Winter 2021 Math 61 Notes

Kyle Chui

2021-2-8

Contents

1 Sets and Functions

1.1 Power Sets

Definition. *Power Set*
If X is a set, the *power set* of X, denoted $\mathscr{P}(X)$, is the set of subsets of X.

Example. *Power Sets*

- $\mathscr{P}(\varnothing) = \{\varnothing\}$
- $\mathscr{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
- $\mathscr{P}(\{a, b, c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

Definition. *Cardinality of Finite Sets*
If X has finitely many elements, then $|X|$ denotes the number of elements of X.

Theorem — *Cardinality of Power Sets*
If X is finite, then $|\mathscr{P}(X)| = 2^{|X|}$.

Proof. Let us induct on the cardinality of the set X. Suppose $|X| = 0$, so that $X = \varnothing$. Then $\mathscr{P}(X) = \{\varnothing\}$, so $|\mathscr{P}(X)| = 1 = 2^0$. Thus the statement is true when $|X| = 0$.

Suppose that the statement holds for some non-negative integer k. Let Y be a set such that $|Y| = k + 1$, and $y \in Y$. Observe that we may split $\mathscr{P}(Y)$ into two groups: the subsets containing y, and the subsets that do not contain y. A subset of Y that does not contain y is exactly $Y \setminus \{y\}$, which has k elements. By the inductive hypothesis, there exist 2^k such subsets. A subset of Y that does contain y is obtained by adding y to a subset of Y which does not contain y. Again, there are 2^k such subsets. Any subset of Y either does or does not contain y (but not both), so there are $2^k + 2^k = 2^{k+1}$ subsets of Y. Therefore $\mathscr{P}(X) = 2^{|X|}$ for all finite sets $|X|$. $\square$

1.2 Functions

Definition. *Function*
If X, Y are sets, a function f from X to Y, written $f \colon X \to Y$ is a subset of $X \times Y$ satisfying two properties:

- For all $a \in X$, there exists $b \in Y$ such that $(a, b) \in f$
  - Everything in the domain must get mapped to something in the codomain
- For all $a \in X$ and $b, b' \in Y$, if $(a, b), (a, b') \in f$, then $b = b'$
  - Every element in the domain can map to at most one element in the codomain

Note (Function Notation). If $(a, b) \in f$, we write $f(a) = b$.

Example. *Functions*

- $f\colon \mathbb{Z} \to \mathbb{N}$ such that $f(x) = x^2$
- $g\colon \mathbb{N} \to \mathbb{N}$ such that $g(x) = x^2$

Note that f and g are different functions.

Definition. *Domain and Codomain of a Function*
If $f\colon X \to Y$, X is the domain of f and Y is the codomain of f.

Definition. *Range of a Function*
For $f\colon X \to Y$, the range of f is:

$$\operatorname{range} f = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}$$

Definition. *Surjectivity*
A function $f\colon X \to Y$ is *onto* or *surjective* if $\operatorname{range} f = Y$. In other words, a function is surjective if its range is equal to its codomain.

Example. *Surjective Functions*

- $f\colon \{a, b, c\} \to \{d, e, f\}$ defined by $f = \{(a, d), (b, e), (c, f)\}$
- $f\colon \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = |x|$

Definition. *Injectivity*
A function $f\colon X \to Y$ is *one-to-one* or *injective* if, for all $x, y \in X$, $f(x) = f(y)$ implies that $x = y$. In other words, different elements in the domain map to different elements in the codomain.

Example. *Injective Functions*

- $g\colon \mathbb{N} \to \mathbb{N}$ defined by $g(x) = x^2$

Note (Properties of Functions). Observe that the both the domain and codomain of a function matter when it comes to determining whether the function satisfies certain properties. For instance, $f\colon \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = x^2$ is not injective, but restricting the domain to $\mathbb{N}$ would make it injective. Similarly, a function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective, but restricting the codomain to $\mathbb{N}$ would make it surjective.

Definition. *Composition of Functions*
If $f\colon X \to Y, g\colon Y \to Z$ are functions, then $g \circ f\colon X \to Z$ is a function defined by $(g \circ f)(x) = g(f(x))$.

Theorem — *Composition of Injective/Surjective Functions is Injective/Surjective*
Let $f\colon X \to Y$, $g\colon Y \to Z$.

- If f, g are injective, so is $g \circ f$
- If f, g are surjective, so is $g \circ f$

Proof. Suppose f, g are injective functions. Let $x, x' \in X$ such that $(g \circ f)(x) = (g \circ f)(x')$. Then

$$\begin{aligned} g(f(x)) &= g(f(x')) \\ f(x) &= f(x') && \text{(Because } g \text{ is injective)} \\ x &= x' && \text{(Because } f \text{ is injective)} \end{aligned}$$

Therefore $g \circ f$ is injective. □

Proof. Suppose f, g are surjective functions. Let $z \in Z$. Because g is surjective, there exists some $y \in Y$ such that $g(y) = z$. Furthermore, because f is surjective, there exists some $x \in X$ such that $f(x) = y$. Thus, for every $z \in Z$, there exists some $x \in X$ such that $(g \circ f)(x) = g(f(x)) = g(y) = z$, so $g \circ f$ is surjective. □

Definition. *Bijectivity*
If a function is both injective and surjective, then we say that it is *bijective*.

Note (Cardinality and Bijections). If there is a bijection between two sets, they have the same number of elements.

1.3 Inverses of Functions

Definition. *Inverse of a function*
Suppose $f\colon X \to Y$, $g\colon Y \to X$ is an inverse to f (soon we'll prove that inverses are unique if they exist) if $f \circ g$ and $g \circ f$ are the identity. In other words, $(g \circ f)(x) = x$, $(f \circ g)(y) = y$ for all $x \in X$, $y \in Y$.

Theorem — *Bijective $\iff$ Inverse*
For $f\colon X \to Y$, f is a bijection if and only if f has an inverse.

Proof. Suppose f has an inverse function g. Then $f \circ g$ and $g \circ f$ are the identity. Suppose $f(a) = f(b)$. Then

$$\begin{aligned} f(a) &= f(b) \\ g(f(a)) &= g(f(b)) \\ (g \circ f)(a) &= (g \circ f)(b) \\ a &= b. \end{aligned}$$

Thus f is injective.

Suppose $b \in Y$. Since $f \circ g$ is the identity, we have that $(f \circ g)(b) = b$, so $f(g(b)) = b$. Thus f is surjective. Therefore f is a bijection.

Now suppose that f is a bijection. We define $f^{-1}(a)$ by $f^{-1}(a) = b$, where $a = f(b)$.

- Because f is surjective, we have that for all $a \in Y$, there exists some $b \in X$ such that $a = f(b)$.

- Because f is injective, any $a \in Y$ is *uniquely* mapped by some $b \in X$.

Thus f^{-1} is a function. We will now show that f^{-1} is the inverse of f. For all $x \in X$, $(f^{-1} \circ f)(x) = x$ by definition. For all $y \in Y$,

$$\begin{aligned}(f \circ f^{-1})(y) &= f(f^{-1}(y)) \\ &= f(f^{-1}(f(x))) && \text{(Because } f \text{ is surjective)} \\ &= f(x) && ((f^{-1} \circ f)(x) = x) \\ &= y.\end{aligned}$$

Therefore f^{-1} is the inverse of f. □

Theorem — *Uniqueness of Inverses*
Inverses of functions are unique, provided they exist.
Suppose $f\colon X \to Y$. If f has inverses $g, h\colon Y \to X$ such that $g \circ f = h \circ f = \mathrm{id}_X$, $f \circ g = f \circ h = \mathrm{id}_Y$, then $g = h$.

Proof. Let $y \in Y$. By the previous theorem we know that f is surjective, so $y = f(x)$, for some $x \in X$. Thus

$$\begin{aligned}g(y) &= g(f(x)) \\ &= x \\ &= h(f(x)) \\ &= h(y).\end{aligned}$$

Thus $g = h$ and the inverse is unique. □

1.4 Special Functions

Definition. *Sequence of elements*
A sequence in X is a function $s\colon D \to X$ where $D \subseteq \mathbb{Z}$.

Example. *Sequence*

(a) $X = \{a, b, c\}$, $D = \{1, 2, 3, 4, 5\}$. We may define $s\colon D \to X$ by:

$$\begin{aligned}1 &\mapsto a \\ 2 &\mapsto b \\ 3 &\mapsto c \\ 4 &\mapsto b \\ 5 &\mapsto a\end{aligned}$$

(b) The Fibonacci numbers are a sequence of natural numbers. They are defined by: $F_0 = 0, F_1 = 1$, and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$.

(c) Sequence of even natural numbers: $0, 2, 4, 6, 8, \ldots$. The function $e\colon \mathbb{N} \to \mathbb{N}$ is defined by $e(n) = 2n$. Observe that the sequence of the powers of 2 is a subsequence of the even natural numbers.

Definition. *Subsequences*
A *subsequence* of $s\colon D \to X$ is a sequence obtained by restricting the domain of s. In other words, a *subsequence* is a sequence of the form $t\colon D' \to X$ where $D' \subseteq D$.

Definition. *Strings*
If X is a finite set, a *string* over X is a finite sequence of elements of X.

Example. *Strings*

(a) Let X be the English alphabet. Then c, a, t and d, o, g and m, a, t, h are all strings over X. We write strings without parentheses and commas, so c, a, t becomes cat.

Definition. *Special strings*
We will let X^* denote the set of strings over X. Additionally, let λ be the null string.

If α, β are strings over X, we can concatenate them to get a new string $\alpha\beta$.

Example. *Concatenation*
The string c, a, t concatenated with d, o, g becomes c, a, t, d, o, g or $catdog$.

Definition. *Substrings*
A *substring* is a string obtained by selecting some or all consecutive terms of another string. Observe that the terms must be consecutive, unlike subsequences.

2 Relations

Definition. *Relations*
A *relation* R from a set X to a set Y is a subset of $X \times Y$. We write $R(x, y)$ or xRy to denote $(x, y) \in R$. If R is a relation from X to X, we say that R is a relation on X.

Note (Relations and functions). Functions are a special type of relation.

Example. *Relations*

(a) Let X = students at UCLA, Y = Classes at UCLA in Winter '21 Quarter. Define R to be a relation between X and Y such that

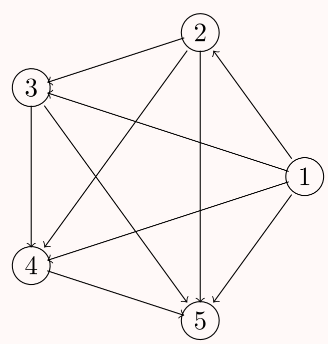
$$R = \{(x, y) \in X \times Y \mid x \text{ is a student in } y\}.$$

Is R a function? No, because a student can be taking more than one class during the Winter '21 Quarter.

(b) Let $X = \{2, 3, 4, 5\}$ and $Y = \{4, 5, 6, 7, 8\}$. Define the relation R to be: xRy if x divides y. Then

$$R = \{(2, 4), (2, 6), (2, 8), (3, 6), (4, 4), (4, 8), (5, 5)\}.$$

(c) Let $X = \{1, 2, 3, 4, 5\}$ and define a relation R on X so that xLy if $x < y$. We can visualise this by drawing an arrow $x \to y$ if $x < y$.



(d) Let $X = \{1, 2, 3, 4, 5\}$, and define a relation LE on X such that $xLEy$ if $x \leq y$. The diagram is the exact same as above, but every element is also related to itself (because $x \leq x$ for all x).

2.1 Types of Relations

(a) Reflexive: R is reflexive if for all $x \in X$, xRx (x relates to itself).

(b) Symmetric: R is symmetric if for all $x, y \in X$, $xRy \implies yRx$.

(c) Antisymmetric: R is antisymmetric if for all $x, y \in X$, xRy and yRx implies $x = y$.

(d) Transitive: R is transitive if for all $x, y, z \in X$, xRy and yRz implies xRz.

Example. *Types of relations*

(a) The relation $<$ over the reals is transitive, (vacuously) antisymmetric, not symmetric, and not reflexive.

(b) The relation $\leq$ over the reals is transitive, antisymmetric, not symmetric, and not reflexive.

(c) Let $X =$ people, and xNy if x and y have the same name. Then N is reflexive, symmetric, and transitive.

(d) Let $X =$ people, and xTy if x is taller than y. Then T is transitive, because if x is taller than y, and y is taller than z, then x is taller than z.

Definition. *Inverse of a relation*
If R is a relation from X to Y, then R^{-1} is the relation from Y to X defined by:

$$R^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in R\}.$$

Definition. *Composition of relations*
If $R \subseteq X \times Y$, and $S \subseteq Y \times Z$, then $S \circ R \subseteq X \times Z$ such that

$$S \circ R = \{(x, z) \in X \times Z \mid \text{there exists } y \in Y \text{ such that } (x, y) \in R \text{ and } (y, z) \in S\}.$$

2.2 Equivalence Relations

Definition. *Equivalence relation*
A relation R on aset X is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Note. An equivalence relation gives us a notion of two different elements in a set being "the same".

- Reflexive: Everything is "the same" as itself
- Symmetric: If x is "the same" as y, then y is "the same" as x
- Transitive: If x is "the same" as y, and y is "the same" as z, then x is "the same" as z

Example. *Equivalence Relations*

(a) The relation E on the integers where xEy if $x - y$ is even.

- Reflexive: For all $x \in \mathbb{Z}$, $x - x = 0$, which is even, so xEx
- Symmetric: For all $x, y \in \mathbb{Z}$, if $x - y$ is even, so is $-(x - y) = y - x$. Thus if xEy, then yEx
- Transitive: For all $x, y, z \in \mathbb{Z}$, if $x - y$ is even and $y - z$ is even, then their sum, $x - z$, is also even. Thus if xEy and yEz, then xEz.

Observe that this relation relates two integers if they have the same parity.

(b) Let Y be any finite set, and $a, b \in Y^*$ (the set of all strings constructed using Y). Consider the relation L over Y^* such that aLb if a and b have the same length.

(c) Let X be the set of all animals, with animals $x, y \in X$. Consider the relation S over X such that xSy if x and y are of the same species.

(d) Let $x, y \in \mathbb{R}$. Consider the relation C over $\mathbb{R}$ such that xCy if $x - y$ is an integer.

Definition. *Equivalence Classes*
If R is an equivalence relation on a set X, then for $x \in X$, the *equivalence class* of X is the set (with respect to R), denoted by $[x] = [x]_R = \{y \in X \mid xRy\}$.

Example. *Equivalence Classes*

(a) Let E be a relation on $\mathbb{Z}$, where xEy if $x - y$ is even. The equivalence classes for E are $[0]$ (the evens) and $[1]$ (the odds). So, the set of equivalence classes $= \{[0], [1]\}$.

(b) Let $x, y \in \mathbb{R}$, with the relation C over $\mathbb{R}$ defined by xCy if $x - y$ is an integer. The set of equivalence classes $= \{[x] \mid x \in [0, 1)\}$.

If R is an equivalence relation on a set X, then:

- For all $x \in X$, if $x \in [y]$ and $x \in [z]$, then $[y] = [z]$.

  Proof. Suppose $x \in [y]$ and $x \in [z]$. Let $w \in [y]$. Because $w \in [y]$, we know that yRw. We also know that yRx because $x \in [y]$. By symmetry of R, we have wRy, and by transitivity, we have wRx. But $x \in [z]$, so zRx, and by symmetry we have xRw. By transitivity, zRw so $w \in [z]$. Thus $[y] \subseteq [z]$.

  By a similar argument, we have that $[z] \subseteq [y]$, so $[y] = [z]$. □

- For any $x \in X$, x is in some equivalence class, $x \in [x]$ by reflexivity.
  So, for every $x \in X$, x is in exactly one equivalence class. If x is in another equivalence class $[y]$, then by the above $[x] = [y]$.

Definition. *Partition*
For X a set, a *partition* $\mathcal{S}$ of X is a set of nonempty subsets of X such that every element of X is an element of exactly one of the subsets. In other words, for all $A, B \in \mathcal{S}$

- $A, B \subseteq X$
- $A, B \neq \varnothing$
- If $A \cap B \neq \varnothing$ then $A = B$
- For all $x \in X$, there exists exactly one $A \in \mathcal{S}$ such that $x \in A$

Note. We showed that if R is an equivalence relation on X then $\{[x]_R \mid x \in X\}$ is a partition of X.

Theorem — *Equivalence Relations and Partitions*
For X a set, there is a bijection $F\colon$ Set of equivalence relations on $X \to$ Set of partitions of X, defined by

$$F(E) = \{[x]_E \mid x \in X\},$$

the inverse function F^{-1} sends a partition $\mathcal{S}$ to the equivalence relation $F^{-1}(\mathcal{S})$ defined by $xF^{-1}(\mathcal{S})y$ if and only if x and y are in the same element of $\mathcal{S}$ (in the same equivalence class of E).

Note. For the theorem above, we need to verify:

- $F^{-1}(\mathcal{S})$ is an equivalence relation,
- $F \circ F^{-1}(\mathcal{S}) = \mathcal{S}$ for all partitions $\mathcal{S}$,
- $F^{-1} \circ F(R) = R$ for all equivalence relations R.

Example. *Equivalence relations $\iff$ partitions*
Let

$$\begin{aligned} X &= \{1, 2, 3, 4, 5\} \\ R &= \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,5), (5,1), (1,3), (3,1), (3,5), (5,3), (2,4), (4,2)\}. \end{aligned}$$

What is the corresponding partition, i.e. what is $F(R)$?
The corresponding partition to the aforementioned relation R is $\{\{1,3,5\}, \{2,4\}\}$.

Let $\mathcal{S} = \{\{1,2,3\}, \{4,5\}\}$ what is the corresponding equivalence relation? i.e. what is $F^{-1}(\mathcal{S})$?
The corresponding equivalence relation for S is

$$\{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,5), (5,4)\}.$$

3 Counting

Question. If $|X| = n$, and $|Y| = m$, how many functions are there from X to Y?

Every element in the domain must get mapped to something in the codomain, but it does not matter *which* element in the codomain. Furthermore, the function maps each element in the domain to *exactly one* element in the codomain. Observe that for each $x \in X$, there are m "choices" for where x gets mapped. Thus there are $\underbrace{m \cdot m \cdots m}_{n \text{ times}} = m^n$ total functions.

Theorem — *Multiplication principle*
If a set can be enumerated/constructed in t steps (where each step is independent of the other steps) and each step has n_i choices/outcomes, then the set has $n_1 n_2 \cdots n_t$ elements.

Example. I am going to get a pizza from Vito's or D'more's:

Vito's:	D'more's:
2 crusts	1 crust
6 toppings	2 sauces
2 cheeses	3 toppings

The total number of pizzas I could order is: $2 \cdot 6 \cdot 2 + 1 \cdot 2 \cdot 3 = 30$.

Theorem — *Addition principle*
If X and Y are disjoint finite sets, then $|X \cup Y| = |X| + |Y|$.

Example. How many strings of length 5 in $\{0, 1\}$ start with 10 or end with 01?

By the multiplication principle, we know there are 2^3 strings that start with 10. By similar reasoning, there are 2^3 strings that end with 01. Furthermore, there are 2 strings that satisfy both of these properties. Thus the total number of strings satisfying the statement above is $2^3 + 2^3 - 2 = 16$.

Theorem — *Inclusion/Exclusion principle*
If X, Y are finite sets, then

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Note. The addition principle is just a special case of the inclusion/exclusion principle where $X \cap Y = \varnothing$.

Proposition. If $X_1, X_2, \ldots, x_n$ are finite sets, then

$$|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \cdot |X_2| \cdots |X_n|.$$

Proof. Let the n_i be the cardinality of X_i. The proposition is true by the multiplication principle and definition of cartesian product. □

Example. How many injective functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

There are $5 \cdot 4 \cdot 3$ functions. When constructing f, there are five elements that a can map to, four elements that b can map to (because it cannot map to $f(a)$), and three elements that c can map to (because it cannot map to $f(a)$ or $f(b)$).

Example. If the cardinality of a set X is 50, how many symmetric relations are there on X?

Let the elements of X be $x_1, \dots, x_{50}$. We can depict the set of all relations on X as shown:

$$\begin{bmatrix} (x_1, x_1) & \dots & (x_1, x_{50}) \\ \vdots & \ddots & \vdots \\ (x_{50}, x_1) & \dots & (x_{50}, x_{50}) \end{bmatrix}$$

Observe that every symmetric relation on X can be represented as a subset of the top right triangle of the matrix. There are $\frac{50(51)}{2}$ elements in that triangle (observe that the diagonals form the integers from 1 to 50), so there are $2^{\frac{50(51)}{2}}$ symmetric relations on X.

3.1 Permutations and Combinations

Example. My, my wife, my cat, and my baby are going to line up for a photo. In how many ways can this be done?

There are four "choices" for where I go, 3 choices for where the cat goes, 2 for where the baby goes, and 1 for where the wife goes. Thus there are $4! = 24$ ways to line up for a photo.

Note. This is the same as the number of bijections on the set $\{\text{me}, \text{wife}, \text{cat}, \text{baby}\}$.

Definition. *Permutation*
A *permutation* of an n-element set is an ordering of the n elements. In other words, a permutation of a set X is a bijection from X to itself.
An n element set has $n!$ permutations.

Example. Ten distinct people form a circle. How many different circles are there? (We define two circles to be the same if you can rotate one of them to get the other)

Pick one "favorite" person from the group. Then each circle has a unique representation where the favorite person remains at the top of the circle, so there are 9 remaining slots for the others to fill. There are 9! different circles.

Example. In my family of four, in how many ways can two of us line up for a photo?

There are four choices for the first person, and three choices for the second person (note that the order of the people taking the photo still matters). There are $4 \cdot 3 = 12$ ways to do this.

Definition. *r-permutation*
An *r-permutation* from an n element set is an ordering of r elements from the set. In other words, it is a function $f \colon \{1, 2, \dots, r\} \to \{1, 2, \dots, n\}$.
The number of r-permutations from a set with n elements is denoted

$$P(n, r) = \frac{n!}{(n-r)!} = n(n-1)\cdots(n-r+1).$$

We say $P(n, r) = 0$ if $r > n$ (or if n or r is negative).

Example. Five people are stranded on an island. They find a boat that can hold three people. In how many ways can they choose three people to escape?

Note that the order of the people being rescued *does not* matter. Say we choose the first three people out of a permutation of the five people. We overcount because the order of the first three people doesn't matter, nor does the order of the two people left on the island. Thus the total number is $\binom{5}{3} = \frac{5!}{3!(5-3)!}$ ways to choose three survivors.

Definition. *r-combination*
An *r-combination* from an n-element set is a choice of r elements from the set.
The number of r-combinations from an n-element set is denoted

$$C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}.$$

We say $\binom{n}{r} = 0$ if $r > n$ (or if n or r is negative).

Note. If $|X| = n$ for some set X, then there are $\binom{n}{r}$ subsets of X with r elements.

3.2 More Counting

Example. *Poker Hands*
A deck of cards has 52 cards in four suits. There are thirteen different denominations:

- The numbers 2-10
- Jack
- Queen
- King
- Ace

A hand in poker is just five cards.

(a) How many distinct hands are there?

There are $\binom{52}{5} \sim 2.5$ million ways to choose 5 cards out of 52.

(b) How many flushes are there? (When all the cards are the same suit)

There are $\binom{13}{5} \cdot 4$ ways, because there are $\binom{13}{5}$ ways to get a flush for a given suit, and you multiply by 4 because there are 4 suits.

(c) How many hands have three cards of one denomination and two of another?

There are $13 \cdot \binom{4}{3} \cdot 12 \cdot \binom{4}{2}$ such hands. There are 13 choices for the first denomination, and you choose 3 out of the 4 cards to form your hand, then 12 remaining denominations, and you choose 2 out of those 4 cards to form your hand.

Example. How many words/strings can be formed using all of the letters of COMBINATORICS? (i.e. how many ways are there to rearrange the letters of COMBINATORICS)

Although the word has 13 letters, it is not 13! because you have repeated letters that are indistinguishable from each other, so you will overcount. For example, C_1OMBINATORIC_2S and C_2OMBINATORIC_1S are the same word, although 13! would count them differently. Thus we divide by the number of ways to rearrange the indistinct letters, namely the 2 C's, 2 O's, and 2 I's. We get $\frac{13!}{2!2!2!}$.
Alternatively, we could also imagine filling thirteen slots with the letters in the word combinatorics. There are $\binom{13}{2}$ ways to put down the two C's, $\binom{11}{2}$ ways to put the two O's in the remaining 11 slots, and $\binom{9}{2}$ ways to put down the two I's in the 9 remaining slots. Finally, the last 7 letters may be put in any order. Thus we have $\binom{13}{2}\binom{11}{2}\binom{9}{2}7!$ ways.

Note (Generalized permutations). If a collection of n items has: n_1 of one type (all identical), n_2 of another type (also all identical), $\ldots$, n_t of type t (where $n_1 + n_2 + \cdots + n_t = n$), then the number of ways to order the n items is:

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-(n_1+\cdots n_{t-1})}{n_t},$$

or we may also write

$$\frac{n!}{n_1!n_2!\cdots n_t!}.$$

Example. Harry, Ron, and Hermione are sharing 10 (distinct) every flavor beans. Harry gets 5, Hermione 3, and Ron gets 2. In how many ways can they distribute the beans?

There are 10! total ways to arrange 10 distinct beans. We then divide by the number of ways to rearrange each person's beans, so we have $\frac{10!}{5!3!2!}$ total ways to distribute the beans.
Alternatively, we may choose 5 beans from 10 to give to Harry, 3 from the remaining 5 for Hermione, and 2 from the last 2 for Ron. Thus we have $\binom{10}{5}\binom{5}{3}\binom{2}{2}$ ways to distribute the beans.

Example. Harry, Ron, and Hermione have 10 identical beans. In how many ways can they divide up the beans?

We will denote the beans as stars, and use bars to divvy up the beans between the three people. Thus we have 10 stars and 2 bars. An example distribution looks like this:

$$\underbrace{**}_{\text{Harry's beans}} \mid \underbrace{*****}_{\text{Hermione's beans}} \mid \underbrace{***}_{\text{Ron's beans}}$$

Observe that any such distribution is akin to having 12 items total and just choosing where the 2 bars go. Thus we have $\binom{10+3-1}{3-1}$ ways to distribute the beans (The -1 is because three people only need 2 bars, not 3).

Note (Stars and Bars). If a set has t elements, the number of unordered selections from the set with k-elements (with repetitions allowed) is $\binom{k+t+1}{t-1}$.

Example. How many solutions are there to the equation:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 25, \text{where all } x_i \geq 0 \text{ and } x_i \in \mathbb{Z}$$

We have 25 stars (the total sum) and 4 bars (dividing the 25 stars into 5 categories). The number of stars in each area represents the value of each variable. Thus we have $\binom{25+5-1}{5-1} = \binom{29}{4}$ ways to satisfy the equation with the given restrictions.

Problem. What if all $x_i \geq 1$?

This is the same as if the number of solutions to $x_1 + x_2 + x_3 + x_4 + x_5 = 20$.

Warm Up. Find the number of solutions to $x_1 + x_2 + x_3 + x_4 = 20$, where $x_i \in \mathbb{N}$.

We have 20 "stars" and 3 bars, so the number of possible solutions to this is $\binom{23}{3}$.

What if $x_4 \geq 5$?

We will first allocate 5 stars to the compartment for x_4, so this is equivalent to finding the number of solutions to the equation $x_1 + x_2 + x_3 + x_4 = 15$. There are $\binom{18}{3}$ such solutions.

What if $x_4 \leq 4$? (and all $x_i \in \mathbb{N}$)

We can do complementary counting–we subtract the solutions to $x_1 + x_2 + x_3 + x_4 = 20$ with $x_4 \geq 5$ from the solutions to $x_1 + x_2 + x_3 + x_4 = 20$. Thus we have $\binom{23}{3} - \binom{18}{3}$.
or we may count the cases where $x_4 = 0, 1, 2, 3, 4$. In other words, adding the number of solutions to the equations $x_1 + x_2 + x_3 = 20, 19, 18, 17, 16$. Thus we have

$$\binom{22}{2} + \binom{21}{2} + \binom{20}{2} + \binom{19}{2} + \binom{18}{2} = \binom{23}{3} + \binom{18}{3}.$$

3.3 Combinatorial Identities

Example. Let's expand $(x+y)^5 = (x+y)(x+y)(x+y)(x+y)(x+y)$.
When creating a term in their product, observe that we either choose an x term or a y term from each $x + y$. Thus every term is a sum of monomials of the form $x^i y^j$ where $i + j = 5$. There are 2^5 terms before gathering like terms. We ask ourselves, what is the coefficient on an arbitrary monomial $x^i y^j$? In other words, how many ways are there to choose an i number of x terms and a j number of y terms from the $i + j$ total terms? There are $(i + j)!$ ways to order all $i + j$ terms, but we have i identical x terms and j identical y terms. Thus we must divide by $i!$ and $j!$ to account for the redundancies. Thus the coefficient on the $x^i y^j$ term is $\frac{(i+j)!}{i!j!} = \binom{i+j}{i} = \binom{i+j}{j}$.

Theorem — *Binomial Theorem*
For $n \in \mathbb{N}$, we have

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

The proof uses the same argument as the above.

Example.

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

Additionally, observe that 2^n is the total number of subsets of a set X with cardinality n. Furthermore, the right hand side is the sum of the number of subsets with cardinality k of X, for all $0 \leq k \leq n$. Thus they are equal.

Example.

$$3^n = (2+1)^n = \sum_{k=0}^{n} \binom{n}{k} 2^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} 2^k$$

Exercise. Try to find a counting argument to prove this identity. Hint: If $|X| = n$, there are 3^n pairs of subsets of X of the form (A, B) where $A \subseteq B$.

3.4 Pascal's Triangle

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Each term is the sum of the two terms above it, and the outermost diagonals are all 1's.

Note (Pascal's Triangle Observations).

- It is symmetrical about the vertical axis
- $\binom{n}{1} = \binom{n}{n-1} = n$
- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$
- The sum of the nth row is 2^{n-1}
- $\sum_{i-k}^{n} \binom{i}{k} = \binom{n+1}{k+1}$

Claim. $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$.

Proof. Let X be a set with $n+1$ elements. The left hand side counts the number of ways to choose an i-element subset from X. Observe that $\binom{n}{i}$ counts the number of i-element subsets that don't contain a particular element x_1 of X, while $\binom{n-1}{i}$ counts the number of i-element subsets that do contain x_1. Thus these two sets form a partition for the subsets of X with i elements, so $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$. $\square$

Note. The above proof may be thought of more concretely by letting X be the set $\{0, 1, \ldots, n\}$, and choosing subsets of X with and without 0.

Claim. $\sum_{i=k}^{n}\binom{i}{k}=\binom{n+1}{k+1}$.

Proof. We know that $\binom{n+1}{k+1}$ is the number of ways to choose $k+1$ distinct objects from $n+1$ objects. We partition these ways into sets S_k, S_{k+1}, S_n, where $|S_i|=\binom{i}{k}$. Consider fixing the maximum of the set, and then choosing the remaining k items from the items less than the "max". Then for some maximum $i+1$, there are $\binom{i}{k}$ ways to choose the remaining k items from the first i items. Iterating from $i=k$ to $i=n$, we see that this counts the ways to choose $k+1$ items from $n+1$ total items, so the statement holds. □

Example. How many ways are there to choose 4 items from the numbers 1-7 where the largest item is 6?

You first pick 6, then you need to pick 3 items from the first 5 items, so we have $\binom{6-1}{4-1}=\binom{5}{3}$ ways to do this. This is the same logic that we are using in the above, except we are also steadily increasing the maximum to form a partition.

Alternative Proof of the Above Claim. We will use the fact that $\binom{n}{i}+\binom{n}{i-1}=\binom{n+1}{i}$.

Proof.

$$\begin{aligned}\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{n}{k}&=\binom{k}{k}+\left(\binom{k+2}{k+1}-\binom{k+1}{k+1}\right)+\cdots+\left(\binom{n+1}{k+1}-\binom{n}{k+1}\right)\\&=\binom{k}{k}-\binom{k+1}{k+1}+\binom{n+1}{k+1}\\&=\binom{n+1}{k+1}.\end{aligned}$$

□

3.5 Pigeonhole Principle

If n pigeons fly into k holes, and $n>k$, at least one hole will contain more than one pigeon.

Claim. There are at least two people in this Zoom room that were born on the same day of the month (not necessarily the same month).

There are 31 possible days of the month to be born on (the holes), and there are 45 people in the Zoom room (the pigeons), so there is at least one day which has more than one person born on it.

Definition. *Pigeonhole Principle*
If X and Y are finite sets and $|X|>|Y|$, then every function $f\colon X\to Y$ is *not* injective.

Example. There is a party with 10 people—at least 2 people know the same number of people there (assume knowing is symmetric).

Let the ten people be denoted $p_1, p_2, \ldots, p_{10}$. There are 10 options for how many other people they can know (0-9). However, because knowing is symmetric, we cannot simultaneously have someone who knows 0 people and someone who knows 9 people (everyone else). So, there are really 9 options (either 0-8 or 1-9). Thus, by pigeonhole principle, there exists two people that know the same number of people.

Note. The pigeonhole principle is an *existence proof.* It doesn't tell us who the people are, how many of them there are—just that they *exist.* It is also called *non-constructive*, because we don't explicitly say who the two people are (construct the group).

Example. In this class there are 170 people. What's the largest number of people (in the class) that we know for sure are born in the same month?

Because $170 > 12 \cdot 14$, we know that it can't be the case that in each month ≤ 14 people were born in that month. So, there must exist some month where at least 15 of us were born in that month.

Definition. *Generalized Pigeonhole Principle*
If there are more than $m \cdot k$ pigeons that go into k holes, then some hole has more than m pigeons. In other words, if $f\colon X \to Y$, $|X| = n$, $|Y| = m$, $k = \left\lceil \frac{n}{m} \right\rceil$, then there are k distinct values $a_1, \ldots, a_k \in X$ with $f(a_1) = f(a_2) = \cdots = f(a_k)$.

Example. There is a number consisting only of 1s (i.e. $11111\ldots111$) that is divisible by 137529.

Notice that if n_1 has remainder r_1 when divided by m and n_2 has remainder r_2 when divided by m, then $n_1 + n_2 = mk + r_1 + r_2$, for some integer k.

39 has a remainder of 4 when divided by 5, and 41 has a remainder of 1 when divided by 5, so $39 + 41$ has a remainder of 5 when divided by 5 (aka no remainder).

Two numbers consisting only of 1s have the same remainder when dividing by 137529, provided that the string of 1s is sufficiently long, so their difference is divisible by 137529. Notice that their difference will be of the form $111\ldots1100\ldots0$. Thus 137529 divides this number consisting of only 1s (because we can factor out some 10^k).

Example. In any group of six people, there are either 3 people that know each other or 3 people that don't know each other (where knowing is symmetric).

In other words: Take six nodes, and draw all possible edges between them. Color each edge blue or red. There is a triangle with all blue or all red edges.

By the generalized pigeonhole principle, each person either knows at least three people or they don't know at least three people. Consider the case where one person knows three other people, say P_1 knows P_2, P_3, P_4. Then if any of P_2, P_3, P_4 knows anyone else in the group, then we have our group of 3 people that know each other. However, if all of them don't know each other, then we have a group of 3 people that don't know each other.

3.6 Recurrence Relations

Say we are building a garden wall. It's 20 feet long, 2 feet high, and made out of 1×2 foot bricks. In how many ways can I build the wall(the many combinations come from either stacking the bricks vertically or horizontally)?

Let w_n be the number of ways to build an n foot wall. Then

n	1	2	3	4	5	6	7	8	$\cdots$
w_n	1	2	3	5	8	13	21	34	$\cdots$

In building a wall, observe that the number of ways to build an n foot wall where the first brick is upright is w_{n-1}, because after putting down the first brick you need to build a $n-1$ foot wall. Similarly, the number of ways to build a n foot wall where the first brick is sideways is w_{n-2}, because after putting down the first brick (or two), you need to build a $n-2$ foot wall. Thus for $n \geq 3$, we have $w_n = w_{n-1} + w_n - 2$.

Definition. *Recurrence Relation*
A *recurrence relation* is an equation for the nth term of a sequence in terms of the previous terms of the sequence. Given *initial conditions*, you can use the relation to compute all terms of the sequence (in the example above, we computed w_1 and w_2).

Example. I have \$1000, it earns 7% interest, compounded annually. How much do I have after n years?

Let P_n be the amount of money I have after n years. Then $P_n = (1.07)P_{n-1}$, $P_0 = 1000$.

What if I add \$1000 dollars each year?

Then the new recurrence relation becomes $P_n = (1.07)P_{n-1} + 1000$.

Example. Suppose you have an $n \times n$ board. How many routes can you take from the lower left corner to the top right corner of the board, only moving to the right and up that don't go above the diagonal? We will denote this number as C_n.

By convention, we say that $C_0 = 1$. Looking at 1×1 and 2×2 grids, we see that $C_1 = 1$ and $C_2 = 2$. Observe that the "first move" that we make is fixed because we can't go up with our first move. We ask, what is the number of allowed routes in the $n \times n$ board that first hit the diagonal at (k, k)? Observe that this partitions the board into two smaller boards, one of size k and another of size $n - k$. However, because we do not hit the diagonal until (k, k), our first move must be to the right, and our last move must be up. Thus we have that the number of routes from $(0, 0)$ to (k, k) is C_{k-1}. Then we have C_{n-k} ways to traverse the remaining $(n - k) \times (n - k)$ grid. Letting k be anything between 1 and n, we have

$$C_n = \sum_{k=1}^{n} C_{k-1}C_{n-k}.$$

3.7 Solving Recurrence Relations

Example. *The Towers of Hanoi*
We have n discs of increasing size, 3 posts, where each disc rests on a post. We can only move a disc if it rests upon a larger disc. In how few moves can we move all the discs to another post?

If we have one disc, then we can move it to another post in one move. With two discs, we need three moves. To solve a tower with n discs, we can move a tower with $n-1$ discs to the middle post, move the bottom disc to the third post, and then move the $n-1$ discs back on top of the largest disc. Thus we have the recurrence relation $h_n = 2h_{n-1} + 1$.

How can we get an explicit form for this relation? Observe that

$$\begin{aligned}
h_n &= 2h_{n-1} + 1 \\
&= 2(2h_{n-2} + 1) + 1 \\
&= 2(2(2h_{n-3} + 1) + 1) + 1 \\
&\vdots \\
&= 2^n h_0 + 2^0 + 2^1 + \cdots + 2^{n-1} && \text{Prove using induction} \\
&= 2^n h_0 + 2^n - 1 \\
&= 2^{n+1} - 1
\end{aligned}$$

Example. Consider the sequence defined by $s_0 = 2$, $s_1 = 5$, and $s_n = 5s_{n-1} - 6s_{n-2}$ for $n \geq 2$.

Ansatz: s_n grows exponentially, for example $s_n = x^n$ for some x. Then

$$\begin{aligned}
x^n &= 5x^{n-1} - 6x^{n-2} \\
x^n - 5x^{n-1} - 6x^{n-2} &= 0 \\
x^{n-2}(x^2 - 5x - 6) &= 0.
\end{aligned}$$

Thus we have that $x = 0, 2, 3$. Any sequence $s_n = a3^n + b2^n$ for some real numbers a, b will satisfy the recurrence relation. All that's left is to make sure our recurrence relation matches the initial conditions given. We have

$$\begin{aligned}
s_0 &= a + b = 2 \\
s_1 &= 3a + 2b = 5,
\end{aligned}$$

so $a = b = 1$, and $s_n = 2^n + 3^n$.

Note. Linear combinations of recurrence relations also satisfy the recurrence relation.