x) = (1+x)(1+x^2)(1+x^3)...$

Odd parts: $g(x) = (\frac{1}{1-x})(\frac{1}{1-x^3})(\frac{1}{1-x^5})...$

Claim they are identical. So set both generating functions equal and use the trick that $1+x = \frac{1-x^2}{1-x}$

$(1+x)(1+x^2)(1+x^3)... = (\frac{1}{1-x})(\frac{1}{1-x^3})(\frac{1}{1-x^5})...$

$(\frac{1-x^2}{1-x})(\frac{1-x^4}{1-x^2})(\frac{1-x^6}{1-x^3})... = (\frac{1}{1-x})(\frac{1}{1-x^3})(\frac{1}{1-x^5})...$

We notice that term cancel neatly to provide that the two sides are directly equal and therefore this theorem has been proved.

7 Solving Recurrences

7.1 Intro to Solving Recurrence Equations

Problem 3. Given $a_n = a_{n-1} + 8a_{n-2} - 12a_{n-3}$; $a_0 = 2, a_1 = 3$, $a_2 = 19$, find the generating function $g(x) = \sum_{n=0}^{\infty} a_n x^n$ and formula for a_n.

Solution
Let's start with $g(x) = \sum_{n=0}^{\infty} a_n x^n$

Since we know the first three terms from our initial condition, we can add up our base cases and the summation of a_n from $n = 3$ to $n = \infty$.

$g(x) = 2 + 3x + 19x^2 + \sum_{n=3}^{\infty} a_n x^n$

We know the recurrence relation so we can substitute it into the equation we have above

$g(x) = 2 + 3x + 19x^2 + \sum_{n=3}^{\infty}(a_{n-1} + 8a_{n-2} - 12a_{n-3})x^n$

and expand it properly

$g(x) = 2 + 3x + 19x^2 + \sum_{n=3}^{\infty} a_{n-1}x^n + \sum_{n=3}^{\infty} 8a_{n-2}x^n - \sum_{n=3}^{\infty} 12a_{n-3}x^n$

Now, we need to make some manipulations. First, we want the subscript of each of the a_n's to match the power to which each x is being raised. To do so, let's factor out the coefficients and the appropriate number of x's from each term.

$g(x) = 2+3x+19x^2+x\sum_{n=3}^{\infty} a_{n-1}x^{n-1}+8x^2\sum_{n=3}^{\infty} a_{n-2}x^{n-2}-12x^3\sum_{n=3}^{\infty} a_{n-3}x^{n-3}$

The second manipulation involves shifting the indices such that the term within the summation is a_nx^n.

$g(x) = 2 + 3x + 19x^2 + x\sum_{n=2}^{\infty} a_nx^n + 8x^2\sum_{n=1}^{\infty} a_nx^n - 12x^3\sum_{n=0}^{\infty} a_nx^n$

Now that we have the new summations in terms of a_nx^n, they can all be rewritten using the original $g(x)$ function minus the initial terms that are excluded from the summation:

$g(x) = 2 + 3x + 19x^2 + x(g(x) - a_0 - a_1x) + 8x^2(g(x) - a_0) - 12x^3g(x)$
$= 2 + 3x + 19x^2 + x(g(x) - 2 - 3x) + 8x^2(g(x) - 2) - 12x^3g(x)$

Given this equation, we can finally solve for $g(x)$ by moving terms around. After we do this, we can see that our final equation for $g(x)$ is

$\boxed{g(x) = \frac{2+x}{1-x-8x^2-12x^3}}$

****Notice**: *If we move all of the terms in the original a_n equation to one side, we obtain $a_n - a_{n-1} - 8a_{n-2} + 12a_{n-3} = 0$. This resembles the denominator of our final $g(x)$ equation.*

Now let's find the formula for a_n. With our equation for $g(x)$, we can factor the denominator into $(1 + 3x)(1 - 2x)^2$ to determine an equation for a_n. More specifically, we can use *partial fraction decomposition* to breakdown the function into terms that will be more useful to us.

$g(x) = \frac{2+x}{1-x-8x^2-12x^3} = \frac{A}{1+3x} + \frac{B}{1-2x} + \frac{C}{(1-2x)^2}$

To conduct partial fraction decomposition, we multiply the denominator of $g(x)$ on both sides of the equation.

$2 + x = A(1 - 2x)^2 + B(1 + 3x)(1 - 2x) + C(1 + 3x)$

Once we solve this equation, by plugging in different values for x, we get $A = \frac{3}{5}, B = \frac{2}{5}, C = 1$. This allows as to rewrite $g(x)$ as a sum of fractions.

$g(x) = \frac{3}{5}(\frac{1}{1+3x}) + \frac{2}{5}(\frac{1}{1-2x}) + \frac{1}{(1-2x)^2}$

Looking closer, we notice that each fraction can be rewritten as a summation. We can convert the equations by using the following principles:

1) $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ and 2) $\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \left(\!\binom{n}{k}\!\right) x^n$

With these principles, we get the following equation:

$g(x) = \frac{3}{5}\sum_{n=0}^{\infty}(-3x)^n + \frac{2}{5}\sum_{n=0}^{\infty} 2x^n + \sum_{n=0}^{\infty}(n + 1)(2x)^n$

We can now use this equation to achieve our final equation for a_n. To do so, we simply remove the summations and the x^n's from the equation.:

$\boxed{a_n = \frac{3}{5}(-3)^n + \frac{2}{5}(2^n) + (n + 1)2^n}$

■

Problem 4. Given $a_n = 6a_{n-1} - 9a_{n-2}$; $a_0 = 1, a_1 = 9$, find a_n.

Solution We find the generating function....

$g(x) = \sum_{n=0}^{\infty} a_n x^n$

$g(x) = 1 + 9x + \sum_{n=2}^{\infty}(6a_{n-1} - 9a_{n-2})x^n$

$g(x) = 1 + 9x + \sum_{n=2}^{\infty} 6a_{n-1}x^n - \sum_{n=2}^{\infty} 9a_{n-2}x^n$

$g(x) = 1 + 9x + 6x\sum_{n=2}^{\infty} 6a_{n-1}x^{n-1} - 9x^2\sum_{n=2}^{\infty} a_{n-2}x^{n-2}$

$g(x) = 1 + 9x + 6x\sum_{n=1}^{\infty} 6a_n x^n - 9x^2\sum_{n=0}^{\infty} a_n x^n$

$g(x) = 1 + 9x + 6x(g(x) - a_0) - 9x^2 g(x)$

$g(x)(1-6x-9x^2) = 1+9x-6x$

$g(x) = \frac{1+3x}{1-6x-9x^2}$

Then, we use partial fractions...

$\frac{1+3x}{1-6x-9x^2} = \frac{A}{1-3x} + \frac{B}{(1-3x)^2}$

$1+3x = A(1-3x)+B$

If $x = 1/3 ... 2 = B$
If $x = 0 ... 1 = A+2$, $A = -1$

This gives us an expression like so...

$g(x) = -\frac{1}{1-3x} + \frac{2}{(1-3x)^2}$

Using summation principles mentioned above, we get...

$g(x) = -1\sum_{n=0}^{\infty}(3x)^n + 2\sum_{n=0}^{\infty}(n+1)(3x)^n$

$a_n = (-1)3^n + 2(n+1)3^n$

$a_n = 3^n(-1+2n+2)$

and

$a_n = (2n+1)3^n$

■

Problem 5. given $a_n = -3a_{n-1} + 10a_{n-2} + 3(2^n)$; $a_0 = 1, a_1 = 6$, find a_n.

Solution We will use the steps from above to find a_n.

First let's find the generating function:

$g(x) = 0 + 6x + \sum_{n=2}^{\infty} a_n x^n$

$g(x) = 6x + \sum_{n=2}^{\infty}(-3a_{n-1} + 10a_{n-2} + 3(2^n))x^n$

$g(x) = 6x + -3\sum_{n=2}^{\infty} a_{n-1}x^n + 10\sum_{n=2}^{\infty} a_{n-2}x^n + 3\sum_{n=2}^{\infty}(2x)^n$

$g(x) = 6x - 3x\sum_{n=2}^{\infty} a_{n-1}x^{n-1} + 10x^2\sum_{n=2}^{\infty} a_{n-2}x^{n-2} + 3\sum_{n=2}^{\infty}(2x)^n$

$g(x) = 6x - 3x\sum_{n=1}^{\infty} a_n x^n + 10x^2\sum_{n=0}^{\infty} a_n x^n + 3\sum_{n=2}^{\infty}(2x)^n$

$g(x) = 6x - 3x(g(x) - 0) + 10x^2(g(x)) + 3(\frac{1}{1-2x} - 1 - 2x)$

$g(x)[1 + 3x - 10x^2] = 6x + \frac{3}{1-2x} - 3 - 6x = \frac{6x}{1-2x}$

$g(x) = \frac{6x}{(1-2x)(1+3x-10x^2)} = \frac{6x}{(1-2x)^2(1+5x)}$

Now for a_n:

$\frac{6x}{(1-2x)^2(1+5x)} = \frac{A}{1-2x} + \frac{B}{(1-2x)^2} + \frac{C}{1+5x}$

By solving this partial fraction equation, we get $A = \frac{-12}{49}$, $B = \frac{6}{7}$, and $C = \frac{-30}{49}$. Since these are messy numbers, we will hold off on substituting them into our equations until the end.

$g(x) = A\sum_{n=0}^{\infty} 2^n x^n + B\sum_{n=0}^{\infty}(n+1)2^n x^n + C\sum_{n=0}^{\infty}(-5)^n x^n$

$a_n = A * 2^n + B(n+1)2^n + C(-5)^n$

Once we plug in the values of A, B, and C into the equation, we get our final equation for a_n:

$\boxed{a_n = \frac{-12}{49}2^n + \frac{6}{7}(n+1)2^n + \frac{-30}{49}(-5)^n}$

■

7.2 Generating Function for Catalan Numbers

Recall:

$$C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i}$$
$$C_0 = C_1 = 1$$

Or in other words: $C_{n+1} = \sum_{i=0}^{n} C_i C_{n-1}$

Let's find a mathematical, instead of combinatorial, formula for C_n:
Define $f(x) = \sum_{n=0}^{\infty} C_n x^n$
Notice that $f(x) = C_0 + C_1 x + C_2 x^2 + C_3 x^3 + ...$
$f(x)^2 = C_0^2 + (C_0 C_1 + C_1 C_0)x + (C_0 C_2 + C_1 C_1 + C_2 C_0)x^2 + ...$
$= C_1 + C_2 x + C_3 x^2 + C_4 x^3 + ...$
$xf(x)^2 = C_1 x + C_2 x^2 + C_3 x^3 + C_4 x^4 + ...$
$xf(x)^2 = f(x) - C_0 = f(x) - 1$
$xf(x)^2 - f(x) + 1 = 0$
Now, use the quadratic formula to get:
$f(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$
However, we need to express this in series notation, in order to directly know the nth coefficient.

Recall from p.20 of Unit 1, Section 3.2:
$(1-x)^{\frac{1}{2}} = \frac{\sum \frac{1}{2}^{\underline{k}}}{k!} x^k$
$= 1 - \frac{1}{2} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \frac{1}{4^n} x^{n+1}$
So, $(1-4x)^{\frac{1}{2}} = 1 - \frac{1}{2} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \frac{1}{4^n} x^{n+1}$
$(1-4x)^{\frac{1}{2}} = 1 - 2 \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} x^{n+1}$

Based on what we previously found, $(1-4x)^{\frac{1}{2}} = 1 - 2 \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} x^{n+1}$, we know to choose the solution of $f(x) = \frac{1-\sqrt{1-4x}}{2x}$.

Now, we simplify, to get that the generating function for the Catalan Numbers is:

$$\boxed{f(x) = \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} x^n}$$

7.3 Method of Undetermined Coefficients

General Setup

Given a recursive function defined as $a_n + Aa_{n-1} + Ba_{n-2} = 0$, we can see that $\sum_{n=2}^{\infty} (a_n + Aa_{n-1} + Ba_{n-2}) = 0$.

If we decompose this summation, we notice that, if we define $g(x) = \sum_{n=0}^{\infty} a_n x^n$ to be the OGF of the recurrence relationship:

$$\sum_{n=2}^{\infty} a_n x^n = g(x) - a_0 - a_1 x$$

$$\sum_{n=2}^{\infty} A a_{n-1} x^n = Ax(g(x) - a_0)$$

$$\sum_{n=2}^{\infty} B a_{n-2} x^n = Bx^2 g(x)$$

Therefore, $(g(x) - a_0 - a_1 x) + Ax(g(x) - a_0) + Bx^2 g(x) = 0$. Rearranging and factoring $g(x)$ out of the expression, we get $(1 + Ax + Bx^2)g(x) = (a_1 + Aa_0)x + a_0 = Cx + D$ for appropriately- defined constants C and D. Then, if we define r_1 and r_2 such that $(1 - r_1 x)(1 - r_2 x) = 1 + Ax + Bx^2$:

$$g(x) = \frac{Cx + D}{1 + Ax + Bx^2} = \frac{E}{1 - r_1 x} + \frac{F}{1 - r_2 x}$$

Case One: $r_1 \neq r_2$

If we rearrange the equation $(1 - r_1 x)(1 - r_2 x) = 1 + Ax + Bx^2$ (divide both sides by x^2 and replace $1/x$ wih x), we obtain $(x - r_1)(x - r_2) = x^2 + Ax + B$. Then, using this result, we can rewrite $g(x) = E \sum_{n=0}^{\infty} r_1^n x^n + F \sum_{n=0}^{\infty} r_2^n x^n$. Then, because we defined $g(x)$ as the OGF of the recurrence relationship, the generalized $a_n = Er_1^n + Fr_2^n$, where we can solve for the arbitrary E and F.

Remark. *As a general method, we can follow the below steps to determine a generalized closed form for a recursion given by $a_n + Aa_{n-1} + Ba_{n-2} = 0$:*

Step 1: *Solve $(x - r_1)(x - r_2) = x^2 + Ax + B$.*

Step 2: *Write $a_n = C_1 r_1^n + C_2 r_2^n$ (which correspond to E and F from before).*

Step 3: *Use initial conditions (most often given as a_0 and a_1) to solve C_1 and C_2.*

Example . Determine a closed form for a_n given the recursion $a_n = 7a_{n-1} - 10a_{n-2}$; $a_0 = 0, a_1 = 7$.

Solution

Step 1: Moving everything to the LHS, we get $a_n - 7a_{n-1} + 10a_{n-2} = 0$. Then, $x^2 - 7x + 10 = (x - 5)(x - 2) = 0$. Therefore, $r_1 = 5$ and $r_2 = 2$

Step 2: We can write the general $a_n = C_1 5^n + C_2 2^n$.

Step 3: We will now plug in the two base cases:
$a_0 = 0 = C_1 + C_2$
$a_1 = 7 = 5C_1 + C_2$

Step 4: Solving, we obtain $C_1 = \frac{7}{3}$ and $C_2 = -\frac{7}{3}$

Step 5: Putting this all together, we obtain $\boxed{a_n = \frac{7}{3}5^n - \frac{7}{3}2^n}$.

■

Case Two: $r_1 = r_2 = r$

Taking the definition of r_1 and r_2 such that $(1-r_1x)(1-r_2x) = 1+Ax+Bx^2$:

$$g(x) = \frac{Cx+D}{1+Ax+Bx^2} = \frac{E}{1-r_1x} + \frac{F}{1-r_2x}$$

we replace r_1 and r_2 with r since they are all equal, resulting in:

$$\begin{aligned} g(x) = \frac{Cx+D}{1+Ax+Bx^2} &= \frac{Cx+D}{(1-rx)^2} = \frac{E}{1-rx} + \frac{F}{(1-rx)^2} \\ &= E\sum_{n=0}^{\infty} r^n x^n + F\sum_{n=0}^{\infty} \left(\!\!\binom{2}{n}\!\!\right) r^n x^n \end{aligned}$$

thus giving us:

$$\begin{aligned} a_n &= Er^n + F(n+1)r^n \\ &= E'r^n + F'nr^n \end{aligned}$$

which is the Standard form for a quadratic with a repeated root.

Remark. *If r_i has multiplicity 3 or more* $\rightarrow a_n = Er^n + Fnr^n + Gn^2r^n + \dots$

Example . Determine a closed form for a_n given the recursion $a_n = -6a_{n-1} - 9a_{n-2}$; $a_1 = 1, a_2 = 2$.

Remark. *Initial conditions do not always have to be a_0 and a_1.*

Solution *Step 1:* Moving everything to the LHS, we get $a_n + 6a_{n-1} + 9a_{n-2} = 0$. Then, $x^2 + 6x + 9 = (x+3)^2 = 0$. Therefore, $r_1 = r_2 = -3$

Step 2: We can write the general $a_n = C_1(-3)^n + C_2n(-3)^n$.

Step 3: We will now plug in the two base cases:
$a_1 = 1 = 3C_1 + 3C_2$

$a_2 = 2 = 9C_1 + 18C_2$

Step 4: Solving, we obtain $C_1 = -\frac{8}{9}$ and $C_2 = \frac{5}{9}$

Step 5: Putting this all together, we obtain $\boxed{a_n = -\frac{8}{9}(-3)^n + \frac{5}{9}n(-3)^n}$.

■

Recurrence Problems Classwork

Example 1. $a_n = 2a_{n-1} + n - 1; a_0 = 1$

Solution

$$\begin{aligned} g(x) &= 1 + 2xg(x) + \sum_{n=1}^{\infty} nx^n - \sum_{n=1}^{\infty} x^n \\ g(x)(1-2x) &= 1 + \sum_{n=1}^{\infty} nx^n - \sum_{n=1}^{\infty} x^n \\ &= 1 + \frac{x}{(1-x)^2} - \left(\frac{1}{1-x} - 1\right) \\ &= 2 + \frac{x}{(1-x)^2} - \frac{1}{(1-x)} \\ &= 2 + \frac{2x-1}{(1-x)^2} \\ g(x) &= \frac{2}{1-2x} - \frac{x}{(1-x)^2} \\ &\rightarrow \boxed{a_n = 2(2)^n - \left(\binom{2}{n}\right)} \end{aligned}$$

■

7.4 Recursive Problems with Inhomogeneous Terms

Problem 1. We draw n lines in the plane. How many regions can we create?

Solution We can solve this with recursion. Obviously, $a_0 = 1$, but consider the a_{n-1} case. If we add another line, consider every place it can intersect. There are $n-1$ lines to intersect with, and if we have $n-1$ arbitrary lines, putting a line through them adds n regions to the total (imagine that the lines are all parallel since their intersections have nothing to do with the new line). Thus, we write $a_n = a_{n-1} + n$ with $a_0 = 1$, giving us

$$a_n = a_0 + \sum_{k=1}^{\infty} k = 1 + \frac{k(k+1)}{2} = \boxed{\left(\!\!\binom{3}{n-1}\!\!\right) + 1}.$$

■

Problem 2. How many sequences of length n using $0 - 3$ contain an even number of zeroes?

Solution Since we're using sequences, we need to consider even and odd zeros. Construct two sequences O_n and E_n where $O_0 = 0$ and $E_0 = 1$. Then, we have $E_{n+1} = 3E_n + O_n$. We also have $O_n + E_n = 4^n$ since every sequence consists of an odd or even number of zeroes and there are four choices per digit in the sequence.
Thus, we write $E_{n+1} = 3E_n + (4^n - E_n) = 2E_n + 4^n$. If we instead write this as $E_n = 2E_{n-1} + 4^{n-1}$, we can solve for our generating function as follows:

$$(1-2x)g(x) = 1 + \frac{x}{1-4x} = \frac{1-3x}{1-4x}$$

$$\rightarrow g(x) = \frac{1-3x}{(1-2x)(1-4x)} = \frac{1/2}{1-2x} + \frac{1/2}{1-4x}$$

so we have $E_n = \boxed{\frac{2^n + 4^n}{2}} = 2^{2n-1} + 2^{n-1}$. ■

7.5 Extra Terms (Inhomogeneous Terms)

Definition. *Say we have $\sum_{i=0}^{n} c_i a_i = f$ for some function f. Then f is the **forcing function** or **inhomogeneity** of the recursion.*
Definition. *If we have $\sum_{i=0}^{n} c_i a_i = f$ as before, then the solution to the equation $\sum_{i=0}^{n} c_i a_i = 0$ is called the **homogeneous** solution to the equation while the solution to the original equation is called the **particular** solution. Note that neither uses the initial conditions.*
We'll need both solutions to solve recurrences in general since the real solution will be a linear combination of what we have because initial conditions are annoying. Specifically, our particular solution cannot change, but we can always add a multiple of the homogeneous solution to get our final answer based on the initial equations. If $p(n)$ is our particular solution and $h(n)$ is our homogeneous, the solution will always be of the form $p(n) + c \cdot h(n)$ for some constant c.

Problem 3. Given $a_n + 2a_{n-1} = n + 3, a_0 = 3$, solve for a_n.

Solution The homogeneous solution is $(-2)^n$ (or a nonzero constant multiple of that) because our characteristic equation is $x^2 + 2x = 0$ and 0 clearly doesn't work.
Let's look for the particular solution now. Consider that the inhomogeneity is linear. We agree that $a_n = Bn + D$ by the **Method of Undetermined Coefficients,** which is essentially a way of "guessing" what the solution will look like. We have

$$a_n + 2a_{n-1} = Bn + D + 2(B(n-1) + D) = 3nB + 3D - 2B = n + 3,$$

so we have $B = \frac{1}{3}$ and $3D - 2B = 3D - \frac{2}{3} = 3 \to D = \frac{3+2/3}{3} = \frac{11}{9}$. Thus, our particular solution is $a_n = \frac{1}{3}n + \frac{11}{9}$.
Finally, let's combine the two. At $n = 0$, our particular says $\frac{11}{9}$, but our homogeneous says 1. Thus, we have $\frac{11}{9} + c \cdot 1 = 3$ since the solution is of the form $p(n) + c \cdot h(n)$. Thus, $c = \frac{16}{9}$. This gives us the solution

$$a_n = \boxed{\frac{1}{3}n + \frac{11}{9} + \frac{16}{9}(-2)^n}.$$

■

Let's now look at the original two problems again.

Problem 2 (revisit). Let $a_n = 4^{n-1} + 2a_{n-1}$. Solve for a_n.

Solution The homogeneous is clearly 2^n, but the particular is less clear-cut. Writing $a_n = c4^n$, we have $c(4^n - 2 \cdot 4^{n-1}) = 4^{n-1}$ which gives $c = \frac{1}{2}$. If we then write $a_n = \frac{1}{2}4^n + d \cdot 2^n$ and use $a_1 = 3$, we have $a_1 = 2 + d \cdot 2 = 3 \to d = \frac{1}{2}$, so we get $a_n = \frac{4^n+2^n}{2}$ as before. ■

Problem 1 (revisit). Let $a_n = a_{n-1} + n$. Solve for a_n.

Solution The homogeneous for $a_n = a_{n-1} + n$ is literally 1. However, to find the particular here, the Method of Undetermined Coefficients says that we must use a quadratic since a linear term will cancel if we set $a_n - a_{n-1} = n$. (In more specific terms, if we write $a_n = Bn + D$, we find that $a_n - a_{n-1} = Bn + D - B(n-1) + D = B$, leaving us with no information.) Thus, write $a_n = An^2 + Bn + C$. Using $a_0 = 1, a_1 = 2, a_2 = 4$, we have $C = 1, A+B+C = 2$, and $4A+2B+C = 4$. This gives $A = \frac{1}{2}, B = \frac{1}{2}, C = 1$. Thus, our final solution is $a_n = \frac{1}{2}n^2 + \frac{1}{2}n + 1 + d$, where d is the coefficient on the homogeneous solution. Taking $a_0 = 1$ again, we get $d = 0$, so the answer is just the particular: $a_n = \boxed{\frac{1}{2}n^2 + \frac{1}{2}n + 1}$ which equals our original answer.

■

7.6 Complex Roots

Consider the series expansion of function $\frac{1}{1+x^2}$. It is trivially true that

$$\frac{1}{1+x^2} = \sum_{n=0}^{\infty} (-1)^n x^{2n}$$

Thus the nth coefficient is 0 if n is odd and $(-1)^k$ if $n = 2k$. Alternatively,

$$\frac{1}{1+x^2} = \frac{A}{1+xi} + \frac{B}{1-xi} = A \sum i^k x^k + B \sum (-i)^k x^k$$

Problem 1. Solve $a_n = -a_{n-2};\ a_0 = 1, a_1 = 1$

Solution We see the characteristic polynomial is x^2+1 with roots $x = \pm i$, so $a_n = A(i)^n + B(-i)^n$. Solving with our initial conditions, our sequence can be represented as

$$a_n = \frac{1}{2i}(i)^n + \frac{-1}{2i}(-i)^n$$

Because i is the fourth root of unity, our sequence cycles with period 4. Alternatively, we can use Euler's identity and De Moivre's Formula to get

$$\begin{aligned} a_n &= \frac{1}{2i}\left(\cos\frac{n\pi}{2} + i\sin\frac{n\pi}{2}\right) + \frac{-1}{2i}\left(\cos\frac{n\pi}{2} - i\sin\frac{n\pi}{2}\right) \\ &= (A+B)\cos\frac{n\pi}{2} + (Ai - Bi)\sin\frac{n\pi}{2} \end{aligned}$$

Thus, we could've instead tried to solve

$$a_n = C\cos\frac{n\pi}{2} + D\sin\frac{n\pi}{2}$$

and avoid using complex numbers in the first place. ■

Problem 2. Solve $a_n = a_{n-1} - a_{n-2};\ a_1 = 1, a_2 = 0$

Solution The characteristic equation $x^2 - x + 1 = 0$ has roots

$$r_\pm = \frac{1 \pm \sqrt{3}}{2} = \exp\left(\pm\frac{i\pi}{3}\right)$$

Thus, we ansatz $a_n = C\cos\frac{n\pi}{3} + D\sin\frac{n\pi}{3}$. Using the initial conditions, we get

$$a_n = \cos\frac{n\pi}{3} + \frac{1}{\sqrt{3}}\sin\frac{n\pi}{3}$$

■

In general, if our roots do not lie on the unit circle, we have to prepend the sines and cosines with powers of the roots. Because of the Conjugate Root Theorem, we are guaranteed that the modulus will factor out nicely.

7.7 Interlude: Bell Numbers

The number of non-empty partitions of a set of n elements is the nth *Bell number*, which obeys relation

$$B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}$$

Recall that

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^{\underline{k}}$$

Let X be some random variable. By linearity of expectation,

$$E[X^n] = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} E[X^{\underline{k}}]$$

If we can find a random variable that obeys $E[X^{\underline{k}}] = 1$, then we can compute the nth Bell number.
Let $X \sim Poisson(\lambda)$. By definition of the Poisson distribution,

$$Pr[X = k] = \frac{\lambda^k}{k!} e^{-\lambda}$$

Our first step is to prove that this a valid probability distribution. Observe

$$Pr[X \geq 0] = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} = e^{-\lambda} \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} = e^{-\lambda} e^{\lambda} = 1$$

Our next step is to find the expected value of X

$$E[X] = \sum_{k=0}^{\infty} \frac{k\lambda^k}{k!} e^{-\lambda} = e^{-\lambda} \lambda \sum_{k=1}^{\infty} \frac{\lambda^{k-1}}{(k-1)!} = e^{-\lambda} \lambda e^{\lambda} = \lambda$$

Rather than use a moment generating function, we shall compute $E[X^n]$ directly.

$$E[X^n] = \sum_{k=0}^{\infty} Pr[X = k] k^n = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} k^n$$

To find $E[X^{\underline{k}}]$, we notice that falling factorials come out ff powers, so we observe the *factorial generating function*, $E[t^X]$

$$E[t^X] = \sum_{k=0}^{\infty} Pr[X = k] t^k = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} t^k = e^{-\lambda} e^{t\lambda} = e^{\lambda(t-1)}$$

It follows, from taking $\frac{\partial^n}{\partial t^n}$, that

$$\sum_{k=0}^{\infty} \frac{k^{\underline{n}} t^{k-n} \lambda^k}{k!} e^{-\lambda} = \lambda^n e^{\lambda(t-1)}$$

Letting $t = 1$, we get

$$\lambda^n = \sum_{k=0}^{n} \frac{k^{\underline{n}} \lambda^k}{k!} e^{-\lambda} = E[X^{\underline{n}}]$$

Further letting $\lambda = 1$, we get $E[X^{\underline{k}}] = 1$. Thus, using the first formulas of the section, we get $B_n = E[X^n]$ where $X \sim Poisson(\lambda = 1)$, but we also know from above that $E[X^n] = \sum_{k=0}^{\infty} \frac{k^n}{k!} e^{-1}$ for this distribution. This gives

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

As a bonus, we can write a recurrence of the Bell numbers:

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$$

To see this, construct the partition contain element a_{n+1} and partition the rest.

8 Exponential Generating Functions

Definition. *A* structure *is a particular organization of the elements of a set or sets.*

For example, some structures include a set, a non-empty set, an even-sized set, a permutation, an increasing permutation, or a function from A into B

Definition. *The exponential generating function for a sequence $f_0, f_1, f_2, f_3 \dots$ is*

$$F(x) = \sum_{k=0}^{\infty} f_n \frac{x^n}{n!}$$

Definition. *$[n]$ is the set $1, 2, \dots, n$, or the set of n elements.*

Theorem 8.1. *If f_n counts the number of F-structures on $[n]$, then*

$$F(x) = \sum_{n=0}^{\infty} f_n \frac{x^n}{n!}$$

is the exponential generating function for the structure F.

Let's look at some examples of exponential generating functions.

- $\frac{1}{1-x}$ is the exponential generating function of $n!$
- e^{ax} is the exponential generating function of a^n

Exponential generating functions add as expected, which corresponds combinatorially to *OR*, or disjoint union. Multiplication of exponential generating function is more involved. Let $A(x) = \sum_p a_p \frac{x^p}{p!}$ and $B(x) = \sum_q b_q \frac{x^q}{q!}$. Then

$$\begin{aligned}
A(x)B(x) &= \sum_{p,q} a_p b_q \frac{x^{p+q}}{p!q!} \\
&= \sum_n \sum_p \frac{a_p b_{n-p} n!}{p!(n-p)!} \frac{x^n}{n!} \\
&= \sum_n \sum_p \binom{n}{p} a_p b_{n-p} \frac{x^n}{n!}
\end{aligned}$$

Thus, if $C(x) = A(x)B(x) = \sum C_n \frac{x^n}{n!}$, then

$$C_n = \sum_p \binom{n}{p} a_p b_{n-p}$$

Recall that the Bell numbers obey recurrence

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

Let $b(x) = \sum B_n \frac{x^n}{n!}$ and let $a(x) = e^x$, the exponential generating function for $(1, 1, 1, \ldots)$. Plugging into the recurrence,

$$\begin{aligned}
\sum_{n=0}^{\infty} B_{n+1} \frac{x^n}{n!} &= \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \binom{n}{k} B_{n-k} \frac{x^n}{n!} \\
b'(x) &= b(x)e^x \\
b(x) = e^{e^x - 1}
\end{aligned}$$

where we use the initial condition $b(0) = 1$. Now, notice

$$b(x) = \frac{1}{e} \sum_{k=0}^{\infty} \frac{(e^x)^k}{k!} = \frac{1}{e} \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{1}{k!} \frac{(kx)^n}{n!}$$

We can pull out our coefficient

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

8.1 Exponential Generating Functions for Structures

Let's consider some structures on sets. Consider some trivial structures:

- a set on $[n]$ is $f_n = 1$, so $F(x) = e^x$
- a non-empty set on $[n]$ is $f_n = 1 - \delta_{0n}$, so $F(x) = e^x - 1$
- an empty set on $[n]$ is $f_n = \delta_{0n}$, so $F(x) = 1$
- a singleton set on $[n]$ is $f_n = \delta_{1n}$, so $F(x) = x$
- a 2-element set on $[n]$ is $f_n = \delta_{2n}$, so $F(x) = \frac{1}{2}x^2$
- an even length set on $[n]$ has $F(x) = \cosh x$
- an odd length set on $[n]$ has $F(x) = \sinh x$

Theorem 8.2. *Addition Property: If G and H are exponential generating functions of structures, then $F = G + H$ is the exponential generating functions of the union of the structures*

To see the above theorem in action, notice that the exponential generating function for empty sets, 1 , added to the exponential generating function for non-empty set, $e^x - 1$, gives the exponential generating function for all sets, e^x

Theorem 8.3. *Multiplication Property: Let g and h be structures on sets and let f be a gh-structure. For set A, if we partition A into disjoint sets $A_1 \cup A_2$, put all elements in A_1 into a g-structure and A_2 into a h-structure, then the exponential generating function of f is $F(x) = G(X)H(x)$*

Example 1. Let us count subsets of $A = [n]$. Partition A into a set and another set (the complement). The number of ways to do this is given by the coefficient

$$f(x) = g(x)h(x) = e^x e^x = e^{2x} = \sum 2^n \frac{x^n}{n!}$$

Thus a set of size n has 2^n different subsets.

Example 2. Let us count non-empty subsets of $A = [n]$. Analogous to above, partition A in g-structure representing non-empty sets and h-structure representing sets. This gives

$$f(x) = g(x)h(x) = (e^x - 1)(e^x) = \sum_{n=0}^{\infty} (2^n - 1) \frac{x^n}{n!}$$

Thus a set of size n has $2^n - 1$ non-empty subsets.

Example 3. Let us count functions from $[n] \to [k]$. Let $A = A_1 \cup A_2 \cup \ldots A_k$ where A_i is the preimage of i in $[n]$, so

$$f(x) = (e^x)^k = \sum_{n=0}^{\infty} k^n \frac{x^n}{n!}$$

Thus we have k^n functions from $[n] \to [k]$

Example 4. Let us count surjective functions from $[n] \to [k]$. By analogy to above problem, we have to let each of sets A_i be nonempty, so we have

$$f(x) = (e^x - 1)^k = \sum k! S(n,k) \frac{x^n}{n!}$$

where we appeal to the 12-fold table. Thus, the exponential generating function of the Stirling numbers of the second kind is

$$\sum_{n=0}^{\infty} S(n,k) \frac{x^n}{n!} = \frac{(e^x - 1)^k}{k!}$$

Let's continue the derivation of the exponential generating function of the Stirling numbers of the second kind.

$$\begin{aligned}
\sum_{n=0}^{\infty} S(n,k) \frac{x^n}{n!} &= \frac{1}{k!} (e^x - 1)^k \\
&= \frac{1}{k!} \sum_{t=0}^{k} \binom{k}{t} e^{tx} (-1)^{k-t} \\
&= \frac{1}{k!} \sum_{t=0}^{k} \binom{k}{t} \sum_{n=0}^{\infty} \frac{(tx)^n}{n!} (-1)^{k-t} \\
&== \frac{1}{k!} \sum_{n=0}^{\infty} \left(\sum_{t=0}^{k} \binom{k}{t} (-1)^{k-t} t^n \right) \frac{x^n}{n!}
\end{aligned}$$

This gives

$$S(n,k) = \frac{1}{k!} \sum_{t=0}^{k} \binom{k}{t} (-1)^{k-t} t^n$$

which we had derived earlier by using Principle of Inclusion and Exclusion

Theorem 8.4. *Composition Property: Let g, h be structures on sets and let $f = g \circ h$, the structure by*

- *partitioning A into an arbitrary number of blocks $A_1 \cup A_2 \cup \ldots A_k$*

- *giving each A_i an h-structure*
- *and giving the partition itself a g-structure*

The exponential generating function obeys $F(x) = G(H(X))$

Example 5. Let us count the number of ways to partition a set. Each of our partitions of A must be non-empty sets, but the structure for the partitions is merely a set, so our exponential generating function is e^{e^x-1}. This gives again our exponential generating function for the Bell numbers.

Example 6. Let us count the number of ways to partition a set into subsets with at least two elements. Our exponential generating function is e^{e^x-1-x}

Example 7. Let us count the number of ways to partition a set into subsets with even number of elements. The exponential generating function is $e^{\cosh x}$

9 Interlude: Calkin-Wilf Tree

9.1 Hyperbinaries

Example 1. What is the 23rd positive rational number?

Solution We need an enumeration of the rational numbers! ■

We introduce the hyperbinary numbers, where we write binary numbers, but allow for multiple representation of numbers by also letting us use the number 2. For example,

$$\begin{aligned} 4 &= 100 \\ &= 20 \\ &= 12 \end{aligned}$$

Let us count the number of ways we can write integer n in hyperbinary, $b(n)$. If we sum $b(n)$, restarting every time we hit a 1, we get powers of 3 because it's just showing the number of strings of 3 different digits. To find a recurrence for $b(n)$, let's casework on the last digit:

- The only way to make an odd number is to take a number and append a 1: $b(2n+1) = b(n)$
- The only ways to make an even number is to take a number and append a 0 (which doubles it) or a 2 (which doubles it and adds 2): $b(2n+2) = b(n+1) + b(n)$

Donald Knuth called this recurrence $fusc(n)$ (fusc for "obfuscate"). Let's return to our original problem of finding the 23rd rational positive number. Define the nth rational number to be $b(n)/b(n+1)$. This list contains every rational in reduced form exactly once.

Let's define the *Calkin-Wilf tree* to be a complete binary tree that has as node n the rational b_n/b_{n+1}. Notice that each node that contains b_n/b_{n+1} has as its left child b_{2n+1}/b_{2n+2} and right child b_{2n+2}/b_{2n+3}. Notice that applying the recurrence that we had earlier yields relations

$$\frac{b_{2n+1}}{b_{2n+2}} = \frac{b_n}{b_n + b_{n+1}}$$
$$\frac{b_{2n+2}}{b_{2n+3}} = \frac{b_n + b_{n+1}}{b_{n+1}}$$

Thus the parent of any node containing x/y is either $x/(y-x)$ or $(x-y)/x$ depend- ing on whether it is a left or right child. However, only one of these numbers is positive, so we can deduce the parent of any node.

We know make the following claims:

Theorem 9.1. $\frac{x}{y} \in T, \frac{x}{y} \neq \frac{1}{1} \implies \gcd(x, y) = 1$

Proof. Assume that $\gcd(x, y) = k > 1$ for at least one $\frac{x}{y} \in T$. Let $\frac{kx'}{ky'}$ be the highest node in the tree. However, by our algorithm for finding the parent of any node, we know the parent must have greatest common divisor at least equal to k because it is $\frac{kx'}{k(y'-x')}$ or $\frac{k(x'-y')}{ky'}$. This contradicts our assmption. ■

Theorem 9.2. $\frac{x}{y} \in \mathbb{Q}^+, \gcd(x, y) = 1 \implies \frac{x}{y} \in T$

Proof. Let S be the set of all rationals not in the tree. Let y be the smallest denominator in S and let x be minimal numerator of a number in S with denominator y. If $x > y$, then $\frac{x-y}{y}$ could not be in the tree because it would have child $\frac{x}{y}$ which, by assumption, isn't in the tree. But $\frac{x-y}{y}$ can't be in S because the way we choose our x and y Otherwise, if $x < y$, consider instead $\frac{x}{y-x}$. ■

Theorem 9.3. *Every rational that appears in the tree appears at most once.*

Proof. Using the same rules as the previous proof, we find the "smallest" x/y that appears twice in the tree. However, it must have its parent appear twice, which would be yet "smaller". ■

Theorem 9.4. *The Calkin-Wilf tree contains every reduced positive rational exactly once.*

A nice theorem

Definition. *A* runlength encoding *takes a number applies the "look-and-say" rule: see the length of each block of repeated digit, then write down its length and the digit.* 444411002 → 44212012

Theorem 9.5. *Consider, starting from the least significant digit of the binary representation of any positive integer n, the length of each run. Letting this be the continued fraction representation of a rational, this gives the nth rational under the ordering given by the Calkin-Wilf tree.*

10 Interlude: Partition Numbers

Definition. *Define the nth partition number, $p(n)$, be the number of ways to write n as a sum of positive integers.*

As an example,

$$\begin{aligned} 5 &= 5 \\ &= 4+1 \\ &= 3+2 \\ &= 3+1+1 \\ &= 2+2+1 \\ &= 2+1+1+1 \\ &= 1+1+1+1+1 \\ p(5) &= 7 \end{aligned}$$

Definition. *Let $p_k(n)$ count the number of ways to partition n into exactly k parts.*

Theorem 10.1.

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n) \frac{d}{dn} \left(\frac{1}{\sqrt{n-1/24}} \sinh\left[\frac{\pi}{k} \sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)} \right] \right)$$

where

$$A_k = \sum_{\substack{\gcd(m,k)=1 \\ m<k}} \exp\left(i\pi \left(S(m,k) - \frac{2mn}{k} \right) \right)$$

Proof. Trivial and left as an exercise to the reader. ∎

Theorem 10.2.
$$p_k(n) \geq \frac{1}{k!}\binom{n-1}{k-1}$$

Proof. Let's look for solutions to

$$x_1 + x_2 + \cdots + x_k = n$$

By stars and bars, we there are $\left(\!\binom{k}{n-k}\!\right) = \binom{n-1}{k-1}$ solutions. On the other hand, each partition of k elements is associated with at most $k!$ compositions. Thus,
$$p_k(n) \geq \frac{1}{k!}\binom{n-1}{k-1}$$

■

A *Ferrers graph* or *Young tableau* is a way of drawing partitions graphically. Each row in the tableau contains as many dots as the the magnitude of the corresponding part in the partition. Let the *transpose* of a partition λ into λ^T be the tableau that you get by swapping rows with columns. A partition λ is *self-conjugate* if $\lambda = \lambda^T$

Theorem 10.3. *The number of self-conjugate partitions of n is equal to the number of partitions of n with distinct odd-sized parts.*

Proof. Any self-conjugate partition has symmetry about the main diagonal. If we select the top row and left-most column together to be one part, this gives an odd sized part. The remainder of the tableaux is still self-conjugate and we recursively get more odd-sized parts. Notice to reverse the proof, we need to have the odd-sized parts be distinct sizes, or else they won't stack correctly.

■

Theorem 10.4. *The number of partitions of n into even-sized parts is equal to the number of partitions of n where each part has even multiplicity.*

Proof. Take the transpose.

■

Theorem 10.5.
$$p_4(n) = p_4(3n)$$

Proof. Let λ be a partition of n with 4 parts. Then construct λ^* by replacing each part λ_i with $n - \lambda_i$. This gives a partition of $3n$ into 4 parts.

■

Trivially, the above proof generalizes to yield $p_k(n) = p_k((k-1)n)$.

Theorem 10.6. $p_k(n) = \sum_{i=1}^{k} p_i(n-k)$

Proof. Consider pre-seeding each of the k parts with a 1. Then we have to partition $n-k$, allowing for empty parts; thus we have to sum over the allowed number of non-empty parts. This corresponds to excising the left-most column in the Young tableuax. ■

Part III
Groups and Group Actions

11 Group Theory

11.1 Introduction to Groups

Definition. A **group** is a set A and an binary operation $\cdot$ (we denote this $G = (A, \cdot)$) where the following four properties hold:

1. *Closure.* A is closed under $\cdot$, that is, if elements $a_1, a_2 \in A$ then $a_1 \cdot a_2 \in A$.
2. *Associativity.* The operation $\cdot$ is associative, that is, if elements $a, b, c \in A$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. *Identity.* There exists an element $e \in A$ such that $e \cdot a = a \cdot e = a$.
4. *Inverse.* There exists an element $a^{-1} \in A$ for any element a such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Note that *commutativity* is **NOT** a necessary property of a group. We call groups such that for elements $a, b \in A$ such that $a \cdot b = b \cdot a$ are *abelian* or commutative.
Here are some examples of sets that are groupsThis is a group. /not groups:

- $G = (\mathbb{Z}, +)$. Yes! All these properties hold.
- $G = (\mathbb{Z}, \times)$. No! 0 does not have a multiplicative inverse, and in fact, no element has an inverse other than ± 1.
- $G = (\mathbb{Q}, \times)$. No! 0 does not have a multiplicative iverse.
- $G = (\mathbb{R}, +)$. Yes! Same reasons as the first group.
- $G = (\{\text{set of all 2-by-2 matrices with integer elements}\}, \cdot)$ No! Not all of these matrices are invertible (have determinant zero).
- $G = (\{\text{set of all 2-by-2 matrices with determinant } 1\}, \cdot)$. Yes! This is actually a special group, $SL(2)$.

Definition. A **subgroup** H of G is $H = (B, \cdot)$ where $B \subseteq A$. These groups must have the same operation, and H must also be a group.
An example of a subgroup: $(5\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$, as it retains all the properties of $\mathbb{Z}$.
Defintion. A **coset** $a \cdot H$ of a subgroup H is the set of elements $\{a \cdot h | h \in H\}$ and $a \in G$.
For example, take the example $2{+}5\mathbb{Z} = \{2, 7, 12, 17, \ldots, -3, -8, -13, -18 \ldots\}$. These are the integers that are $\equiv 2 \mod 5$. Similarly, we can form three other unique cosets (that are 1, 3, and 4 mod 5). Note that cosets are **not** generally groups, as this coset is clearly not a group (no identity, not closed under addition, etc.)
Let's consider the following statements:

- Cosets $a \cdot H \cap b \cdot H = \emptyset$ if $a \neq b$. The converse is not always true - as a counterexample, consider $2 + 5\mathbb{Z}$ and $7 + 5\mathbb{Z}$.
- If $a \cdot H \cap b \cdot H \neq \emptyset$, then $a \cdot H = b \cdot H$.
- If H is finite, $|a \cdot H| = |H|$. This is true since a is invertible.
- Every $g \in G$ is in $a \cdot H$ for some a.

If ALL of these statements are true, then we can conclude that $|G|$ is divisble by $|a \cdot H|$, and furthermore, $|H|||G|$.

11.2 Finite Groups and Subgroups

Define $\mathbb{Z}/4\mathbb{Z}$ or "$\mathbb{Z} \mod 4\mathbb{Z}$" as the group of cosets of the latter in the former. These are obviously $\{4\mathbb{Z}, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3\}$. We'll refer to these as $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. The four is implied in context. This is called a **quotient group**. We can prove that this is a group under addition modulo 4, or $+_4$:

1. **Closure:** Let's make a **Cayley Table** for this group:

$+_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

This is a relatively ludicrous way of proving closure, but it works since every two elements under our operator give another element in the set.

2. **Associativity:** Addition is associative, so $+_4$ inherits this property. We can prove this more formally, but it's not really necessary.
3. **Identity:** The zero element, $\overline{0}$. Trivial.
4. **Inverse:** We can look at the table and find that every element has an inverse.

There's nothing special about the 4, really; $\mathbb{Z}/n\mathbb{Z}$ is a group (for $n \geq 2$) by the same reasoning. This group is surprisingly common, so we'll call it $\mathbb{Z}_n$ in general. (Note that $\mathbb{Z}_1 = \mathbb{Z}$).

What if we try to make a 4-element group under multiplication? The quotient group clearly doesn't work under multiplication since we have a 0 in $\overline{0}$. Even if we get rid of the $\overline{0}$, $\overline{2}$ doesn't have an inverse.
Observe that this is the case because 4 is composite. If we take $\mathbb{Z}_5$ on the other hand, we can fill out a Cayley table:

$\times_5$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

So this is closed. Alternatively, we can simply look at two arbitrary elements of the group $\overline{a} = \overline{5k+a}$ and $\overline{b} = \overline{5l+b}$ which gives

$$\overline{a} \times_5 \overline{b} = (\overline{5k+a}) \times_5 (\overline{5l+b}) = 25kl + 5kb + 5la + ab$$
$$= 5(5kl + kb + la) + ab = 5t + ab \text{ where } t = 5kl + kb + la$$

for some t so $\overline{a} \times_5 \overline{b}$ is in the set.

11.3 Group isomorphism

We define two groups as **isomorphic** if we can map the elements from one to the other such that every possibility remains the same.

Can we map our two groups so far to each other? Well, we can try. Define the function f to go from our first group to our second group. Then, if we set $f(\overline{0}) = \overline{1}, f(\overline{1}) = \overline{2}, f(\overline{2}) = \overline{4}, f(\overline{3}) = \overline{3}$, things are equivalent. (We can also set $\overline{1}, \overline{3}, \overline{4}, \overline{2}$ for the four elements of $\mathbb{Z}_5^*$ in order and get an isomorphism.)

To prove that this works, we can simply construct a Cayley table, but with the elements in a different order. There's nothing stopping us from doing this.

$\times_5$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$

This table is equivalent to the first one.

11.4 More Subgroups

Does $(\mathbb{Z}_4, +_4)$ have subgroups? Yes, it has three: the trivial subgroup, the entire group, and $\{\overline{0}, \overline{2}\}$.

There's an easy way to get this from the table, though. Obviously, all we really need to prove is closure because other properties are basically inherited besides inverses. If we take $\overline{0}$ and $\overline{2}$ in the table...

...we clearly see that only these two elements come up in the "mini-table", and every element has an inverse since there's one $\overline{0}$ in every row and column.

As expected, the sizes of these groups are factors of 4.

11.5 Another Group Example

Can we make another different size-4 group that's not isomorphic to our first group? Remember that both groups we found so far are isomorphic. Well, recall that each group we found so far has our first element, which we'll call a, multiply to one of the other two elements b and c (excluding the identity). However, both of these were proven to be equal, and because every row and column must contain the entire set (think about why: if this weren't the case, we could have two inverses of element), we can't do this. Thus, we set $a \times a = e$. The only way to continue from here without contradiction is to set $a \times b = c$ and $a \times c = b$ since we can't multiply the identity by itself. Now, we have the choice between $b \times b$ equals e or a. As it turns out, the latter is isomorphic to both of the previous groups, so we go with the former and obtain the following table:

$+_2$	$[0,0]$	$[0,1]$	$[1,0]$	$[1,1]$
$[0,0]$	$[0,0]$	$[0,1]$	$[1,0]$	$[1,1]$
$[0,1]$	$[0,1]$	$[0,0]$	$[1,1]$	$[1,0]$
$[1,0]$	$[1,0]$	$[1,1]$	$[0,0]$	$[0,1]$
$[1,1]$	$[1,1]$	$[1,0]$	$[0,1]$	$[0,0]$

This is the $\mathbb{Z}_2 \times \mathbb{Z}_2$ group.

Next question: What's the symmetry group of a rectangle? Well, there are four things that we can obviously do that aren't unique: nothing (e), horizontal and vertical reflection (H and V), and rotation by 180 degrees (R), which we'll set clockwise WLOG. We have $H \times V = V \times H = R, V \times R = H$, and so on, so this happens to be the same as $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$+_2$	e	H	V	R
e	e	H	V	R
H	H	e	R	V
V	V	R	e	H
R	R	V	H	e

We can prove that there are only two groups of order four. Proving that there are at most 2 is not possible for the scope of this course, but proving that there are at least 2 is easy because $x^2 = e$ for all x in the rectangle group, but not all such x are covered by one group based on our work earlier. (Plus, we've already found two groups anyway.)

11.6 Multiplicative Groups on Integers

Consider $\mathbb{Z}_5^*$. This is the official definition of our second group; it's the quotient group without the zero under multiplication. In general, the $*$ means that we take out ev- erything without an inverse to make it an actual group for obvious reasons.

For example, think of $\mathbb{Z}_6^*$. The identity under multiplication modulo 6 is still $\overline{1}$, but the only two numbers modulo 6 that can have an inverse mod 6 are 1 and 5, so our group would just be $\{\overline{1}, \overline{5}\}$. Specifically, **every number relatively prime to n** where we're looking for $\mathbb{Z}_n^*$ is in the group.

The number of numbers less than a number relatively prime to the number can be found with **Euler's totient function** $\phi(n)$. For example, $\phi(p) = p - 1$ for any prime p since every number less than a prime is relatively prime to it.

11.7 Cyclic Groups

A **cyclic group** with generator g is simply $\langle g\rangle = \{g^0, g^1, g^2, ..., g^{n-1}\}$.

Examples of cyclic groups include $(Z_{13}^*, \times_{13})$ and $(\mathbb{Z}_{12}, +_{12})$.

$(\mathbb{Z}_4, +_4)$ is also cyclic with generator $\overline{1}$, giving $\langle\overline{1}\rangle = \overline{0}, \overline{1}, \overline{2}, \overline{3}$. We can also use $\overline{3}$ to get $\overline{3} = \{\overline{0}, \overline{3}, \overline{2}, \overline{1}\}$.

The rectangle group (aka $\mathbb{Z}_2 \times \mathbb{Z}_2$) isn't cyclic since every number is its own inverse. In light of this, we can define the **order** of any element a, or $\mathrm{ord}(a)$, to be the smallest number n such that $a^n = e$. For example, the order of any element of the rectangle group besides the identity is 2 while the order of the identity is 1 (in general).

Similarly, we can develop a cyclic subgroup of a group G based on an element $h \in G$. For example, $\{e, V\}$ is a cyclic subgroup since $V^2 = e$. We also have a corollary of Lagrange's Theorem as a result: $|G| \mid \mathrm{ord}(h)$, aka the order of any element in the group is a factor of the cardinality of the group.

11.8 Theorems About Groups

Let G be a group with identity e. (We use the short hand ab when we really mean $a \cdot b$, where $\cdot$ is the group operation).

Theorem 11.1. *The identity e is unique.*

Proof. Let $x \in G$. Assume that we somehow have e_1, e_2 are identities in G. Notice that $e_1 x = x = e_2 x$, and thus $e_1 x x^{-1} = e_2 x x^{-1}$. Since xx^{-1} is an identity, we must have $e_1 = e_2$.

■

Theorem 11.2. *Each element has a unique inverse.*

Proof. Suppose x has two inverses, a and b. Thus, $xa = xb = e$. If we multiply by a on both sides, we have $axa = axb$, or that $a = b$.

■

Theorem 11.3. $(ab)^{-1} = b^{-1}a^{-1}$

Proof. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly we show that $b^{-1}a^{-1}$ has inverse ab.

■

Corollary 1. $(a_1 a_2 \ldots a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \ldots a_1^{-1}$.

Recall from last lecture that we saw $(\mathbb{Z}_4, +) \cong (\mathbb{Z}_5^*, \times)$, but the symmetry group for the rectangle was different. We also found that $(\mathbb{Z}_{12}, +) \cong (\mathbb{Z}_{13}^*, \times)$. Both groups were cyclic – recall that a cyclic group is any group that can be written in the form $\{g, g^2, g^3, \ldots g^k = e\}$, where g here is the generator of the group. Observe then that $(\mathbb{Z}_n, +)$ is always cyclic, as it is always generated by 1. We write this by saying that $(\mathbb{Z}_n, +) = \langle 1 \rangle$.

Problem 1. Is $\mathbb{Z}_n^*$ always cyclic? Is $\mathbb{Z}_p^*$ always cyclic?

The answer is no to the first question: notice that $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, and each element is its own inverse. This is thus not cyclic and it's actually congruent to the rectangle group.

Theorem 11.4. *$\mathbb{Z}_p^*$ is cyclic.*

Proof omitted for brevity.

11.9 Euler's Totient Function

Define $\phi(n)$ to be the number of integers $1 \leq x \leq n$ such that x is relatively prime to n. Notice that if p is prime, $\phi(p) = p - 1$.
In general, suppose that $n = p_1^{e_1} \ldots p_k^{e_k}$. We will compute this by complementary counting. First, we remove numbers that have a factor of p_i, of which there are $\frac{n}{p_i}$, where we do so for all p_i. This gives us (so far)

$$n - \left(\sum \frac{n}{p_i}\right)$$

However, we have already subtracted off too many - we've subtracted off all numbers that are a product of two primes one too many times, so we have to add them back:

$$n - \left(\sum \frac{n}{p_i}\right) + \left(\sum \frac{n}{p_i p_j}\right)$$

We continue in this fashion, adding and removing numbers from our set until we are left with

$$\phi(n) = n - \left(\sum \frac{n}{p_i}\right) + \left(\sum \frac{n}{p_i p_j}\right) - \left(\sum \frac{n}{p_i p_j p_k}\right) + \ldots + (-1)^k \left(\sum \frac{n}{p_1 p_2 \ldots p_k}\right)$$

If we factor, we actually have

$$\phi(n) = n \prod \left(1 - \frac{1}{p_i}\right) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

This immediately tells us that $\phi(p^k) = p^k - p^{k-1}$ for p prime. We also have that $\phi(n)$ is multiplicative (to some extent): if m, n are relatively prime then

$$\phi(mn) = \phi(m)\phi(n)$$

The proof is done by essentially applying the above formula: let m have prime factors p_i and n have prime factors q_j:

$$\begin{aligned}\phi(mn) &= mn\prod\left(1-\frac{1}{p_i}\right)\prod\left(1-\frac{1}{q_j}\right)\\ &= \left(m\prod\left(1-\frac{1}{p_i}\right)\right)\left(n\prod\left(1-\frac{1}{q_j}\right)\right)\\ &= \phi(m)\phi(n)\end{aligned}$$

11.10 More Proofs with Groups

We now prove Lagrange's Theorem with this newfound knowledge: If H is a finite subgroup of the finite group G, then $\text{ord}(H)|\text{ord}(G)$, or $|H|||G|$.

Proof. Consider all the cosets $\{aH\}$ of H for $a \in G$. We now claim that the distinct cosets partition G and all of them are the same size.

To prove this, we claim that two cosets only intersect if they are actually identical. We prove this by supposing that we have two cosets such that $aH \cap bH \neq \varnothing$. There must be some element c in both cosets such that $c = ah_1 = bh_2$. Let us take some element $z \in aH$ such that $z = ah_3$. Now, notice that $a = ch_1^{-1}$, so $z = ch_1^{-1}h_3 = bh_2h_1^{-1}h_3$. By closure, these h's multiplied together must be some other element in the group H, so $z \in bH$ for all z. Thus, $aH \subseteq bH$ and similarly, $bH \subseteq aH$, so $aH = bH$. Thus, all the distinct cosets will cover G exactly once.

We now prove the second statement. Let $f(h) = aH$ for all $h \in H$. Let $f(h_1) = f(h_2)$. Then, if we multiply by the inverse of a, we must have $h_1 = h_2$, so f is bijective.

With these two claims, each aH is the same size and non-overlapping and corresponds to a subgroup H. Thus, $|aH|||G|$ and thus $|H|||G|$.

■

We use these facts to show Euler's Totient Theorem and Fermat's Little Theorem:

$$a^{\phi(m)} \equiv 1 \mod m \quad a^{p-1} \equiv 1 \mod p$$

Proof. Take the group $\mathbb{Z}_m^*$ which has $\phi(m)$ elements. We pick some $a \in \mathbb{Z}_m^*$. Note that we must have $\gcd(a, m) = 1$. Now consider the group generated by a, $\langle a\rangle = \{a, a^2, a^3, \ldots a^k = e\}$. This is in fact a group (and we can check all of its properties easily). Thus, $\text{ord}(\langle a\rangle)|\text{ord}(\mathbb{Z}_m^*)$. As

$a^k \equiv 1 \mod m$ as a^k must be the identity, and $kt = \phi(m)$, so $a^{kt} \equiv 1^t \equiv 1 \mod m$, so then $a^{\phi(m)} \equiv 1 \mod m$.
Letting m be a prime gives Fermat's Little Theorem immediately.

■

Exercise 1. Find the orbits of each of the elements of $\mathbb{Z}_9^*$.

11.11 Permutation Groups

Let S be a set. Let G be a group of permutations, π, acting on elements of S. Then, G is a **permutation group**.

Example 1.

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

$$\pi_1(1) = 3, \pi_1(4) = 5, \text{etc.}$$

We can write π_1 as a product of cycles, as we have done in the past.

$$\pi_1 = (1\,3)(2)(4\,5)$$

This is the **cycle decomposition** of π_1.

Theorem 11.5. *Every permutation can be written as a product of cycles. This is unique up to rotations or the reordering of cycles.*

Example 1.

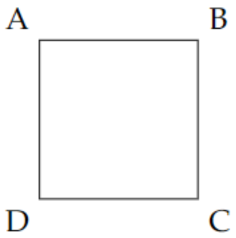
$$\pi_1 = (2)(5\,4)(1\,3)$$

Permutations can also be composed:

$$\pi_1\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e$$

so $\pi_1 = \pi_1^{-1}$.
Thus, $G = \{e, \pi_1\}$ is a permutation group, since it consists of permutations and satisfies the following 4 requirements: closure, identity existence, inverse existence, & associativity.

Example 2. Consider the group of rotations of the square $ABCD$.

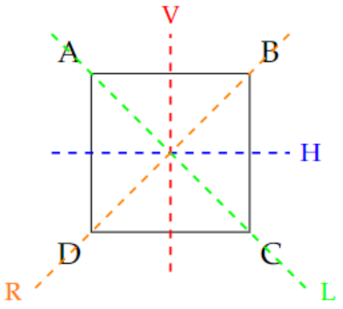


Let S_4 be the **symmetric group**, which is all 24 permutations of $ABCD$. Using only rotations, we can only find 4 of the permutations, as shown here:

r_0	A	B	C	D
r_{90}	D	A	B	C
r_{180}	C	D	A	B
r_{270}	B	C	D	A

This group can be written as $G = \{e = r_0, r_{90}, r_{180}, r_{270}\}$. This group is generated by r_{90} and r_{270}: $\langle r_{90}\rangle = \{r_0, r_{90}, r_{180}, r_{270}\}$.

Example 3. Consider all symmetrices of $ABCD$: $\{e, r_{90}, r_{180}, r_{270}, V, H, L, R\}$, where V is a vertical reflection, H is a horizontal reflection, L is a left diagonal reflection, & R is a right diagonal reflection.



Let's construct a Cayley table!

	e	r_{90}	r_{180}	r_{270}	V	H	L	R
e	e	r_{90}	r_{180}	r_{270}	V	H	L	R
r_{90}	r_{90}	r_{180}	r_{270}	e	R	L	V	H
r_{180}	r_{180}	r_{270}	e	r_{90}	H	V	R	L
r_{270}	r_{270}	e	r_{90}	r_{180}	L	R	H	V
V	V	L	H	R	e	r_{180}	r_{90}	r_{270}
H	H	R	V	L	r_{180}	e	r_{270}	r_{90}
L	L	H	R	V	r_{270}	r_{90}	e	r_{180}
R	R	V	L	H	r_{90}	r_{270}	r_{180}	e

This group is D_4, the dihedral group on 4 elements. We found $|D_4| = 8$ here, which generalizes to $|D_n| = 2n$. It is important to note that the dihedral group is a subgroup of the set of all possible permutations.

Example 4. Below is a table of decomposed operations for square $ABCD$, shown in terms of permutations:

e	e
r_{90}	$(ADCB)$
r_{180}	$(AC)(DB)$
r_{270}	$(ABCD)$
V	$(AB)(CD)$
H	$(AD)(BC)$
L	(BD)
R	(AC)

12 Burnside and Polya

12.1 Burnside's Lemma

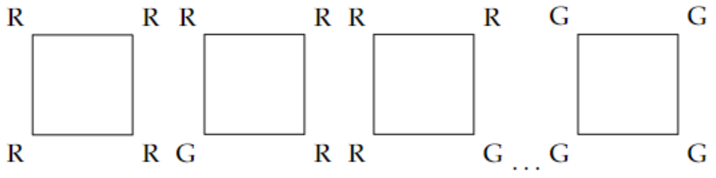
Lemma 1. Given a set S and a permutation group G acting on S, the number of equivalence classes of S is given by $\frac{1}{|G|}\sum_{\pi \in G} |\text{fix}(\pi)|$.

NOTE: in the above, π is an operation on S, and $\text{fix}(\pi)$ is the set of elements in S fixed by π. So, for a given π, count the elements in S that do not change after that operation has been applied.

Example 1. The square, $G = D_4$, S = two-colorings of vertices of a square. Recall that D_4 is the *dihedral group on four elements*. That is,

$$G = e, r_1, r_2, r_3, V, H, L, R$$

where e is the identity, each lowercase r represents a 90°-clockwise rotation applied the number of times indicated by the subscript, V is a vertical reflection, H horizontal, L across the left diagonal, and R across the right. Let us also say that the colors are red (R) and green (G).



We can use Burnside's Lemma to find the number of equivalence groups. First, let's make a table of all $\pi \in G$ and associated values for $|\text{fix}(\pi)|$.

π	$\lvert\text{fix}(\pi)\rvert$
e	$2^4 = 16$
r_1	2 (all red, all green)
r_2	4 (diagonals, all red, all green)
r_3	2 (all red, all green)
V	4
H	4
L	8
R	8

Now, we can use Burnside's:

$$\frac{1}{|G|}\sum_{\pi \in G} |\text{fix}(\pi)| = \frac{1}{8}(16+2+4+2+4+4+8+8) = \boxed{6}$$

So, there are six (6) equivalence groups for D_4.

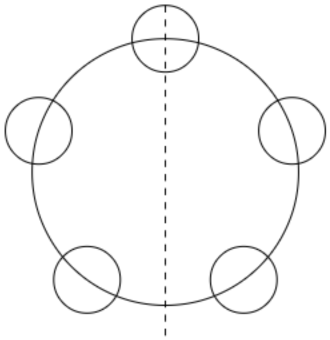
Example 2. Bracelet with 5 beads and colored with red, blue, white, and yellow. You can rotate but not flip the bracelet. How many distinct colorings are there?

Using Burnside's lemma:

π	$\lvert\text{fix}(\pi)\rvert$
e	4^5
r_1	4
r_2	4
r_3	4
r_4	4

$$\frac{1}{|G|}\sum_{\pi \in G} |\text{fix}(\pi)| = \frac{1}{5}(4^5 + 4 \cdot 4) = 4^2 \times 13 = \boxed{208}$$

Example 3. Same as Example 2, but you can reflect.



The above diagram shows an example of such a reflection. In total, there will be five (5) such reflections, bringing the total number of operations on the bracelet to ten (10).

If we were to number the beads 1 through 5 clockwise from the top, the cycle notation for R_1, the illustrated reflection, would be $(1)(2\ 5)(3\ 4)$. So, for all rotations R_i, $1 \leq i \leq 5$, $|\text{fix}(R_i)| = 4^3$.
Apply Burnside's Lemma again, we get

$$\frac{1}{|G|}\sum_{\pi \in G} |\text{fix}(\pi)| = \frac{1}{10}(4^5 + 4 \cdot 4 + 5 \cdot 4^3) = \frac{1}{10}4^2 \times 85 = \boxed{136}$$

Example 4. Let G be the group of rotations of a cube. Write the elements of G in cycle rotations.

A cube has six faces, so there are three pairs of opposite faces. For a spindle going through the centres of two opposite faces there are two possible 90 rotations, one going one way, one the other. This gives six 90 rotations. There is also a 180 rotation when the spindle goes through the centres of two opposite faces. This gives three further rotations.

A cube also has twelve edges, so there are six pairs of opposite edges. For a spindle going through the centres of two opposite edges, the only possibility is a rotation of 180. This gives six rotations, one for each pair of opposite edges.

Finally a cube also has eight corners, so there are four pairs of opposite corners. For a spindle going through two opposite corners, there are two possible rotations, both of 120, one going one way, one the other. This means there are eight 120 rotations, two for each pair of opposite corners.

We have counted 6+3+6+8 different rotations. Add the rotation by 0, which does nothing, and we have a group of $\boxed{24}$ rotations.

12.2 Orbits and Stabilizers

Given $s \in S$ and G a permutation group acting on S.

Definition. $\textit{orbit}(s) = \{\pi s \mid \pi \in G\}$

Definition. $\textit{stabilizer}(s) = \{\pi \in G \mid \pi s = s\}$

Theorem 12.1. *1 Orbit-Stabilizer Theorem: For all $s \in S$ and G acting on S, $|orbit(s)| \cdot |stabilizer(s)| = |G|$*

stabilizer(s) is a subgroup of G, so by Lagrange's theorem, $|\text{stabilizer}(s)| \mid |G|$

Lemma 1. If $\pi \in G$ and $\pi \in$ stabilizer(s), then $\pi^{-1}s = s$.

Proof.

$$\begin{aligned} s &= \pi s \\ \pi^{-1}s &= \pi^{-1}\pi s \\ \pi^{-1}s &= s \end{aligned}$$

■

So now the orbit of S forms cosets of stabilizer(s) (there is a 1-1 corespondence). So $|\text{orbit}(s)|$ = # of cosets of stabilizer(s). Applying Lagrange's theorem gives the orbit-stabilizer theorem.

12.3 Proof of Burnside's Lemma

First, recall Burnside's Lemma:

Lemma 1. The number of equivalence classes in S under the action of permutation group G can be calculated to be

$$\frac{1}{|G|}\sum_{\pi \in G} |\text{fix}(\pi)|$$

Recall also the Orbit-Stabilizer Theorem:

Theorem 12.2. *2 For any $s \in S$ with associated permutation group G,*

$$|Orb(S)| \cdot |stab(s)| = |G|$$

Now, let us count the orbits/equivalence classes of 2-colored vertices of the square under the dihedral group D_4. Suppose we have red and green as our colors. Then the orbits are:

- the all-red coloring
- 3 red, 1 green (in each of the four corners)
- 2 red, 2 green, with reds/greens adjacent (4 such colorings)

- 2 red, 2 green, with reds/greens at opposite corners (2 such colorings)
- 3 green, 1 red (in each of the four corners)
- the all-green coloring

There are 6 equivalence classes. This example is helpful for the proof:

Proof. Count the fixed points in the table $S \times G \to S$. Note that the fixed points with $\pi(s) = s$ can be counted in two ways – counting by group elements or by elements of S, we see that this is

$$\sum_{\pi \in G} |\text{fix}(\pi)| = \sum_{s \in S} |\text{stab}(s)|,$$

which, via the Orbit-Stabilizer Theorem we see to be equal to

$$\sum_{s \in S} \frac{|G|}{|\text{orb}(s)|}.$$

Partitioning the elements of S into their respective orbits, we can rewrite this as

$$\sum_{O_i \in \text{Orbits}} \sum_{s \in O_i} \frac{|G|}{|\text{orb}(s)|} = |G| \sum_{O_i \in \text{Orbits}} \sum_{s \in O_i} \frac{1}{|O_i|} = |G| \sum_{O_i \in \text{Orbits}} |O_i| \cdot \frac{1}{|O_i|}$$

$$= |G| \sum_{O_i \in \text{Orbits}} 1 = |G| \cdot \#\text{orbits}.$$

Dividing both sides by $|G|$, we see

$$\#\text{orbits} = \frac{1}{|G|} \sum_{\pi \in G} |\text{fix}(\pi)|.$$

■

12.4 Polya's Enumeration Theorem

Definition. *Let X be a set ("vertices") and S be a set of functions $X \to C$ (C is a set of "colors"). Let G be a group operating on X. We will say two elements f_i, f_j of S are* equivalent *iff there is some $\pi \in G$ such that $f_i(x) = f_j(\pi(x))$ for all $x \in X$.*

Example 1.

$$\begin{matrix} G & R \\ R & R \end{matrix} \cong \begin{matrix} R & R \\ G & R \end{matrix}$$

because H acting on the first coloring (viewed as a function) turns it into the second.

Explicitly, if we number the vertices as $\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}$, the first coloring is the function f_1 with $1 \mapsto G$, $2, 3, 4 \mapsto R$, and the second coloring is the function f_2 with $3 \mapsto G$, $1, 2, 4 \mapsto R$. H in cycle notation is the permutation $\pi_H = (13)(24)$. We can check:

$$f_1(\pi_H(1)) = f_1(3) = R = f_2(1) \quad f_1(\pi_H(2)) = f_1(4) = R = f_2(2)$$

$$f_1(\pi_H(3)) = f_1(1) = G = f_2(3) \quad f_1(\pi_H(4)) = f_1(2) = R = f_2(4)$$

Definition. *The* weight *of the colors is some function $w : C \to \mathcal{F}$ for some field $\mathcal{F}$.*

Definition. *The* weight *$W(f)$ of a function $f : X \to C$ is defined to be $\prod_{x \in X} w(f(x))$.*

Definition. *The* inventory *of a set S of functions is $\sum_{f \in S} W(f)$.*

Example 2. For the 2-colorings of the square, if we take $w(R) = r$ and $w(G) = g$ (where r, g are some variables that can be added and multiplied), then for the two 2-colorings above, we have that $W(f_1) = r^3 g = W(f_2)$.

The inventory of all 2-colorings of a square is

$$r^4 + 4r^3 g + 6r^2 g^2 + 4rg^3 + g^4 = (r + g)^4.$$

Definition. *The* cycle index polynomial *of a permutation group is*

$$P_G(x_1, x_2, \dots, x_k, \dots) = \frac{1}{|G|} \sum_{\pi \in G} x_1^{b_1} x_2^{b_2} \dots x_k^{b_k} \dots$$

where b_k is the number of cycles of length k in π.

Example 3. For the dihedral group D_4, where the vertices are labeled $\begin{smallmatrix} 1 & 2 \\ 4 & 3 \end{smallmatrix}$:

$$e : (1)(2)(3)(4) \to x_1^4$$

$$r_{90} : (2143) \to x_4^1$$

$$r_{180} : (13)(24) \to x_2^2$$

$$r_{270} : (1234) \to x_4^1$$

$$H : (14)(23) \to x_2^2$$

$$V : (12)(34) \to x_2^2$$

$$L : (24)(1)(3) \to x_1^2 x_2$$
$$R : (13)(2)(4) \to x_1^2 x_2$$

So, the cycle index polynomial for D_4 is

$$\frac{1}{8}(x_1^4 + 3x_2^2 + 2x_1^2 x_2 + 2x_4).$$

Now, to state Polya's theorem:

Theorem 12.3. *The inventory of the equivalence classes of functions $f : X \to C$ under the action of permutation group G is given by*

$$P_G(\sum w(x), \sum w^2(x), \sum w^3(c), \dots)$$

Example 4. For the square under D_4, the inventory is given to be

$$P_G(r+g, r^2+g^2, r^3+g^3, r^4+g^4)$$
$$= \frac{1}{8}((r+g)^4 + 3(r^2+g^2)^2 + 2(r+g)^2(r^2+g^2) + 2(r^4+g^4))$$
$$= g^4 + g^3 r + 2g^2 r^2 + g r^3 + r^4$$

Corollary 1. The number of equivalence classes of functions $f : X \to C$ under the action of permutation group G is $P_G(|C|, |C|, |C|, \dots)$

Proof. Plug in 1 for $w(c)$. So, $w(c) = 1$ for each color. For example, in the examples for the square above, take $w(R) = w(G) = 1$. ■

Example 5. The cycle index polynomial of the symmetries of the cube is:

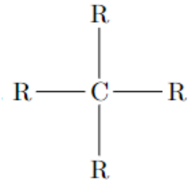
$$P_G(x_1, x_2, x_3, x_4) = \frac{1}{24}(x_1^6 + 3x_1^2 x_2^2 + 6x_2^3 + 6x_1^2 x_4 + 8x_3^2).$$

Plugging $|C| = n$ into the polynomial, we get the number of equivalence classes of colorings of the cube to be equal to

$$C(n) = \frac{1}{24}(n^6 + 3n^4 + 6n^3 + 6n^3 + n^2) = \frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2).$$

Take this example from chemistry:

Example 6. Consider the following tetrahedral structure:



$$R = \begin{cases} CH_3 & \text{methyl} \\ C_2H_5 & \text{ethyl} \\ H & \text{hydrogen} \\ Cl & \text{chlorine} \end{cases}$$

Find (a) the number of molecules, and (b) the ones containing ≥ 1 solitary H atom. It is a chemical fact that these molecules are in fact not planar, but actually tetrahedral.
The symmetry group of the tetrahedron has these categories of elements, written in cycle notation:

$$e : (1)(2)(3)(4) : 1$$

$$r_v : (1)(234) : 4$$

$$r_v^2 : (1)(243) : 4$$

$$r_3 : (12)(34) : 3$$

We can use these to find the cycle index polynomial to be

$$\frac{x_1^4 + 8x_1x_3 + 3x_2^2}{12}.$$

So $C(n) = \frac{n^4+11n^2}{12}$. We then see that $C(4) = 36$ and $C(3) = 15$. Using complementary counting we can find the answer to (b) to be $C(4) - C(3) = 21$.

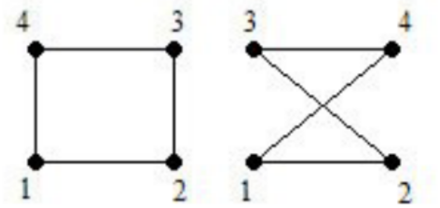
12.5 Applying Polya's Theorem

We can use Polya's Theorem to count unlabeled graphs.

Definition. *A* graph *is a pair of sets (V, E) where V is the set of vertices and $E \subseteq V \times V$.*

Definition. *Two graphs are isomorphic if there is a map $\pi : (V, E) \to (V_2, E_2)$ such that $\pi(E) = \{(\pi(v_1), \pi(v_2)) \, \forall (v_1, v_2) \in E\} = E_2$ and $\pi(V) = V_2$.*

Example 1. These two graphs are isomorphic under the transformation $\pi = (1)(2)(34)$.



Problem 1. Apply Polya's Theorem to count all graphs with $n = 3, 4$ vertices.

For a graph with 3 vertices, we want to consider the cycle index polynomial for S_3:

π	monomial	Action on edges
(1)(2)(3)	x_1^3	$(\overline{12})(\overline{13})(\overline{23})$
(1)(23)	x_1x_2	$(\overline{12}\,\overline{13})(\overline{23})$
(2)(13)	x_1x_2	$(\overline{21}\,\overline{23})(\overline{13})$
(3)(12)	x_1x_2	$(\overline{31}\,\overline{32})(\overline{12})$
(123)	x_3	$(\overline{12}\,\overline{23}\,\overline{31})$
(132)	x_3	$(\overline{13}\,\overline{32}\,\overline{21})$

$$P_{S_3^{(2)}} = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3)$$

To enumerate, let the weight of an edge be r, and the weight of a lack of edge be b, Thus, plugging in in accordance with the enumeration theorem,

$$P_{S_3} = \frac{1}{6}((r+b)^3 + 3(r+b)(r^2+b^2) + 2(r^3+b^3)).$$

Because we don't care about lack of edges, let $b = 1$. Then this simplifies to

$$r^3 + r^2 + r + 1.$$

Next, let $r = 1$ so $x_i = 2$.

$$P_3 = \frac{1}{6}(2^3 + 3 \cdot 4 + 2 \cdot 2) = 4.$$

Now, let's do this for S_4:

Number	form of π	$S_4^{(2)}$ monomial	Action on edges
$\binom{4}{0}(1-1)!$	(1)(2)(3)(4)	x_1^6	$(\overline{12})(\overline{13})(\overline{14})(\overline{23})(\overline{24})(\overline{34})$
$\binom{4}{2}(2-1)!$	(1)(2)(34)	$x_1^2x_2^2$	$(\overline{12})(\overline{13}\,\overline{14})(\overline{23}\,\overline{24})(\overline{34})$
$\binom{4}{3}(3-1)!$	(1)(234)	x_3^2	$(\overline{12}\,\overline{13}\,\overline{14})(\overline{23}\,\overline{34}\,\overline{42})$
$\binom{4}{2} \cdot \frac{1}{2}$	(12)(34)	$x_1^2x_2^2$	$(\overline{12})(\overline{23}\,\overline{14})(\overline{24}\,\overline{13})(\overline{34})$
$(4-1)!$	(1234)	x_2x_4	$(\overline{12}\,\overline{23}\,\overline{34}\,\overline{41})(\overline{13}\,\overline{24})$

Thus,

$$P_{S_4^{(2)}} = \frac{1}{24}(x_1^6 + 9x_1^2 + 8x_3^2 + 6x_2x_4).$$

Then, to enumerate, we let the weight of no edge be 1, and the weight of an edge be x, and get

$$x^6 + x^5 + 2x^4 + 3x^3 + 2x^2 + x + 1.$$

When we let $x = 1$, this simplifies to 11.
We can also do this for $n = 5$ and higher n as well, and the computations are similar.

12.6 Permutations and Transpositions

Any permutation can be written as the product of transpositions, or the permutation of two elements (ie. (1 2), which can become (2 1) by swapping the values). The order of the numbers transpositions does not matter. If your cyclic permutation is made of more than 2 numbers, then permute the first number with every other number in the permutation.

For example, given (1 2 3 4), the product of transpositions will be (12)(13)(14). Given, (425), the transpositions will be (42)(45).

Any permutation can be considered odd or even based on the number of transpositions involved in the permutation. If there are an odd number of transpositions, then the permutation is odd. If there is an even number, then the permutation is even.
Below is a table filled in with examples using the information from above:

π	Product of Transpositions	Type/Sign/Parity
(123)(45)	(12) (13) (45)	odd
(1234)	(12) (13) (14)	odd
(13) (425) (67)	(13) (67) (42) (45)	even
(12345)	(12) (13) (14) (15)	even

Part IV
Coda: Computational Complexity

13 Turing Machines

Turing Machines are a fundamental model of computation postulated to be able to compute all computable problems.

13.1 Basics

Definition. *An* alphabet *is just a set of "characters," or "symbols."*

Definition. *A* word *is just a string of characters from the alphabet.*

Definition. *A* language $\mathcal{L}$ *is a subset of the set of all words*

Example 1. All $\{0,1\}^*$ strings with an even number of 0s form a language.

Example 2. All sentences in $[a-z]^*$ including "the" form a language.

Example 3. All a, b, c, n such that $a^n + b^n = c^n, n > 2$ form a language.

13.2 Push Down Automata

Push Down Automata are a type of automata that also contain something called the "stack," which behaves like the stack we know from programming.
Consider the language $\mathcal{L} = ww^R$, or the palindromes in $\{0,1\}^*$.

- Read a character from input
- Push that character onto the "stack"
- Repeat OR go to the next step
- Read a character and pop off the stack
- Compare the next character to the one popped off the stack
- Repeat previous two steps

- If the stack is empty when we run out of input, we end in ACCEPT state

This specific instance of a Push-Down Automata model is **Nondeterministic**, which means that it somehow always takes the path to an "ACCEPT" state if there is one.

13.3 Turing Machines

Turing Machines are even more robust.

Definition. *A Turing Machine has access to:*

- *Input,*
- *state,*
- *an infinite "tape," which can be read or written to.*

And thus has the ability to perform these operations:

- *Read input OR tape*
- *Write to tape*
- *Move left OR right*

Example 1. Add $x + y$ in unary, i.e. $7 + 3 = 10$ in unary is

$$1111111 + 111 = 1111111111.$$

We model the input as

$$1111111\#111$$

and the code(notated with the state on the left before the colon and the state moved to as after the semicolon,)

$$0 : 1 \rightarrow write(1), right; 0$$

$$0 : \# \rightarrow nothing; 0$$

Example 2. Multiplication in Unary We can take the input for multiplying 1111 and 111 to be 1111#111 Using this, we can get our process to be this:

- Copy input to tape
- Read the first 1 in the tape, and move right until the next blank

- Copy the 1, and then change the first 1 to a 0
- Back up to the 0
- Repeat copying the 1 and pasting and then converting to a 0 until we hit the next string of digits.
- Change that 1 to a 0
- Change all 0s before back to a 1
- Goto step 3
- End at the string "0#1"

Example 3. Convert binary to unary

$$001101 \to ?$$

Code:
s_0 : 0 → nothing; s_0,
s_0 : 1 → write 1; s_1,
s_1 : 0 → double output string; s_1,
s_1 : 1 → double output string, write 1; s_1
double x:
    write $x\#x$
    add, as we previously reviewed

Example 4. Dividing binary strings (integer division, not floating.)

$$1001101//110011$$

Procedure

- Convert to unary
- Subtract the $a - b$ (overwrite ones with zeros)
- $Stop when b < a$

Q: Does a multitape Turing Machine have more power than a single tape Turing Machine?
A: We can interweave the contents of both tapes onto one tape, and then Record the position of each multitape's position on the tape, like so:

$$A_{-1}B_{-1}A_0B_0A_1B_1A_2B_2\ldots\#P_A\#P_B.$$

Because a multitape is simulatable in a single tape Turing Machine, it is not more powerful.

13.4 Non-determinism

$\mathcal{L} = \underline{\text{composite numbers}}$ in binary
We can determine membership either deterministically or non-deterministically:

Deterministic Implementation

Simulate 4 Tapes: x, D, $S_1 = x\#D$, and $S_2 : x \mod D$ And we can use the code:

```
Increment $D$
if $x \mod D \equiv 0$, ACCEPT
Else $D$++
If $D = x$, REJECT
```

This is $pO(divide)$, where p is the smallest prime factor of x. This is an exponential time algorithm in binary length of input.

Non-deterministic Implementation

```
Write $D$ OR $x$,
Accept if $D \mid x$ and $D < x$.
```

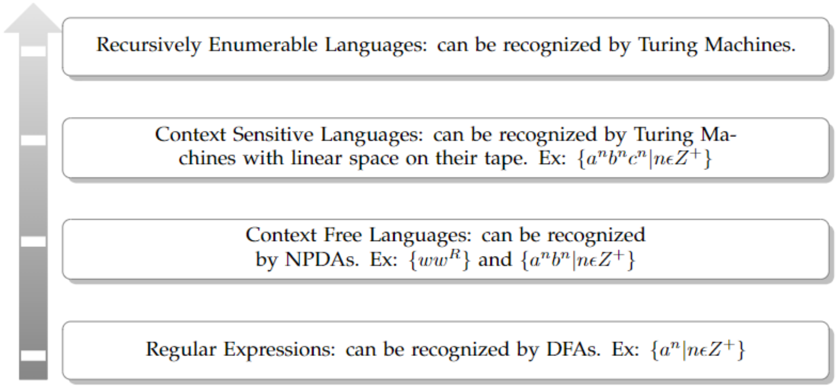
This is $O(divide) = O(n)$

13.4.1 The P-NP problem

The question is, then: Are non-deterministic Turing Machines necessarily faster than their deterministic counterparts? In particular, is the set of languages computable by a non-deterministic Turing machine larger than the set computable by a deterministic Turing machine? If we restrict each of these Turing machines to polynomial time, this is the famous open problem $P = NP$.

14 Computational Complexity

14.1 Chomsky Hierarchy



Recursively Enumerable Languages: can be recognized by Turing Machines.

Context Sensitive Languages: can be recognized by Turing Machines with linear space on their tape. Ex: $\{a^nb^nc^n|n\epsilon Z^+\}$

Context Free Languages: can be recognized by NPDAs. Ex: $\{ww^R\}$ and $\{a^nb^n|n\epsilon Z^+\}$

Regular Expressions: can be recognized by DFAs. Ex: $\{a^n|n\epsilon Z^+\}$

Note: a Turing Machine can "recognize a language" if and only if:
TM(x) answers "Yes", if x is in the language, and
TM(x) either answers "No" or runs forever, for all x not in the language.

14.2 The Halting Problem

Given a Turing Machine M and input x, we are presented with the question: "Does M(x) halt?", or, *does the Turing Machine give an answer instead of running indefinitely?* The following things are true:

1. Turing Machines are enumerable. Any and all Turing Machines can be uniquely represented by a integer. This makes sense when we consider that a binary string is a series of operations.
2. All x's are enumerable. Turing Machines only run on integers.
3. Universal Turing Machines exist.

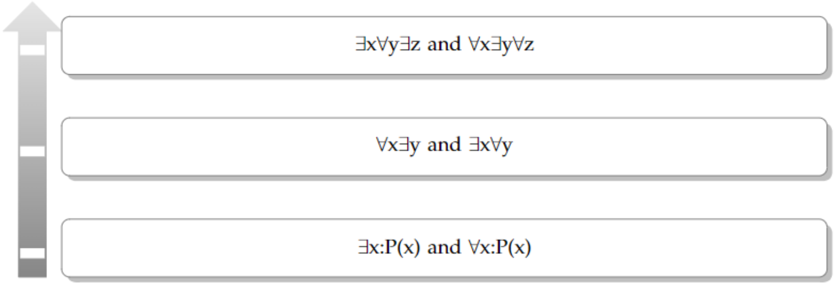
Definition. *A* recursive *language is any language such that a Turing Machine acting on a x within the language will halt if it results in an "Yes" or a "No".*

Definition. *An* alternating *Turing Machine is visualized as a tree that alternates between levels of* $\exists$ *and* $\forall$ *with leaves that are conditional statements.*

14.3 The Arithmetic Hierarchy

$\exists$ = Existential Quantifier, or "there exists".
$\exists x : x > 5$

$\forall =$ Universal Quantifier, or "for all".
$\forall x : x > 5x$
$\forall x \exists y : y < x - d$



In the lowest level of the arithmetic hierarchy → $\exists x : P(x)$, NP and $\forall x : P(x)$, co-NP. It is known that $PRIME \in$ co-NP since it is defined as: for all x, x is not an integer between 1-n, nor does it divide n. However, Pratt's Theorem shows that $PRIME \in NP$.

Theorem 14.1. *Pratt's Theorem: $PRIME \in NP$*

Proof. If p is prime, then $\mathbb{Z}_p^*$ is cyclic. This means that an element g generates the entire group. Then, we use a non-deterministic Turing Machine to guess g. To prove g is a generator, for all primes that divide $p - 1 = q_1^{e_1} \cdot q_2^{e_2} \cdot \ldots, g^{(p-1)/q_i} \not\equiv 1(\mod p)$, we need only perform $\log_2 p$ tests on primes of size and order $\log p$. We need to prove this recursively to show that prime factors are truly prime. Thus, Pratt's Certificate of Primality requires the factorization of $n - 1$ and the method is best applied to small numbers (numbers n known to have easily factorable $n - 1$)

■