Lecture 3: More counting
Binomial Coefficients, Binomial Theorem, Inclusion-Exclusion
Announcements

• Office hours start today
  – In particular, I will be available for office hours starting right after class today (CSE 668)

• Problem Set 1
  – Read the first page for how to write up your homework solutions. Don’t wait until you are working on the questions to figure it out.
  – Section solutions are another good place to look at for examples.

• Resources
  – Textbook readings can provide another perspective
  – Office Hours
  – EdStem discussion

• EdStem discussion etiquette
  – OK to publicly discuss content of the course and any confusion over topics discussed in class, but **not solutions** for current homework problems, or anything about current exams that have not yet been graded.
  – It is also acceptable to ask for clarifications about what current homework problems are asking and concepts behind them, just not about their solutions.
Recap of Last Time

**Permutations.** The number of orderings of \( n \) distinct objects

\[ n! = n \times (n - 1) \times \cdots \times 2 \times 1 \]

**Example:** How many sequences in \( \{1,2,3\}^3 \) with no repeating elements?

**k-Permutations.** The number of orderings of only \( k \) out of \( n \) distinct objects

\[ P(n, k) = n \times (n - 1) \times \cdots \times (n - k + 1) \]

\[ = \frac{n!}{(n-k)!} \]

**Example:** How many sequences of 5 distinct alphabet letters from \( \{A, B, \ldots, Z\} \)?

**Combinations / Binomial Coefficient.** The number of ways to select \( k \) out of \( n \) objects, where ordering of the selected \( k \) does not matter:

\[ \binom{n}{k} = \frac{P(n, k)}{k!} = \frac{n!}{k! \cdot (n-k)!} \]

**Example:** How many size-5 subsets of \( \{A, B, \ldots, Z\} \)?

**Example:** How many shortest paths from Gates to Starbucks?

**Example:** How many solutions \((x_1, \ldots, x_k)\) such that \( x_1, \ldots, x_k \geq 0 \) and \( \sum_{i=1}^{k} x_i = n \)?
Recap* Example – Counting Paths

A slightly modified example

Path $\in \{\uparrow, \rightarrow\}^7$

Example path:
$(\uparrow, \rightarrow, \uparrow, \rightarrow, \rightarrow, \uparrow, \rightarrow)$

Also like Seattle example.

Imagine $\uparrow, \uparrow, \uparrow, \rightarrow, \rightarrow, \rightarrow, \rightarrow$ under multiply.

$7! = \frac{7!}{3!4!}$

Order of $\uparrow$ doesn’t matter.
Agenda

• Binomial Coefficients
• Binomial Theorem
• Inclusion-Exclusion
Binomial Coefficient – Many interesting and useful properties

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

\[
\begin{align*}
\binom{n}{n} &= 1 \\
\binom{n}{1} &= n \\
\binom{n}{0} &= 1
\end{align*}
\]

Fact. \( \binom{n}{k} = \binom{n}{n-k} \)

Symmetry in Binomial Coefficients

Fact. \( \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \)

Pascal’s Identity

Fact. \( \sum_{k=0}^{n} \binom{n}{k} = 2^n \)
Symmetry in Binomial Coefficients

Fact. \( \binom{n}{k} = \binom{n}{n-k} \)

This is called an Algebraic proof, i.e., Prove by checking algebra

Proof. \[
\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!} = \binom{n}{n-k}
\]

Why??
Symmetry in Binomial Coefficients – A different proof

Fact. \( \binom{n}{k} = \binom{n}{n-k} \)

Two equivalent ways to choose \( k \) out of \( n \) objects (unordered)
1. Choose which \( k \) elements are included
2. Choose which \( n-k \) elements are excluded

\[
\binom{4}{1} = 4 = \binom{4}{3}
\]
Symmetry in Binomial Coefficients – A different proof

Fact. \( \binom{n}{k} = \binom{n}{n-k} \)

Two equivalent ways to choose \( k \) out of \( n \) objects (unordered)
1. Choose which \( k \) elements are included
2. Choose which \( n - k \) elements are excluded

Format for a combinatorial argument/proof of \( a = b \)
- Let \( S \) be a set of objects
- Show how to count \( |S| \) one way \( \Rightarrow |S| = a \)
- Show how to count \( |S| \) another way \( \Rightarrow |S| = b \)
Combinatorial argument/proof

- Elegant
- Simple
- Intuitive

Algebraic argument

- Brute force
- Less Intuitive
Pascal’s Identity

**Fact.** \( \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \)

How to prove Pascal’s identity?

**Algebraic argument:**

\[
\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)! (n-k)!} + \frac{(n-1)!}{k! (n-1-k)!} \\
= \frac{20 \text{ years later} ...}{n!} \\
= \frac{n!}{k! (n-k)!} \\
= \binom{n}{k}
\]

Hard work and not intuitive

Let’s see a combinatorial argument
Example – Pascal’s Identity

**Fact.** \( \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \)

|S| = |A| + |B|

**Combinatorial proof idea:**
- Find *disjoint* sets \( A \) and \( B \) such that \( A, B, \) and \( S = A \cup B \) have the sizes above.
- The equation then follows by the Sum Rule.
Example – Pascal’s Identity

Fact. \( \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \)

\[ |S| = |A| + |B| \]

**Combinatorial proof idea:**
- Find *disjoint* sets \( A \) and \( B \) such that \( A, B, \) and \( S = A \cup B \) have these sizes

\( S \): set of size \( k \) subsets of \([n] = \{1, 2, \ldots, n\} \).

- \( \text{e.g. } n = 4, k = 2, \ S = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\} \)

\( A \): set of size \( k \) subsets of \([n] \) that *DO* include \( n \)

- \( A = \{\{1,4\}, \{2,4\}, \{3,4\}\} \)

\( B \): set of size \( k \) subsets of \([n] \) that *DON’T* include \( n \)

- \( B = \{\{1,2\}, \{1,3\}, \{2,3\}\} \)
Example – Pascal’s Identity

Fact. \( \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \)

|S| = |A| + |B|

\( S \): set of size \( k \) subsets of \([n] = \{1, 2, \ldots, n\} \).

\( A \): set of size \( k \) subsets of \([n] \) that DO include \( n \)

\( B \): set of size \( k \) subsets of \([n] \) that DON’T include \( n \)

Combinatorial proof idea:
• Find disjoint sets \( A \) and \( B \) such that \( A, B \), and \( S = A \cup B \) have these sizes

\( n \) is in set, need to choose other \( k - 1 \) elements from \([n - 1]\)

\[ |A| = \binom{n-1}{k-1} \]

\( n \) not in set, need to choose \( k \) elements from \([n - 1]\)

\[ |B| = \binom{n-1}{k} \]
Agenda

• Binomial Coefficients
• Binomial Theorem
• Inclusion-Exclusion
Binomial Theorem: Idea

\[(x + y)^2 = (x + y)(x + y) = xx + xy + yx + yy = x^2 + 2xy + y^2\]

\[(x + y)^4 = (x + y)(x + y)(x + y)(x + y) = xxxx + yyyyy + xyxy + yxyy + \ldots\]

Poll: What is the coefficient for \(xy^3\)?

A. 4
B. \(\binom{4}{1}\)
C. \(\binom{4}{3}\)
D. 3

https://pollev.com/paulbeameo28
Binomial Theorem: Idea

\[(x + y)^n = (x + y) \ldots (x + y)\]

Each term is of the form \(x^k y^{n-k}\), since each term is made by multiplying exactly \(n\) variables, either \(x\) or \(y\), one from each copy of \((x + y)\).

How many times do we get \(x^k y^{n-k}\)?

The number of ways to choose \(x\) from exactly \(k\) of the \(n\) copies of \((x + y)\) (the other \(n - k\) choices will be \(y\)) which is:

\[
\binom{n}{k} = \binom{n}{n-k}
\]
Binomial Theorem

**Theorem.** Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$ a positive integer. Then,

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

Many properties of sums of binomial coefficients can be found by plugging in different values of $x$ and $y$ in the Binomial Theorem.

**Corollary.**

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

- Binomial Coefficients
- Binomial Theorem
- Inclusion-Exclusion
Recap Disjoint Sets

Sets that do not contain common elements ($A \cap B = \emptyset$)

**Sum Rule:** $|A \cup B| = |A| + |B|$
Inclusion-Exclusion

But what if the sets are not disjoint?

Fact. \(|A \cup B| = |A| + |B| - |A \cap B|\)

|A| = 43
|B| = 20
|A \cap B| = 7
|A \cup B| = ???
Inclusion-Exclusion

What if there are three sets?

What if there are three sets?

\[|A| = 43\]
\[|B| = 20\]
\[|C| = 35\]
\[|A \cap B| = 7\]
\[|A \cap C| = 16\]
\[|B \cap C| = 11\]
\[|A \cap B \cap C| = 4\]
\[|A \cup B \cup C| = ??\]

Fact.

\[|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|\]
Inclusion-Exclusion

Let $A, B$ be sets. Then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

In general, if $A_1, A_2, \ldots, A_n$ are sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \text{singles} - \text{doubles} + \text{triples} - \text{quads} + \cdots$$

$$= (|A_1| + \cdots + |A_n|) - (|A_1 \cap A_2| + \cdots + |A_{n-1} \cap A_n|) + \cdots$$
Example: RSA

• In encrypting messages using RSA one starts with
  – Two big prime numbers \( p \) and \( q \) that are kept secret
  – Encodes messages using arithmetic \( \text{mod } N \) for \( N = pq \).
  – One needs to work with numbers \( \text{mod } N \) that have no common factors with \( N \) (“co-prime with \( N \)’’)
    • Otherwise the secret leaks or decryption may not be defined uniquely.

  – To define RSA one needs to know how many such numbers there are…
Example: $p = 3, q = 5 \mod 15 = 3 \times 5$

$B = \{0, 5, 10\}$

$A = \{0, 3, 6, 9, 12\}$

$|B| = 3$

$|A| = 5$

$A \cap B$ contains multiples of 3 & 5 (mod 15)  

$A \cap B = \{0\}$

# Integers between 0 and 14 that share a non-trivial divisor with 15 =  

$|A| + |B| - |A \cap B| = 3 + 5 - 1 = 7$

# Integers between 0 and $N - 1$ that are co-prime with $N$  

$= 15 - 7 = 8 \equiv 2 \cdot 4$
Integers mod $N$ co-prime with $N = pq$ for $p, q$ prime

$B = \{0, q, 2q, ..., (p - 1)q\}$

$A = \{0, p, 2p, ..., (q - 1)p\}$

$|B| = p$

$|A| = q$

$A \cap B$ contains multiples of $p$ & $q$ (mod $N$)  $A \cap B = \{0\}$

# Integers between 0 and $N - 1$ that share a non-trivial divisor with $N$

$= |A| + |B| - |A \cap B| = p + q - 1$

# Integers between 0 and $N - 1$ that are co-prime with $N$

$= N - (p + q - 1) = pq - p - q + 1 = (p - 1)(q - 1)$
Agenda

• Binomial Coefficients
• Binomial Theorem
• Inclusion-Exclusion