CS70 @ UC Berkeley, Spring 2026

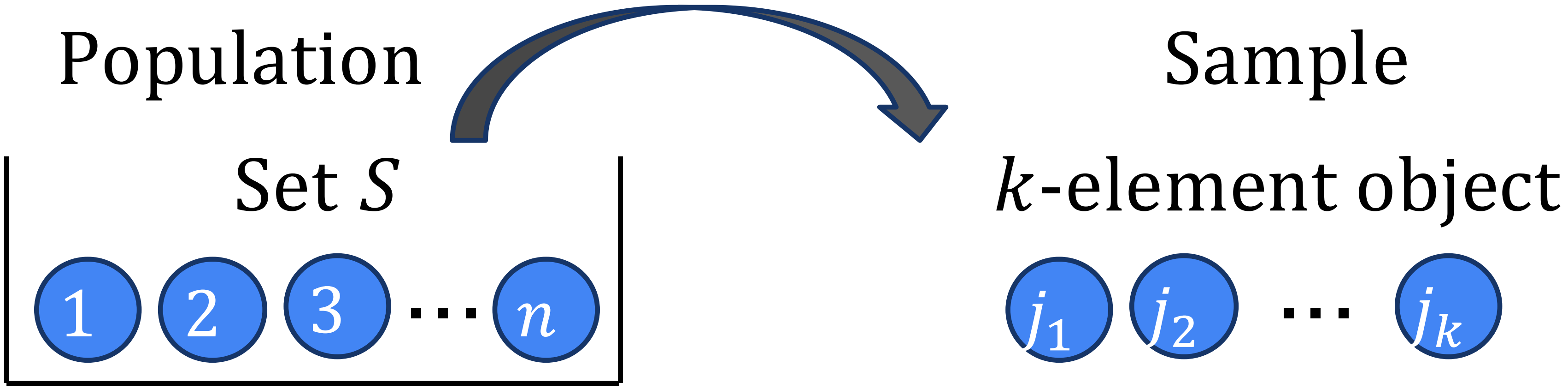
Lecture 15
Counting II

March 10, 2026

Last Lecture

1. Counting
2. Sampling k-element objects from some set S
3. Counting functions $f: X \to S$ between two finite sets, where $|X| = k$ and $|S| = n$.
4. Key rules of counting

Sampling



\# **inequivalent** k-element objects depends on whether

- sampled objects are **ordered** or **unordered.**

  (2 3 and 3 2 are distinct 2-element **ordered** objects, but the same **unordered** objects.)

- sampling is done with or without **replacement**

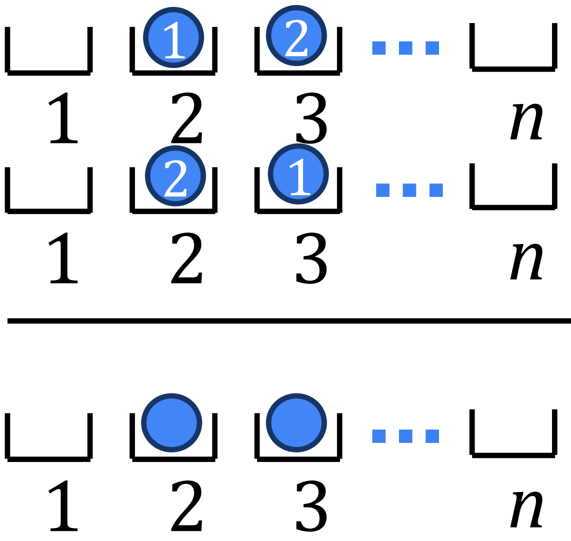
Counting functions between two finite sets

$$\boxed{f: X \to S, \text{ where } |X| = k \text{ and } |S| = n}$$

The number of inequivalent functions f depends on:

- **Restrictions** on f
  - f is arbitrary (no restriction).
  - f is injective (one-to-one). Need $k \le n$.
  - f is surjective (onto). Need $k \ge n$.
- Whether the elements of X and S are **distinguishable** or **indistinguishable**.

Balls and Bins



Summary

$$\boxed{f: X \to S, \text{ where } |X| = k \text{ and } |S| = n}$$

	Elements of X	**Elements of S**	**Arbitrary f** (Sampling with replacement)	**Injective f** (Sampling without replacement)
Ordered	Distinguishable	Distinguishable	Case 1 n^k	Case 2 $\frac{n!}{(n-k)!}$
Unordered	Indistinguishable	Distinguishable	Case 4 $\binom{n+k-1}{k}$	Case 3 $\binom{n}{k}$

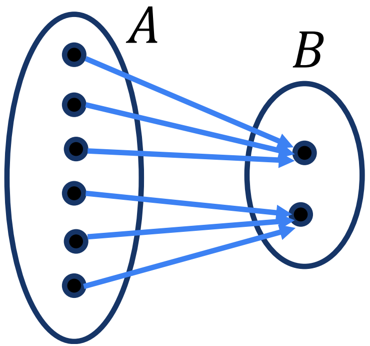
Second Rule of Counting

- More generally, if there exists an m-to-1 surjective map

$$g: A \to B$$

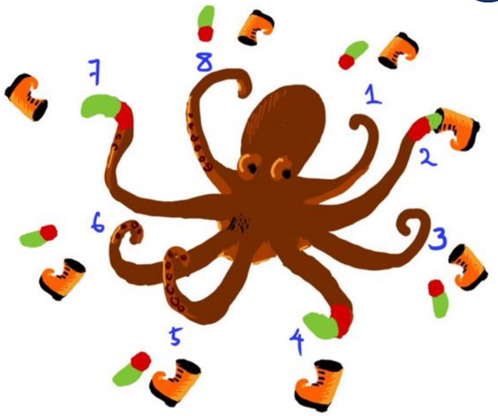
(i.e., for every $x \in B, |g^{-1}(x)| = m$), then

$$|B| = \frac{|A|}{m}$$



Why is this useful?

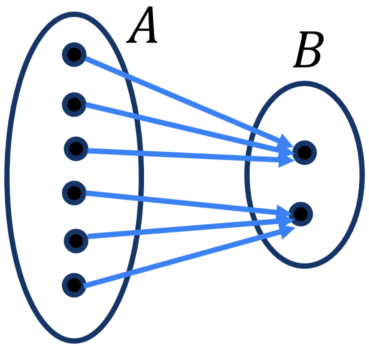
A can be easier to count than B.
Recall the octopus problem from Lecture 14



Key Rules of Counting

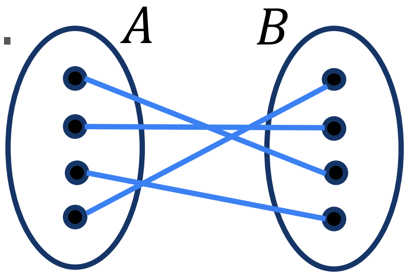
Second Rule of Counting

- More generally, if there exists an m-to-1 surjective map
$$g: A \to B$$
(i.e., for every $x \in B, |g^{-1}(x)| = m$), then
$$|B| = \frac{|A|}{m}$$



Zeroth Rule of Counting

- If there exists a bijection (one-to-one correspondence) between two finite sets A and B, then $|A| = |B|$.



This Lecture

1. Combinatorial Proofs
2. Combinatorial Identities
3. Permutations and Derangements
4. Inclusion-Exclusion Principle
5. Application

Combinatorial Proofs

Theorem 1 (Binomial Theorem). *For all* $n \in \mathbb{N}$,

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

- Proving this by induction is tedious.
- We will provide a combinatorial proof instead:
- **LHS:** $$\underbrace{(a+b)}_{\text{factor 1}}\underbrace{(a+b)}_{\text{factor 2}} \times \cdots \times \underbrace{(a+b)}_{\text{factor n}}$$

  Each factor contributes either a or b when expanded out.
- **RHS:**
  - k copies of a and $n-k$ copies of b leads to $a^k b^{n-k}$.
  - #ways to choose exactly k factors from {factor 1, ..., factor n} without replacement so that they contribute a instead of b is $\binom{n}{k}$.
  - $k \in \{0, \dots, n\}$

A Useful Lemma

Theorem 1 (Binomial Theorem). *For all $n \in \mathbb{N}$,*

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

Lemma 1. *For all $n \in \mathbb{N}$,*

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

Proof: Set $a = -1$ and $b = 1$ in Binomial Theorem. $\square$

Note: We will make use of this lemma later to prove the Inclusion-Exclusion Theorem.

Combinatorial Identities

Theorem 2. *For all* $n, m, k \in \mathbb{Z}^+$,

Note: $\binom{n}{k} = 0$ if $k > n$.

$$\sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j} = \binom{m+n}{k}$$

Proof:

- RHS: $S = \{1,2,\dots,m+n\}$.
  #ways to choose a k-element subset from S is $\binom{m+n}{k}$.
- LHS: $S = \{\underbrace{1,2,\dots,m,}_{\text{Choose } j \text{ elements from here}}\ \underbrace{m+1,\dots,m+n}_{\text{Choose } k-j \text{ elements from here}}\}$
- For each choice in the first part, there are $\binom{n}{k-j}$ possible choices in the second part.
- There are $\binom{m}{j}$ possible choices for the first part.
- $j \in \{0,\dots,k\}$

$\square$

Pascal's Triangle

$$
\begin{array}{l|ccccccccc}
n = 0 & 1 \\
n = 1 & 1 & 1 \\
n = 2 & 1 & 2 & 1 \\
n = 3 & 1 & 3 & 3 & 1 \\
n = 4 & 1 & 4 & 6 & 4 & 1 \\
n = 5 & 1 & 5 & 10 & 10 & 5 & 1 \\
n = 6 & 1 & 6 & 15 & 20 & 15 & 6 & 1 \\
n = 7 & 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \\
n = 8 & 1 & 8 & 28 & 56 & 70 & 56 & 28 & 8 & 1
\end{array}
$$

$k = 0$, $k = 1$, $k = 2$, $k = 3$, $k = 4$, $k = 5$, $k = 6$, $k = 7$, $k = 8$

The (n, k) entry shows $\binom{n}{k}$

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

$$\binom{2}{2} + \binom{3}{2} + \cdots + \binom{6}{2} = \binom{7}{3}$$

$$1 + 3 + 6 + 10 + 15 = 35$$

Theorem 3 (Hockey-Stick Identity). *For all $n, k \in \mathbb{N}$,*

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

$n = 7$ and $k = 2$ in the above example.

Hockey-Stick Identity

Theorem 3 (Hockey-Stick Identity). *For all $n, k \in \mathbb{N}$,*

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

Proof:

RHS: # ways to choose $k+1$ elements from $S = \{1, \dots, n\}$.

LHS: $S = \{\underbrace{1, 2, \dots, j,}\ j+1, \dots, n-1, n\}$

Choose k elements from here.

There are $\binom{j}{k}$ ways.

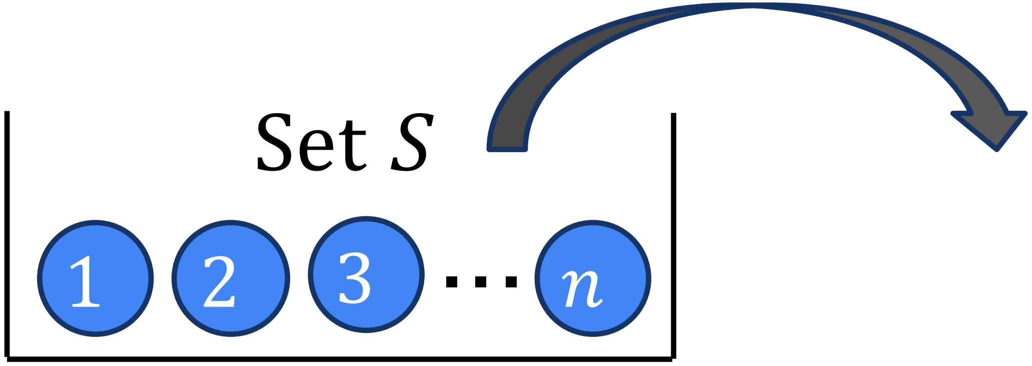
$j \in \{k, k+1 \dots, n-1\}$.

Let this be the **largest** element chosen.

Subsets with different values of the largest element can't be identical.

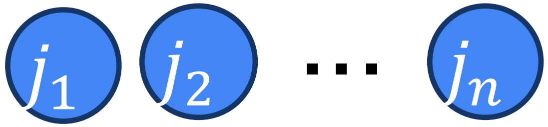
Hence, the total number of ways is given by $\sum_{j=k}^{n-1} \binom{j}{k}$

Permutations and Derangements



Sample without replacement

n-element ordered object



This generates a permutation of $\{1,2,\ldots n\}$.

Total number of permutations $=$ $n!$

Bijection $\pi: S \longrightarrow S$

$\pi: i \longmapsto \pi_i$

Iteration i:	1	2	$\boxed{3}$	4	$\boxed{5}$	…	n
Sampled Label π_i:	7	1	$\boxed{3}$	8	$\boxed{5}$	…	2

Fixed points

Definition: A derangement is a permutation with no fixed points.

Let D_n denote the number of derangements of $\{1,2,\ldots,n\}$.

How does $\frac{D_n}{n!}$ behave as $n \to \infty$?

Derangements

Theorem 4. *Let D_n denote the number of derangements of $\{1, 2, \ldots, n\}$. Then, for $n \geq 3$,*

$$D_n = (n-1)[D_{n-1} + D_{n-2}].$$

Proof: Let π be a **derangement** of $\{1, \ldots, n\}$. So, $\pi_i \neq i$ for all $i = 1, \ldots, n$.

Suppose $\pi_n = 1$

π_1	π_2	π_3	π_4	$\cdots$	π_{n-1}	π_n
$\boldsymbol{n}$	$*$	$*$	$*$	$\cdots$	$*$	**1**
$*$	$\boldsymbol{n}$	$*$	$*$	$\cdots$	$*$	**1**
$*$	$*$	$\boldsymbol{n}$	$*$	$\cdots$	$*$	**1**
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$*$	$*$	$*$	$*$	$\cdots$	$\boldsymbol{n}$	**1**

Derangements of $\{2,3, \ldots, n-1\}$

This gives D_{n-2}

These are not derangements of $\{1,2, \ldots, n-1\}$ but are in bijection with them. **Why?**

This gives D_{n-1}

Replacing n with 1 gives a derangement of $\{1, \ldots, n-1\}$, and all derangements of $\{1, \ldots, n-1\}$ can be obtained this way.

Repeat the argument for $\pi_n = i$, where $i = 2, \ldots, n-1$. $\square$

Derangements

Theorem 4. *Let D_n denote the number of derangements of $\{1, 2, \ldots, n\}$. Then, for $n \geq 3$,*

$$D_n = (n-1)[D_{n-1} + D_{n-2}].$$

- Boundary conditions:
  - $D_1 = 0$
  - $D_2 = 1$

π_1	π_2
2	1

- Solving the recursion gives $$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Can we obtain this formula without having to solve the recursion?

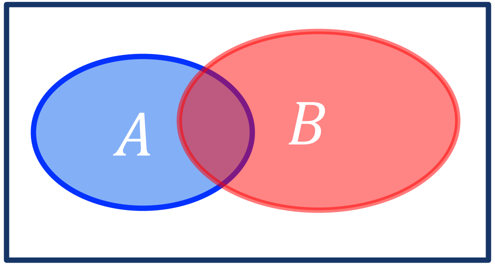
- Asymptotic proportion of derangements:

$$\lim_{n\to\infty} \frac{D_n}{n!} = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} = e^{-1}$$

- Let $A_i = \{\text{permutations } \pi \text{ such that } \pi_i = i \text{ (i.e., } i \text{ is a fixed point)}\}$. Then,

$$D_n = n! - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

Inclusion-Exclusion Principle



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

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

Theorem 5. *Let $A_1, \ldots, A_n$ be arbitrary subsets of the same set Ω. Then,*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1,\ldots,n\}:|S|=k} \left| \bigcap_{i \in S} A_i \right|.$$

- Back to derangements:
  - If $|S| = k$, then $|\bigcap_{i \in S} A_i| = (n-k)!$
  - \# such subsets $= \binom{n}{k}$

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}$$

Hence, $D_n = n! - |A_1 \cup A_2 \cup \cdots \cup A_n| = n! \left[1 - \sum_{k=1}^{n} (-1)^{k-1} \frac{1}{k!} \right] = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

Proof of the Inclusion-Exclusion Formula

Theorem 5. *Let $A_1, \dots, A_n$ be arbitrary subsets of the same set Ω. Then,*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1,\dots,n\}:|S|=k} \left| \bigcap_{i \in S} A_i \right|.$$

Proof:

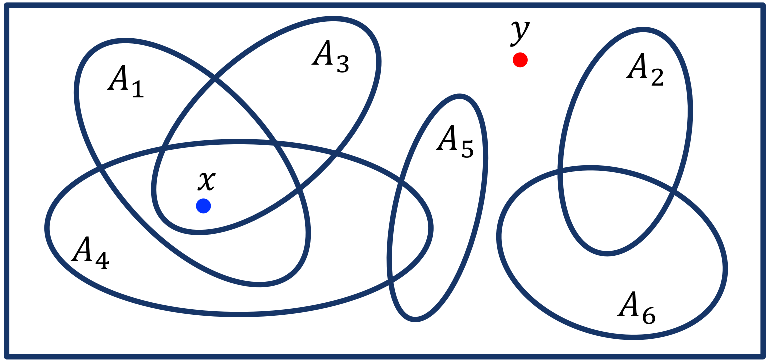
1. Every element that is not contained in $A_1 \cup A_2 \cup \cdots \cup A_n$ does not appear on the RHS.

$$y \notin A_1 \cup A_2 \cup \cdots \cup A_n \implies y \notin A_i, \forall i = 1, \dots, n \implies y \notin \cap_{i \in S} A_i, \forall S \subseteq \{1, \dots, n\}$$

2. Every element that is contained in $A_1 \cup A_2 \cup \cdots \cup A_n$ appears exactly once on the RHS.

- Suppose $x \in A_1 \cup A_2 \cup \cdots \cup A_n$
- Define $I_x = \{i \in \{1, 2, \dots, n\} : x \in A_i\}$

$I_x = \{1,3,4\}$



What happens if $S \not\subseteq I_x$?

What happens if $S \subseteq I_x$?

Proof of the Inclusion-Exclusion Formula

Theorem 5. *Let $A_1, \ldots, A_n$ be arbitrary subsets of the same set Ω. Then,*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1,\ldots,n\} : |S| = k} \left| \bigcap_{i \in S} A_i \right|.$$

Proof:

1. Every element that is not contained in $A_1 \cup A_2 \cup \cdots \cup A_n$ does not appear on the RHS.

$$y \notin A_1 \cup A_2 \cup \cdots \cup A_n \implies y \notin A_i, \forall i = 1, \ldots, n \implies y \notin \cap_{i \in S} A_i, \forall S \subseteq \{1, \ldots, n\}$$

2. Every element that is contained in $A_1 \cup A_2 \cup \cdots \cup A_n$ appears exactly once on the RHS.

- Suppose $x \in A_1 \cup A_2 \cup \cdots \cup A_n$
- Define $I_x = \{i \in \{1, 2, \ldots, n\} : x \in A_i\}$
- If $S \subseteq \{1, \ldots, n\}$ contains any $j \notin I_x$, then $x \notin \cap_{i \in S} A_i$ since $x \notin A_j$
- If $S \subseteq I_x$ and $|S| \geq 1$, then $x \in \cap_{i \in S} A_i$ since $x \in A_i$ for every $i \in S$.
- Hence, # times x appears on RHS is

Lemma 1. *For all $n \in \mathbb{N}$, $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.*

which we proved earlier

$$\sum_{k=1}^{|I_x|} (-1)^{k-1} \sum_{S \subseteq I_x : |S| = k} 1 = \sum_{k=1}^{|I_x|} (-1)^{k-1} \binom{|I_x|}{k} = 1$$

$\square$

Euler's Totient Function

Recall Q3 from Homework 4: For $n \in \mathbb{Z}^+$, how many positive integers $m \leq n$ are relatively prime to n? $(\gcd(n,m) = 1)$. Let $\varphi(n)$ denote this number.

We wish to solve this problem using counting!

Let $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ be its prime factorization. $(p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r$ are positive integers.)

For $i = 1, \ldots, r$, define $A_i := \{m \in \mathbb{Z}^+ | m \leq n \text{ and } p_i \text{ divides } m\}$

Then, $\varphi(n) = n - |A_1 \cup \cdots \cup A_r| = n \left[1 - \sum_{k=1}^{r} (-1)^{k-1} \sum_{S \subseteq \{1,\ldots,r\} : |S| = k} \frac{1}{\prod_{i \in S} p_i} \right]$

By inclusion-exclusion

$$|A_i| = \frac{n}{p_i}$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j} \text{ for } i \neq j$$

For $S \subseteq \{1, 2, \ldots, r\}$, $\left| \bigcap_{i \in S} A_i \right| = \frac{n}{\prod_{i \in S} p_i}$