

CSCI 104 Counting

CSCI 104 Teaching Team

Tips

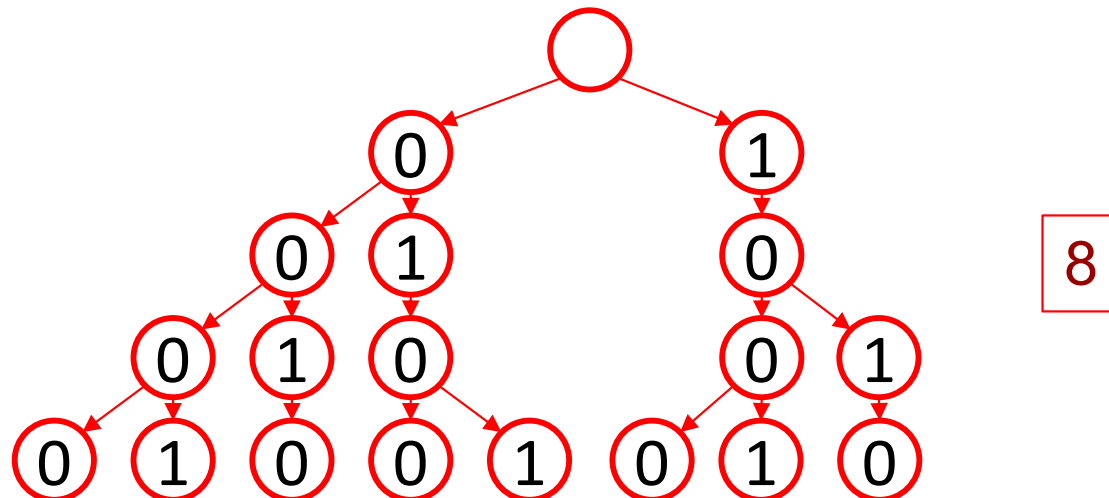
- Know some of the basic rules and formulas we provide
- But don't just look for a formula as your first step. STOP! Think through the problem, your intuitions, and what rules/formulas **may** seem useful
- Write some examples and then determine your approach
- Often you may need to break the problem up and apply the rules/formulas to the parts

Brute-Force Counting

- How many ways are there to roll a total of 6 with two standard dice?
- How many bit strings of length 4 do not have two consecutive 1s?

Brute-Force Counting

- How many ways are there to roll a total of 6 with two standard dice?
 - 1-5, 2-4, 3-3, 4-2, 5-1 = 5
- How many bit strings of length 4 do not have two consecutive 1s?



FUNDAMENTAL COUNTING RULES

Key Ideas

- Fundamental Counting Rules
 - **Product**, **Division**, **Subtraction**, and **Addition** rules
 - These can be used to fully solve "simple" problems or as a technique to decompose a problem into or solve subproblems
- Permutations and Combinations
 - Counting subsets when **order** DOES or DOES NOT matter
 - Counting techniques differ when elements/options CAN or CANNOT be **replaced** (chosen again)
- Distributing elements to "boxes/bins"
 - Different techniques based on distinguishability and indistinguishability of both elements and the "boxes/bins"

PERMUTATIONS AND COMBINATIONS

Product Rule Motivation

- A company has 3 new employees: Aaron, Simone, and Jenna. There are 12 offices. How many different ways are there to assign offices?

_____ _____ _____
A S J

The Product Rule

Fundamental Rule

- A company has 3 new employees: Aaron, Simone, and Jenna. There are 12 offices. How many different ways are there to assign offices?
 - $12 \cdot 11 \cdot 10 = 1320$
- The **Product Rule** states that if a procedure can be broken up into a **sequence of k tasks**, and there are n_i ways to do the i-th task, then there are a total of

$\prod_{i=1}^k n_i$ ways to do the procedure,

or $|A \times B| = |A| \cdot |B|$

$\{ABC\} \times \{1,2\}$	1	2
A	A1	A2
B	B1	B2
C	C1	C2

Replacement Or Non-Replacement

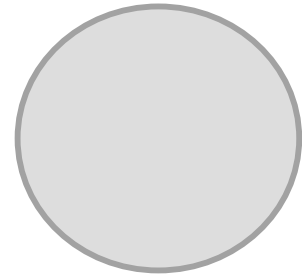
- Ex. 1: How many ways are there to arrange 10 people in a line?
- Ex. 2: If a license plate must have 3 letters followed by 3 digits, how many unique license plates are there?
- A helpful discriminator in solving these kinds of problems is to determine if the same option can be reused (aka "replaced/used multiple times") in subsequence selections (tasks)
 - Without replacement: Answer often involves _____
 - How many ways to arrange {A,B,C,D}? _____
 - With replacement: Answer often involves _____
 - How many unique strings exist use only characters {A,B,C,D}? _____

Replacement Or Non-Replacement

- Ex. 1: How many ways are there to arrange 10 people in a line?
 - $10! = 3628800$
- Ex. 2: If a license plate must have 3 letters followed by 3 digits, how many unique license plates are there?
 - $26^3 \cdot 10^3 = 17576000$
- A helpful discriminator in solving these kinds of problems is to determine if the same option can be reused (aka "replaced/used multiple times") in subsequence selections (tasks)
 - Without replacement: Answer often involves **factorials**
 - How many ways to arrange {A,B,C,D}? ___ ___ ___ ___
 - $4!$
 - With replacement: Answer often involves **exponents**
 - How many length 3 strings exist use only characters {A,B,C,D}? ___ ___ ___
 - 4^3

Division Rule Motivation

- How many different ways are there to seat 4 people around a circular table, where two seatings are considered identical if each person has the same left neighbor in both seatings, and the same right neighbor in both seatings?
- How many ways are there to arrange 10 people in a line, when it is unspecified which end is the front?



The Division Rule

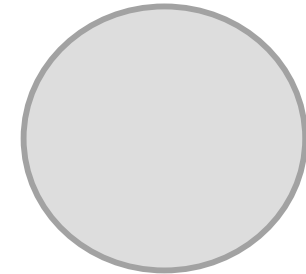
Fundamental Rule

- How many different ways are there to seat 4 people around a circular table, where two seatings are considered identical if each person has the same left neighbor in both settings, and the same right neighbor in both settings?

$$- \frac{4!}{4} = 6$$

- The **Division Rule** states that there are $\frac{n}{d}$ ways to do a task which can be done in one of n different ways, but for each specific way, it is identical to $d-1$ other ways.
- How many ways are there to arrange 10 people in a line, when it is unspecified which end is the front?

$$- \frac{10!}{2}$$



r Permutations

- How many ways can we select 3 students from a group of 5 to stand in line for groceries?
 - Consider the use of the multiplication and division rule

A	B	C	D	E
A	B	C	E	D
A	B	D	C	E
A	B	D	E	C
A	B	E	C	D
A	B	E	D	C
...				
E	D	C	A	B
E	D	C	B	A

r Permutations

Subsets when order DOES matter

- How many ways can we select **3** students from a group of **5** to stand in line for groceries?

- Consider the use of the multiplication and division rule

- $\frac{5!}{2!}$

- An **r**-permutation is an **ordered** arrangement of **r** elements from a set of **n**, denoted **nPr**,

$$P(n, r), \text{ or } {}_n P_r = \frac{n!}{(n-r)!}$$

- Note: Permuting all **n** items in the set

yields: $({}_n P_n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$

A	B	C	D	E
A	B	C	E	D
A	B	D	C	E
A	B	D	E	C
A	B	E	C	D
A	B	E	D	C
...				
E	D	C	A	B
E	D	C	B	A

Ordered r permutation

$${}_n P_r = \frac{n!}{(n-r)!}$$

Combinations

Subsets when order does NOT matter

- How many ways are there to select **3** representatives from **5** students to go to a club meeting

$$- \frac{5!}{2! \cdot 3!}$$

- An **r**-combination is an unordered arrangement of **r** elements from a set of size **n**, is commonly spoken as "**n** choose **r**" and is denoted **nCr**, **C(n,r)** or

$$- \binom{n}{r} = \frac{nPr}{rPr} = \frac{n!}{r! \cdot (n-r)!}$$

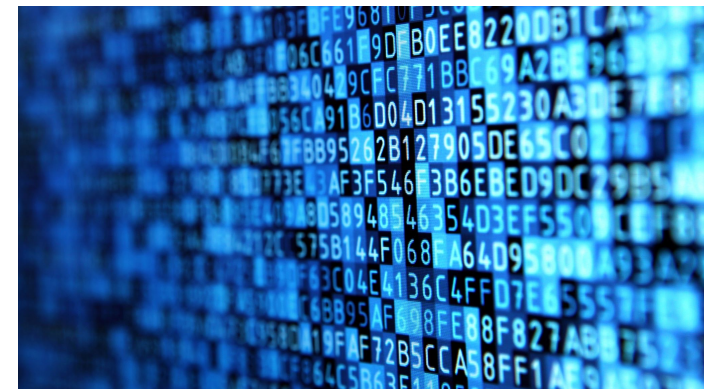
A	B	C	D	E
A	B	C	E	D
A	B	D	C	E
A	B	D	E	C
...				
A	C	B	E	D
A	C	B	D	E
...				
B	A	C	E	D
B	A	C	D	E
...				

r combination

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

Permutation/Combination Examples

- How many permutations of the letters DIJKSTRA contain the substring IJK?
 - _____
- How many different 5-card Poker hands can be dealt from a standard deck of 52 cards?
 - $\binom{52}{5} = 2,598,960$
- How many different 47-card hands can be dealt?
 - $\binom{52}{47} = 2,598,960$



Properties of Combinations

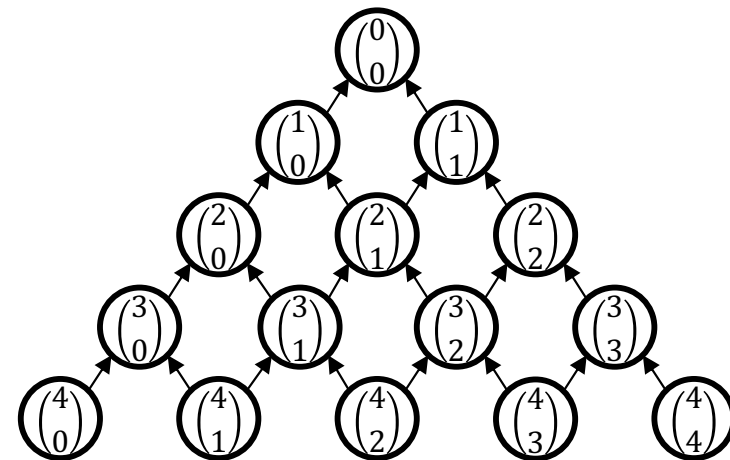
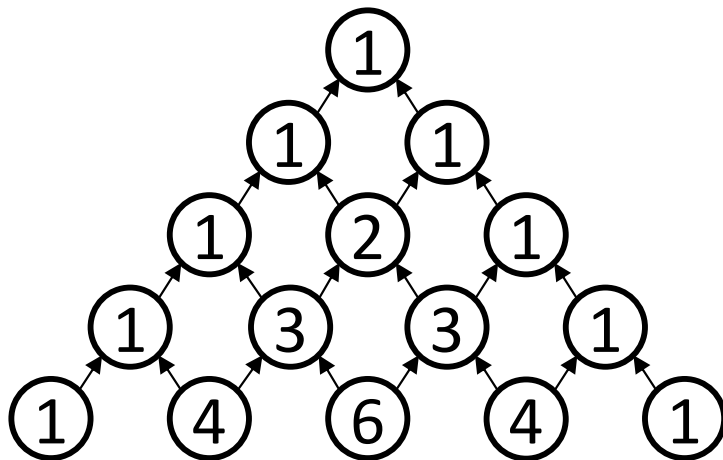
- Fact 1: $\binom{n}{r} = \binom{n}{n-r}$
 - $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ and $\binom{n}{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!(r)!}$
- Fact 2: $\sum_{k=0}^n \binom{n}{k} = 2^n$
 - This sum enumerates all possible subsets and yields the power set (of which there are 2^n total subsets)
 - Ex: {A, B, C}



Binomial Theorem & Pascal's Identity

- Expand $(x + y)^3 = (x + y)(x + y)(x + y)$
 - $x^3 + 3x^2y + 3xy^2 + y^3$
 - $\binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3$
- The Binomial Theorem is as follows:
 - $(x + y)^n = \sum_{j=0}^n \binom{n}{j} x^{n-j} y^j$
- What is the coefficient of $x^{12}y^{13}$ in the expansion of $(x + y)^{25}$?
 - $\binom{25}{13} = \binom{25}{12}$

Pascal's Triangle and Identity



Pascal's Identity:

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

Proof of Pascal's Identity

- Prove: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
- Let T be a set with $n+1$ elements. Let a be an element in T , and let $S = T - \{a\}$
- There are $\binom{n+1}{k}$ subsets of T with k elements: some include a , the rest don't.
- There are $\binom{n}{k}$ ways to choose k elements from S (subsets of T without a)
- There are $\binom{n}{k-1}$ ways to choose $k-1$ elements from S
 - Add a to each of these, corresponding to subsets of T with a .
- Therefore, $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Another Combination Property

- Prove: $\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2$
- $\sum_{k=0}^n \binom{n}{k}^2 = \sum_{k=0}^n \binom{n}{k} \cdot \binom{n}{n-k}$
- Suppose we have a class of $2n$ people, and we need to choose n people to get an A.
- We can divide the room up into the men (there are n of them) and the women (also n).
- The k th term in the summation is the number of ways to assign A's, so that exactly k men get an A and $n-k$ women get an A.
- If we add up over all k , this will give us the total number of ways to assign A's.

DECOMPOSING TO AND COMBINING ANSWERS TO SUBPROBLEMS

Addition Rule Motivation

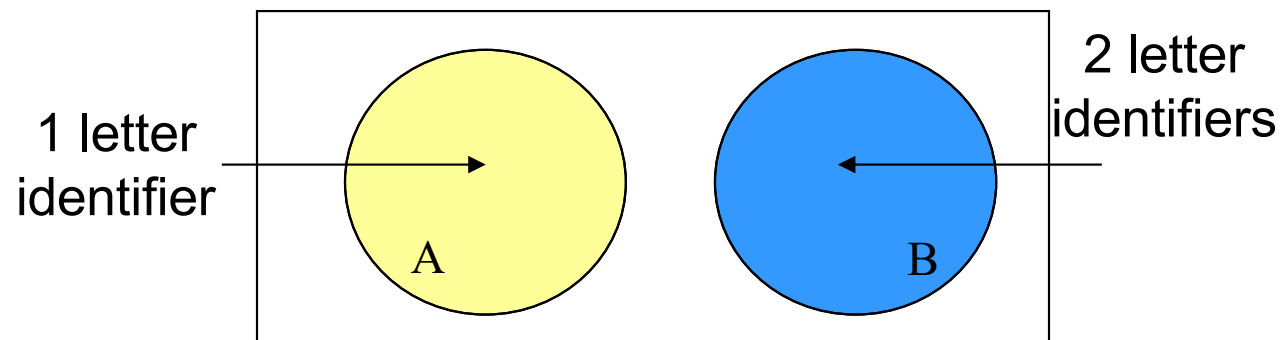
- In a version of BASIC, variables can be **one** or **two** alphanumeric characters (lower-case and upper-case is not distinguished). The first character must be a letter. How many different variable names are there?

-

Addition Rule

Fundamental Rule

- In a version of BASIC, variables can be one or two alphanumeric characters (lower-case and upper-case is not distinguished). The first character must be a letter. How many different variable names are there?
 - $26 + 26 * 36 = 962$
- The **Addition Rule** states that if a task can be done in either one of **n1** ways or one of **n2** ways, and there is **NO** overlap between these groups, then the number of ways to do the task is $n1 + n2$, or $|A \cup B| = |A| + |B|$



Subtraction Rule Motivation

- How many bit strings of length 8 either start with a 1 or end with two 0s?

- The company Grinding Gear Games has 350 job applicants. 220 are CSCI majors, 147 are BUAD majors, and 51 are double majors in both. How many applicants are neither?

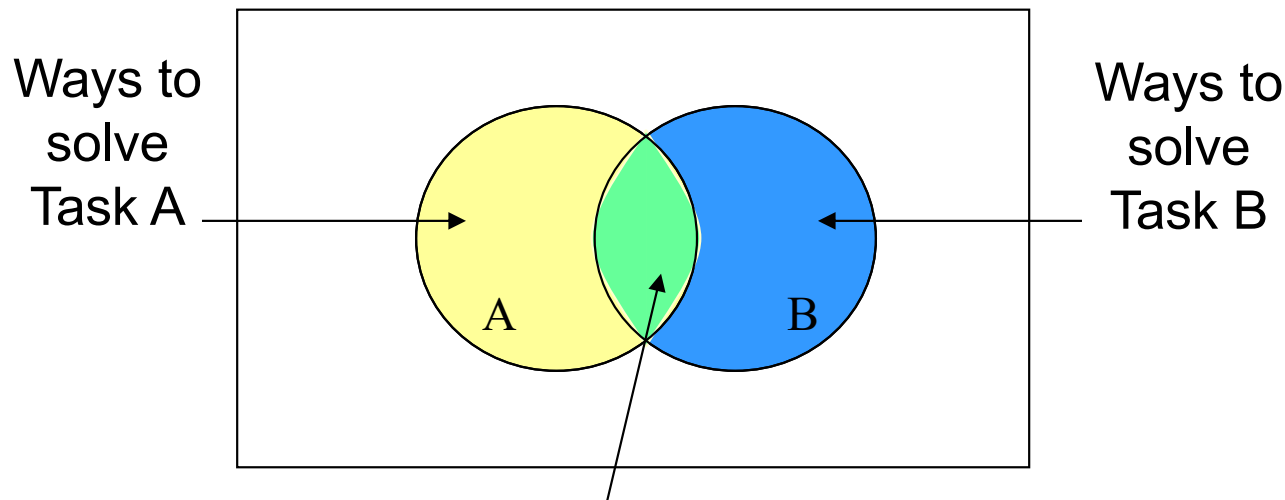
Subtraction Rule

Fundamental Rule

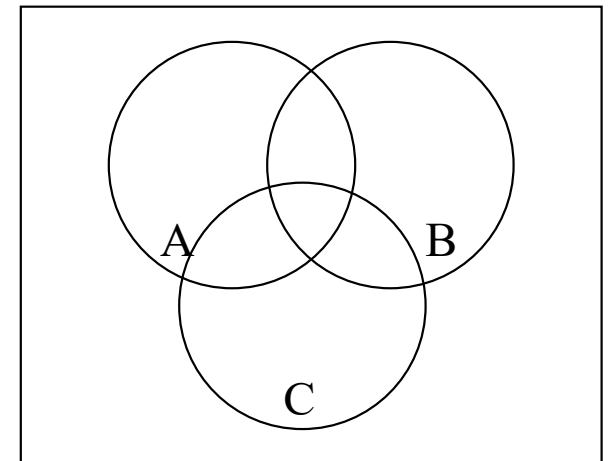
- How many bit strings of length 8 either start with a 1 or end with two 0s?
 - $2^7 + 2^6 - 2^5 = 160$
- The company Grinding Gear Games has 350 job applicants. 220 are CSCI majors, 147 are BUAD majors, and 51 are double majors in both. How many applicants are neither?
 - $350 - (220 + 147 - 51) = 34$
- The **Subtraction Rule** states that if a task can be done in either one of n_1 ways or one of n_2 ways, and there is an overlap between these two methods of n_3 common ways, then the number of ways to do the task is $n_1 + n_2 - n_3$, or $|A \cup B| = |A| + |B| - |A \cap B|$

The Subtraction Rule

- Also, known as the Principle of Inclusion / Exclusion (aka PIE)

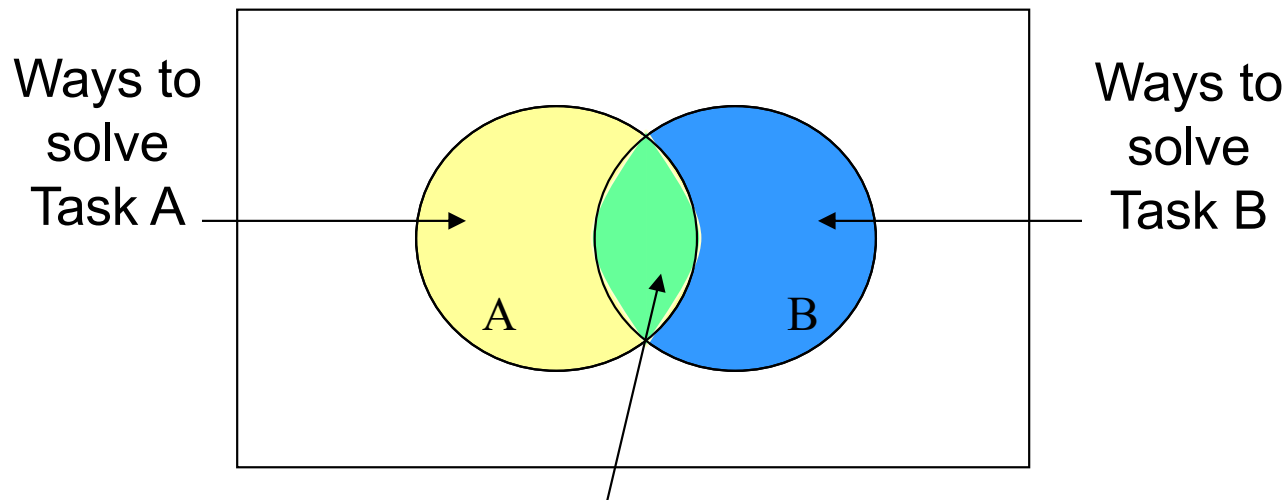


How would you count the ways to solve a task consisting of 3 potentially overlapping subtasks?

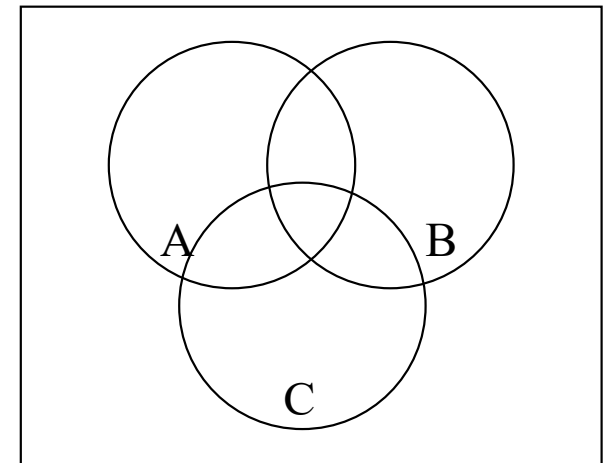


The Subtraction Rule

- Also, known as the Principle of Inclusion / Exclusion (aka PIE)



How would you count the ways to solve a task consisting of 3 potentially overlapping subtasks?



$$|A| + |B| + |C| - |AB| - |AC| - |BC| + |ABC|$$

Fundamental Rule Practice (1)

- How many 7-digit phone numbers are there, if they cannot start with a 0, a 1, or the sequence 911?
- How many odd 4-digit numbers are there with no leading zeroes, and no repeated digits?

Fundamental Rule Practice (1)

- How many 7-digit phone numbers are there, if they cannot start with a 0, a 1, or the sequence 911?
 - $8 \cdot 10^6 - 10^4 = 7990000$
- How many odd 4-digit numbers are there with no leading zeroes, and no repeated digits?
 - $5 \cdot 8 \cdot 8 \cdot 7 = 2240$

Fundamental Rule Practice (2)

- A computer system requires a password between 6 and 8 alphanumeric characters (lower-case and upper-case is not distinguished). At least one character must be a digit. How many different passwords are there?

Fundamental Rule Practice (2)

- A computer system requires a password between 6 and 8 alphanumeric characters (lower-case and upper-case is not distinguished). At least one character must be a digit. How many different passwords are there?
 - $36^6 - 26^6 + 36^7 - 26^7 + 36^8 - 26^8$
 - Why is it not $10 \cdot 36^5 + 10 \cdot 36^6 + 10 \cdot 36^7$?
 - Why is it not $6 \cdot 10 \cdot 36^5 + 7 \cdot 10 \cdot 36^6 + 8 \cdot 10 \cdot 36^7$?

PERMUTATIONS AND COMBINATIONS WITH OR WITHOUT REPLACEMENT

Motivation for Permutations with Repetition

- A message on a Twitter-like service must consist of exactly r characters. Because it is the internet, people only communicate using capital letters, spaces, and the exclamation mark.
- How many different messages can one post on this service?

Motivation for Permutations with Repetition

Permutations with Repetition

- A message on a Twitter-like service must consist of exactly r characters. Because it is the internet, people only communicate using capital letters, spaces, and the exclamation mark.
- How many different messages can one post on this service?
 - 28^r
- The number of r -permutations of a set of n objects, where repetition is allowed, is n^r .

Motivation for Combinations with Repetition

- How many ways are there to select 5 bills from a cash box containing 1, 2, 5, 10, 20, 50, and 100 dollar bills (7 denominations)?
 - Is it just 7^5 ?

Combinations with Repetition (Stars and Bars)

Combinations with Repetition

- How many ways are there to select 5 bills from a cash box containing 1, 2, 5, 10, 20, 50, and 100 dollar bills (7 denominations)?



- We need to write 7-1=6 bars (cash box dividers) and 5 stars (the bills) in some order (choose the locations for the *s or bars)

$\binom{11}{5} = \binom{11}{6} =$	1	2	3	4	5	6	7	8	9	10	11
	—	—	—	—	—	—	—	—	—	—	—
	*			*			*		*	*	
			*	*	*			*			*

- The number of r-combinations of a set of n objects, where repetition is allowed, is $\binom{n-1+r}{r} = \binom{n-1+r}{n-1}$

Summary of Counting (Subsets) Taxonomy

- Summary based on replacement and ordering

	No Replacement	Replacement
Order matters	${}_n P_k = \frac{n!}{(n-k)!}$ <p>n total options, permute k</p> <p>Special case: Permute all n:</p> ${}_n P_n = \frac{n!}{(n-n)!} = n!$	<p>For replacement:</p> k^n <p>Length n, k options (Base-n combinations)</p>
Order does NOT matter	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ <p>n total options, choose k</p>	$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$ <p>Stars and Bars</p>

MULTISETS, ELEMENTS, BOXES, AND DISTINGUISHABILITY

Distributing Elements over Bins

- We will be filling this in over the next slides
- Distributing n items over k boxes

	Distinguishable Boxes	Indistinguishable Boxes
n Indistinguishable Elements		
n Distinguishable Elements		

Motivation for Multisets

- A multiset is a set which may contain duplicates
 - The number of occurrences of each element is its **multiplicity**
 - E.g. The multiplicity of 'S' in "SUCCESS" is 3
- How many different strings can be made by reordering the letters of SUCCESS?

S U C C E S S

Multisets (Approach 1)

- How many different strings can be made by reordering the letters of SUCCESS?
 - What would the answer be if all the characters were unique ("1234567")?
 - But now realize 1 6 7 are interchangeable since they represent the same letter S and 3 and 4 are interchangeable since they represent the letter C
- The number of permutations of n objects, where n_i is the multiplicity (are indistinguishable objects) of type i, is

$$\frac{n!}{\prod_{i=1}^k n_i!}$$

S	U	C	C	E	S	S
1	2	3	4	5	6	7

Multisets (Approach 2)

Permutations with Duplicates

- Take each "type" and choose which locations will have that type
- For SUCCESS, choose the 3 places for S, 2 places for C, etc.?

$$\begin{aligned} \blacktriangleright \binom{7}{3} \cdot \binom{4}{2} \cdot \binom{2}{1} \cdot \binom{1}{1} &= \frac{7!}{3! \cdot 4!} \cdot \frac{4!}{2! \cdot 2!} \cdot \frac{2!}{1! \cdot 1!} \cdot \frac{1!}{0! \cdot 1!} \\ &= \frac{7!}{3! \cdot 2! \cdot 1! \cdot 1!} \end{aligned}$$

- The number of permutations of n objects, where n_i are indistinguishable objects of type i, is

$$\blacktriangleright \frac{n!}{\prod_{i=1}^k n_i!}$$



Distinguishable Objects over Distinguishable Boxes

- 4 people are playing Poker, wherein each player receives 5 cards from a standard deck of 52 distinct cards. How many ways are there to deal out hands?

$$\rightarrow \binom{52}{5} \cdot \binom{47}{5} \cdot \binom{42}{5} \cdot \binom{37}{5}$$

$$\rightarrow = \frac{52!}{5! \cdot 47!} \cdot \frac{47!}{5! \cdot 42!} \cdot \frac{42!}{5! \cdot 37!} \cdot \frac{37!}{5! \cdot 32!}$$

$$\rightarrow = \frac{52!}{5! \cdot 5! \cdot 5! \cdot 5! \cdot 32!}$$

- The number of ways to distribute n distinguishable objects into k distinguishable boxes so that n_i objects are placed in box i is:

$$\rightarrow \frac{n!}{\prod_{i=1}^k n_i!}$$

Transform the problem to permutations with repetition

2♣	2♠	2♥	2♦	3♣	3♠	3♥	3♦	...
P1	D	P4	D	P2	P1	D	P3	

Bijection between cards and player hands (or D=Deck). How many permutations of the 5 P1s, 5 P2s, ..., 32 D (Deck) exist?

Indistinguishable Objects over Distinguishable Boxes

- There are 8 poker players, and there are 10 one-hundred-dollar chips distributed amongst them. How many ways could the chips be distributed?
- The number of ways to distribute r indistinguishable objects into n distinguishable boxes is



Indistinguishable Objects over Distinguishable Boxes

- There are 8 poker players, and there are 10 one-hundred-dollar chips distributed amongst them. How many ways could the chips be distributed?

*** | | ** | * | | ** | | **

➤ $\binom{17}{10}$

- The number of ways to distribute r indistinguishable objects into n distinguishable boxes is

➤ $\binom{n-1+r}{r}$

Indistinguishable Objects over Nonempty Distinguishable Boxes

- If we want to place r indistinguishable objects into n distinguishable boxes, but every box must **have at least one element**, we can start by placing one object in every box.
- Now we need to place $r-n$ indistinguishable objects into n distinguishable boxes.
 - This is the same problem as the previous one, now!
 - $$\binom{r-n+(n-1)}{r-n} = \binom{r-1}{r-n}$$

Practice

- How many ways can ANAGRAM be rearranged?
- How many ways are there to select 4 pieces of fruit from a bowl containing apples, oranges, and pears?
- How many solutions does the equation $x_1+x_2+x_3=11$ have, where x_1 , x_2 , and x_3 are nonnegative integers?

Practice

- How many ways can ANAGRAM be rearranged?
 - $\frac{7!}{3!}$
- How many ways are there to select 4 pieces of fruit from a bowl containing apples, oranges, and pears?
 - Combinations, with repetition
 - $\binom{6}{4}$
- How many solutions does the equation $x_1+x_2+x_3=11$ have, where x_1 , x_2 , and x_3 are nonnegative integers?
 - Indistinguishable objects into distinguishable boxes
 - $\binom{13}{11}$

Distinguishable Objects over Indistinguishable Boxes

- 4 different roommates are playing a multi-player game, and they're distributed over 3 indistinguishable servers. How many ways are there to distribute them?

A B C | | D |
D | | C B A |

Distinguishable Objects over Indistinguishable Boxes

- 4 different roommates are playing a multi-player game, and they're distributed over 3 indistinguishable servers. How many ways are there to distribute them?
 - Consider breaking this problem into non-overlapping subproblems and use the addition rule. For each case, consider the combinations that can be made.
 - $(4,0,0) = 1$
 - $(3,1,0) = 4$
 - $(2,1,1) = 6$
 - $(2,2,0) = 3$
 - Total = 14
 - There is no closed-form formula for this problem.

Indistinguishable Objects over Indistinguishable Boxes

- The company just worries about server-load, not who plays where.
- How many ways can you distribute 6 faceless players over 4 indistinguishable servers?
 - Again, break into case but now each case does not need to consider the different combinations that can be made since the objects are indistinguishable
 - (6,0,0,0)
 - (5,1,0,0) (4,2,0,0) (3,3,0,0)
 - (4,1,1,0) (3,2,1,0) (2,2,2,0)
 - (3,1,1,1) (2,2,1,1)
- Total = 9
- There is no closed-form formula for this problem.

Summary Of Distributing Elements

- Distributing n items over k boxes

	Distinguishable Boxes	Indistinguishable Boxes
n Indistinguishable Elements	<p>Stars and Bars</p> $= \binom{n + k - 1}{k - 1}$ <p>If at least 1 per box:</p> $= \binom{n - 1}{k - 1}$	<ul style="list-style-type: none"> Break into cases: $x_1 + x_2 + \dots + x_k = n$ (i.e. way to sum k non-neg integers to equal n) remembering order of x_i doesn't matter No closed-form formula
n Distinguishable Elements	$\frac{n!}{\prod_i^k n_i!}$ <p>n_i elements in a boxes for $i = 1 \dots k$</p>	<ul style="list-style-type: none"> Break into cases: $x_1 + x_2 + \dots + x_k = n$ For each case, determine number of orderings (ways to choose x_i) but ordering of $x_1 \dots x_k$ doesn't matter No closed-form formula

NOT COVERED

A card trick

- Phillip shuffles a standard deck of 52 cards, and deals himself 5.
- Phillip looks at his 5 cards, then reveals 4 of them to Aaron, one at a time.
- Aaron then correctly determines the 5th card in Phillip's hand.
- There's no information being relayed to Aaron other than the cards Phillip reveals, and the order in which they are revealed.
- There's no magic: you can replicate this feat with a friend who also knows how it works. It comes down to a pigeonhole principle counting argument!

The first card

- There are 4 suits (\clubsuit , \diamondsuit , \heartsuit , \spadesuit) and 5 cards.
- By the pigeonhole principle, Phillip must have 2 cards of the same suit.
- Phillip will choose one of them to be the first card flipped over, and the other to be the card he keeps in his hand.
- There are 13 values (2-10, J=11, Q=12, K=13, A=14).
- If the value of the smaller card is within 6 of the larger card, Phillip will display the smaller card first. Otherwise, the larger card.
- After the first card flip, Aaron has narrowed the possible cards down to 6.
- If $J\diamondsuit$ is displayed, it is either $Q\diamondsuit$, $K\diamondsuit$, $A\diamondsuit$, $2\diamondsuit$, $3\diamondsuit$, or $4\diamondsuit$.
- If it were $5\diamondsuit$, Phillip would display that instead, which leaves $6\diamondsuit$, $7\diamondsuit$, $8\diamondsuit$, $9\diamondsuit$, $10\diamondsuit$, $J\diamondsuit$ as the possibilities.

The remaining cards

- By convention, if two cards have the same value, the tie-breaker is the suit: ♣ < ♦ < ♥ < ♠
- Phillip will choose the order of the remaining 3 cards based on which of the 6 options he wants Aaron to choose.
 - Smallest, then middle, then largest = 1st of the 6 options.
 - Smallest, then largest, then middle = 2nd option.
 - Middle, then smallest, then largest = 3rd option.
 - Middle, then largest, then smallest = 4th option.
 - Largest, then smallest, then middle = 5th option.
 - Largest, then middle, then smallest = 6th option.

XKCD #936

Password Strength

<p style="font-size: small;">(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p style="font-size: x-small;">(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.