

07 Counting

CS201 Discrete Mathematics

Instructor: Shan Chen

Counting

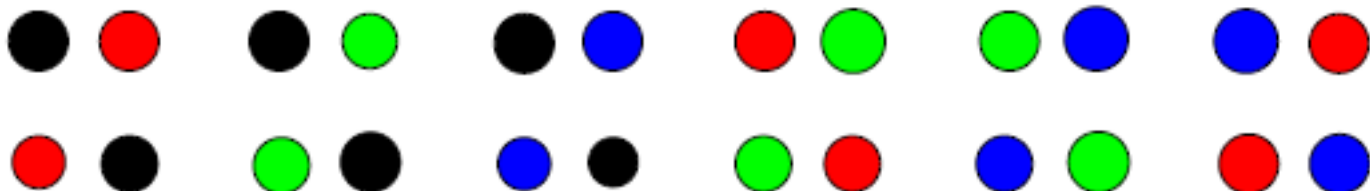
- Assume we have a set of objects with certain properties.
Counting is used to determine **the number of these objects**.

- Example: ● ● ● ●

- How many different ways to choose 2 balls out of 4 colored balls?



- What about when **order counts**?



Counting

- Assume we have a set of objects with certain properties.
Counting is used to determine the number of these objects.
- More examples:
 - the number of steps in a computer program
 - the number of passwords between 6 – 10 characters
 - the number of telephone numbers with 8 digits
- Counting may be very hard, not trivial.
 - simplify the solution by decomposing the problem

The Counting Basics

The Sum Rule

- A count decomposes into a **set** of **independent** counts (elements of counts are alternatives)
- Example: You need to travel from city A to B . You may either fly, take a train, or a bus. There are 12 different flights, 5 different trains and 10 buses.
 - How many options do you have to travel from A to B ?
 $12 + 5 + 10 = 27$
- **The sum rule:** If a count of elements can be broken down into a **set of independent counts** where the first count yields n_1 elements, the second n_2 elements, and k -th n_k elements, then the total number of elements is $n = n_1 + n_2 + \cdots + n_k$.

The Product Rule

- A count decomposes into a **sequence** of **dependent** counts (each element in the first count is associated with **all elements** of the second count).
- Example: In an auditorium, the seats are labeled by **a letter** and **numbers** in between 1 to 50 (e.g., A23).
 - What is the total number of seats?
 $26 \cdot 50 = 1300$
- **The product rule:** If a count of elements can be broken down into a **sequence of dependent counts** where the first count yields n_1 elements, the second n_2 elements, and k -th n_k elements, then the total number of elements is $n = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

Other Rules

- **The subtraction rule:** If a task can be done in either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.
 - E.g., $|A \cup B| = |A| + |B| - |A \cap B|$
- **The division rule:** If a task can be done using a procedure that can be carried out in n “fine-grained” ways, and for every way w , exactly d of the n “fine-grained” ways correspond to way w , then there are n/d ways to do it.
 - E.g., how many kilobytes in one megabyte? $10^6 / 10^3 = 10^3$

More Complex Counting

- Typically, a counting problem requires a combination of more than one rule.
- Example: Each password is 6 to 8 characters long, where each character is a lowercase letter or a digit. Each password must contain at least one digit.
 - How many possible passwords are there?

$$P = P_6 + P_7 + P_8$$

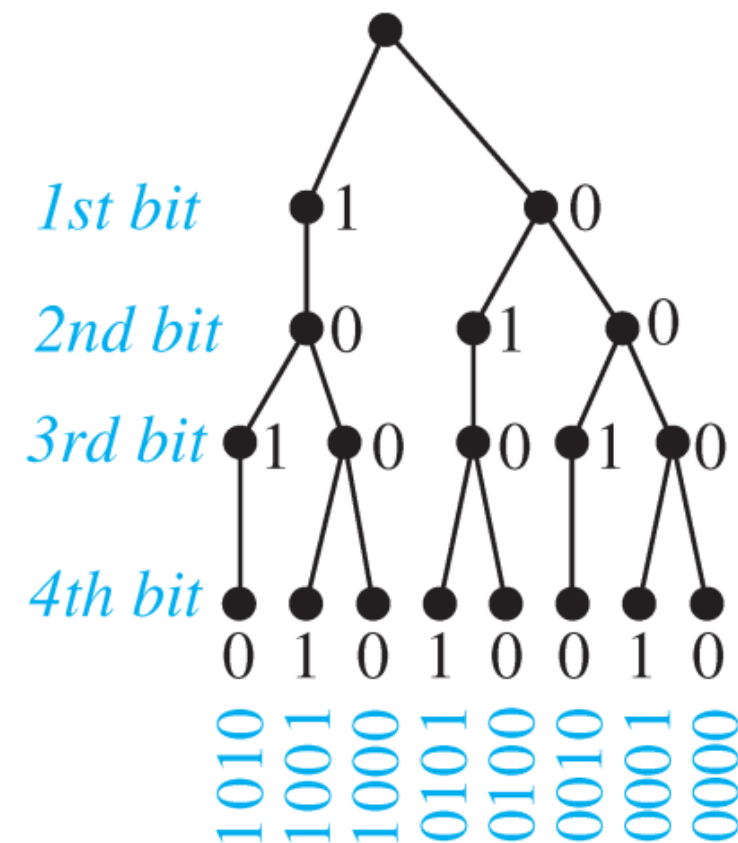
$$P_6 = 36^6 - 26^6$$

$$P_7 = 36^7 - 26^7$$

$$P_8 = 36^8 - 26^8$$

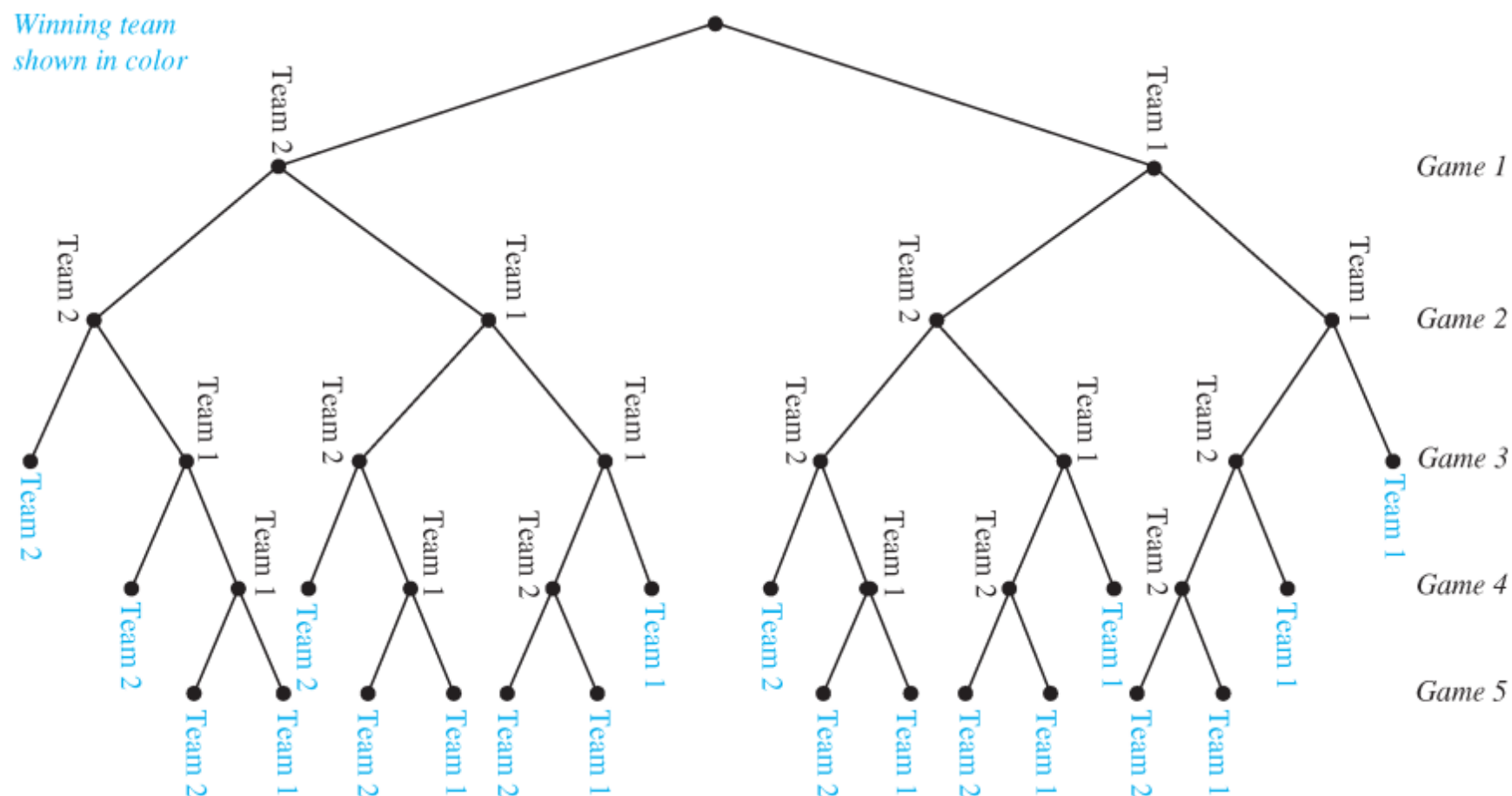
Tree Diagrams

- A **tree** is a structure that consists of a **root**, **branches** and **leaves**.
 - can represent a counting problem and record the choices we made for alternatives, with **the count appears on the leaves**
- Example: What is the number of bit strings of length 4 that **do not have two consecutive 1s**?



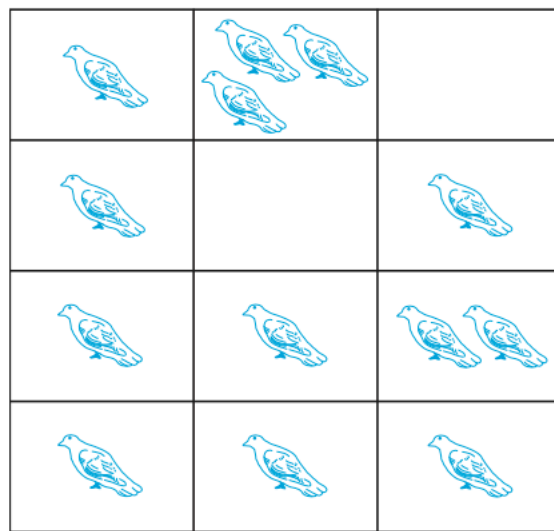
Tree Diagrams

- A **tree** is a structure that consists of a **root**, **branches** and **leaves**.
 - can represent a counting problem and record the choices we made for alternatives, with **the count appears on the leaves**
- Example: The first team that **wins 3 out of 5 games** wins the playoff. In how many different ways can the playoff occur?

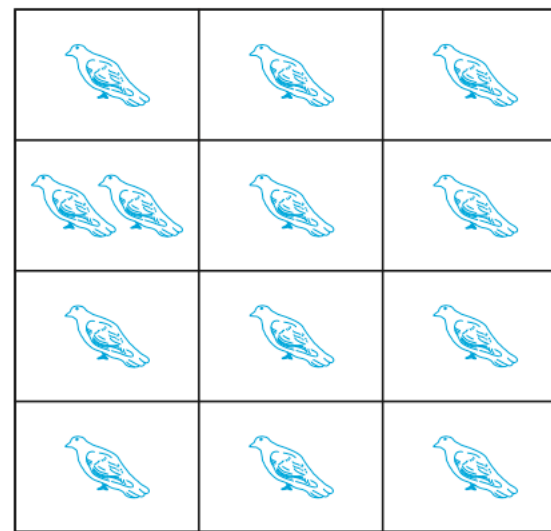


The Pigeonhole Principle

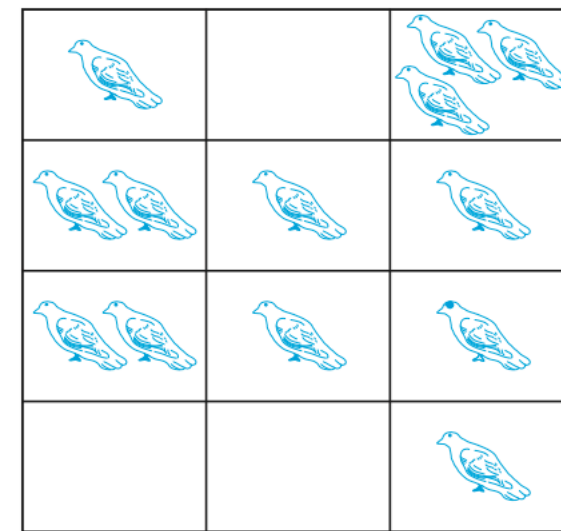
- If a flock of **13 pigeons** flies into a set of **12 pigeonholes** to roost, then **at least one** pigeonhole must have **at least two** pigeons in it.



(a)



(b)



(c)

- **The pigeonhole principle:** If k is a positive integer and **$k + 1$ or more objects** are placed into **k boxes**, then there is **at least one** box containing **two or more** of the objects.
 - proof by contraposition

The Generalized Pigeonhole Principle

- **The generalized pigeonhole principle:** If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.
 - proof by contraposition
- Example:
 - We have 163 students registered CS201. At least how many of you were born in the same month?
 $\lceil 163/12 \rceil = 14$
 - Now we have 156 students left. What about now?
 $\lceil 156/12 \rceil = 13$

Permutations and Combinations

- Many counting problems can be solved by finding the number of ways to arrange or select some distinct elements from a set.
- A **permutation** of a set of distinct objects is an **ordered arrangement** of these objects.
 - E.g., in how many ways can we select three students from a group of five students to stand in line for a picture?
- A **combination** of a set of distinct objects is an **unordered selection** of these objects.
 - E.g., how many different committees of three students can be formed from a group of four students?

r -Permutations

- An ordered arrangement of r distinct elements from a set is called a r -permutation.
 - an n -permutation of a set of size n is simply called a permutation
- Example: what are the 3-permutations of $\{1, 2, 3, 4\}$?
 - $L = \{123, 124, 132, 134, 142, 143, 213, 214, 231, 234, 241, 243, 312, 314, 321, 324, 341, 342, 412, 413, 421, 423, 431, 432\}$.
 - This type of “dictionary” ordering (where we treat numbers as letters) is called a **lexicographic ordering** and is used quite often.

r -Permutations

- **Theorem:** Let n, r be integers and $0 \leq r \leq n$, then there are

$$P(n, r) = n(n - 1)(n - 2) \cdots (n - r + 1)$$

r -permutations of a set with n distinct elements.

** Note that $P(n, 0) = 1$, i.e., there is one way to order 0 element.*

- Proof:

- There are n choices for the **first** number.
For each way of choosing the first number, there are $n - 1$ choices for the **second** number.
For each way of choosing the first **two** numbers, there are $n - 2$ choices for the **third** number.
...
For each way of choosing the first $r - 1$ numbers, there are $n - r + 1$ choices for the r -th number.
- Therefore, by the product rule, there are $n(n - 1)(n - 2) \cdots (n - r + 1)$ r -permutations.

r -Combinations

- An **unordered selection** of r **distinct elements** from a set is called a **r -combination**.
- Example: what are the 3-combinations of $\{1, 2, 3, 4\}$?
 - $L = \{123, 124, 134, 234\}$.
- **Theorem:** Let n, r be integers and $0 \leq r \leq n$, then there are $C(n, r) = P(n, r) / r!$ r -combinations of a set with n distinct elements.
 - * Note that $C(n, 0) = 1$, i.e., there is one way to choose 0 element.
 - Proof: Because the order of elements in a combination does not matter and there are $P(r, r)$ different ways to order r elements in an r -combination, each of the $C(n, r)$ r -combinations of a set with n elements corresponds to exactly $P(r, r)$ r -permutations. Hence, by the division rule, $C(n, r) = P(n, r) / P(r, r) = P(n, r) / r!$.

Exercise (5 mins)

- Answer the following questions using the product rule:
 - How many **different** bit strings of length 7 are there?
 - How many **different** functions from a set with m elements to a set with n elements?
 - How many **one-to-one** functions from a set with m elements to a set with n elements ($m < n$)?
 - How many **onto** functions from a set with m elements to a set with n elements ($m > n$)?

The Birthday Problem

- **The birthday paradox:** Suppose that 23 students are in a room. What is the probability that **at least two of them share a birthday**?
 - It's greater than $1/2$!
- Assume a year has 365 days and there are no twins in the room.
 - **sample space:** $|S| = 365^n$ - all cases occur **equally likely**
- A_n – “there are n students in a room and **at least two** of them share a birthday” B_n – “there are n students in a room and **none** of them share a birthday” $\#E$ – number of cases favorable to E
 - $\#A_n + \#B_n = |S| = 365^n$
 - $\#B_n = C(365, n) = 365 \times 364 \times \dots \times (365 - (n - 1))$
 - $\Pr[A_n] = \#A_n / |S| = 1 - \#B_n / |S|$ * *classical probability*

The Birthday Problem

- Probabilities of A_n and B_n :

n	A_n	B_n	n	A_n	B_n
1	0.00000000	1.00000000	16	0.28360400	0.71639599
2	0.00273972	0.99726027	17	0.31500766	0.68499233
3	0.00820416	0.99179583	18	0.34691141	0.65308858
4	0.01635591	0.98364408	19	0.37911852	0.62088147
5	0.02713557	0.97286442	20	0.41143838	0.58856161
6	0.04046248	0.95953751	21	0.44368833	0.55631166
7	0.05623570	0.94376429	22	0.47569530	0.52430469
8	0.07433529	0.92566470	23	0.50729723	0.49270276
9	0.09462383	0.90537616	24	0.53834425	0.46165574
10	0.11694817	0.88305182	25	0.56869970	0.43130029
11	0.14114137	0.85885862	26	0.59824082	0.40175917
12	0.16702478	0.83297521	27	0.62685928	0.37314071
13	0.19441027	0.80558972	28	0.65446147	0.34553852
14	0.22310251	0.77689748	29	0.68096853	0.31903146
15	0.25290131	0.74709868	30	0.70631624	0.29368375

The Birthday Attack

- In cryptography, the **birthday attack** is an attack that uses the probabilistic model shown in the birthday problem to reduce the complexity of **finding a collision for a hash function**.
 - assume a hash function has **independent random outputs**
- Recall the birthday problem: A_n – “there are n students in a room and **at least two** of them share a birthday” B_n – “there are n students in a room and **none** of them share a birthday”

$$\begin{aligned}\Pr[B_n] &= \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdots \left(1 - \frac{n-1}{365}\right) \\ &= \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right).\end{aligned}$$

$$\Pr[A_n] = 1 - \Pr[B_n] = 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right) \quad p(n; H) := 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{H}\right)$$

The Birthday Attack

- In cryptography, the **birthday attack** is an attack that uses the probabilistic model shown in the birthday problem to reduce the complexity of **finding a collision for a hash function**.
- What is the **smallest** number of values that we have to choose, such that the probability of finding a hash collision is **at least p** ?
 - Let H be the number of possible hash outputs.
 - The **collision probability** when choosing n hash values is

$$p(n; H) := 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{H}\right)$$

Since $e^x = 1 + x + \frac{x^2}{2!} + \dots$, for $|x| \ll 1$, $e^x \approx 1 + x$

Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$. $p(n; H) \approx 1 - e^{-n(n-1)/2H} \approx 1 - e^{-n^2/2H}$

- By **inverting** the above expression, we have the **smallest** number is:

$$n(p; H) \approx \sqrt{2H \ln \frac{1}{1-p}}.$$

Binomial Coefficients and Identities

Binomial Coefficients

- **Theorem:** For integers n and k with $0 \leq k \leq n$, the number of k -element subsets of an n -element set is

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

This is the number of k -combinations of a set with n elements.

- Properties:

- $\binom{n}{0} = \binom{n}{n} = 1$ * only one subset of size 0 and one of size n
- $\binom{n}{k} = \binom{n}{n-k}$ * obvious by definition
- $\sum_{k=0}^n \binom{n}{k} = 2^n$ * the number of subsets of an n -element set

Binomial Coefficients

- Each row starts with a 1

- $\binom{n}{0} = 1$

- Each row ends with a 1

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

- Second half of each row is the **reverse** of the first half.

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

- Sum on the n -th row is 2^n

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

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Pascal's Triangle

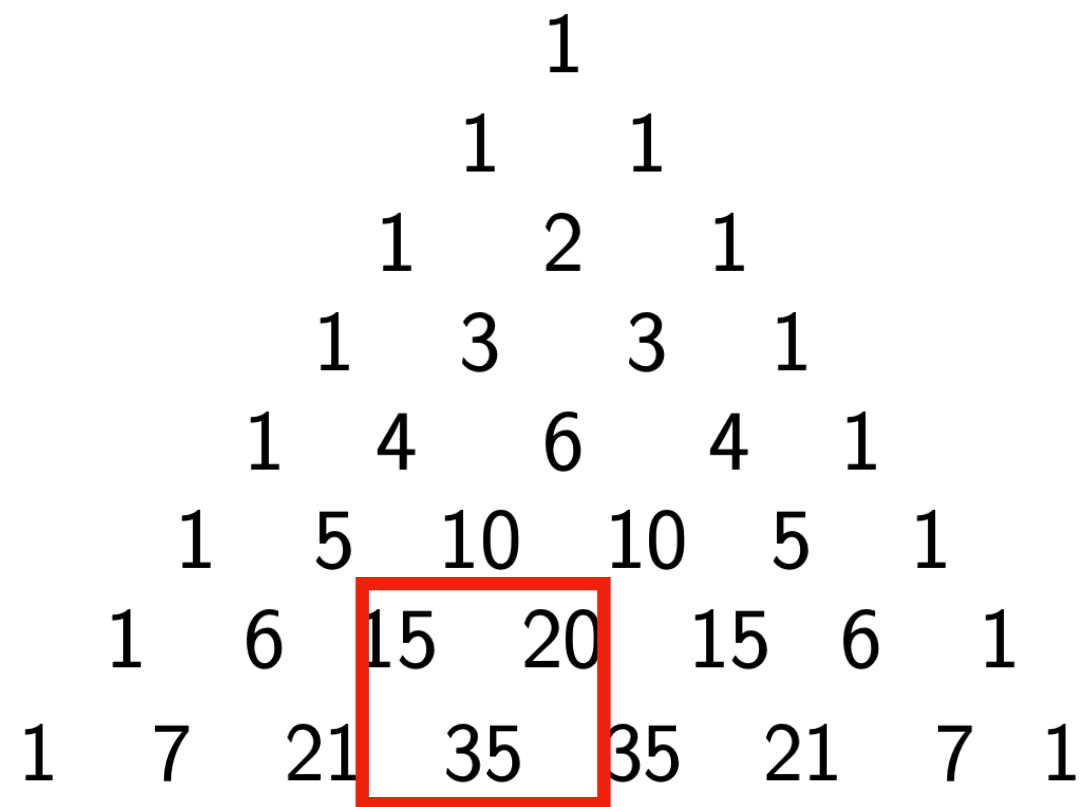
- Take the table and shift each row slightly such that middle element is in the center

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

							1					
						1		1				
				1		2		1				
			1	3		3		1				
		1	4		6		4		1			
	1	5	10		10		5		1			
1	6	15	20		15		6		1			

Pascal's Identity

- What is the next row?
- What can you observe here?
 - each (non-1) entry in Pascal's Triangle is the sum of the two entries directly above it (to left and to right)
- **Pascal's identity:**
 - $$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$
 - A purely algebraic proof (manipulating formulas) is possible. We will use a combinatorial proof.



A Combinatorial Proof

- **Pascal's identity:** $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
 - $\binom{n}{k}$ is the number of k -subsets of an n -element set
 - $\binom{n-1}{k-1}$ is the number of $(k-1)$ -subsets of an $(n-1)$ -element set
 - $\binom{n-1}{k}$ is the number of k -subsets of an $(n-1)$ -element set
- Proof by the **sum rule**:
 - Let S_1 be the set of all k -element subsets and x_n be the n -th element. To apply the sum rule, partition S_1 into S_2 and S_3 :
Let S_2 be the set of k -element subsets that **contain** x_n .
Let S_3 be the set of k -element subsets that **don't contain** x_n .

Blaise Pascal

- French Mathematician (1623~1662)
- A Founder of Probability Theory
- Inventor of one of the first mechanical calculating machines
- Pascal programming language named in honor of him



The Binomial Theorem

- **The binomial theorem:** Let x and y be variables, and let n be a nonnegative integer. Then $\sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = (x + y)^n$.

** the proof is easy: how many ways one can derive the term $x^{n-k} y^k$?*

- Let $x = y = 1$. We have $\sum_{k=0}^n \binom{n}{k} = 2^n$.
- Let $x = 1, y = -1$. We have $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.
- Let $y = 1$. We have $\sum_{k=0}^n \binom{n}{k} x^k = (1 + x)^n$.

- Why the name “binomial”?

- because these numbers occur as coefficients in the expansion of powers of binomial expressions such as $(x + y)^n$.

Trinomial Coefficients

- **Q:** What is the coefficient of $x^{k_1} y^{k_2} z^{k_3}$ in $(x + y + z)^n$?
- **A:** If we have k_1 red labels, k_2 blue labels, and $k_3 = n - k_1 - k_2$ purple labels, then in how many different ways can we apply these labels to n objects?
 - How many ways to choose the k_1 red items? How many ways to choose the k_2 blue items from the remaining $n - k_1$ items? Finally, the remaining $k_3 = n - k_1 - k_2$ items get labelled purple.

$$\binom{n}{k_1} \binom{n - k_1}{k_2} = \frac{n!}{k_1!(n - k_1)!} \frac{(n - k_1)!}{(k_2)!(n - k_1 - k_2)!} = \frac{n!}{k_1!k_2!k_3!}$$

- When $k_1 + k_2 + k_3 = n$, we call $n!/(k_1! k_2! k_3!)$ a trinomial coefficient and denote it as $\binom{n}{k_1 k_2 k_3}$.

Inclusion-Exclusion

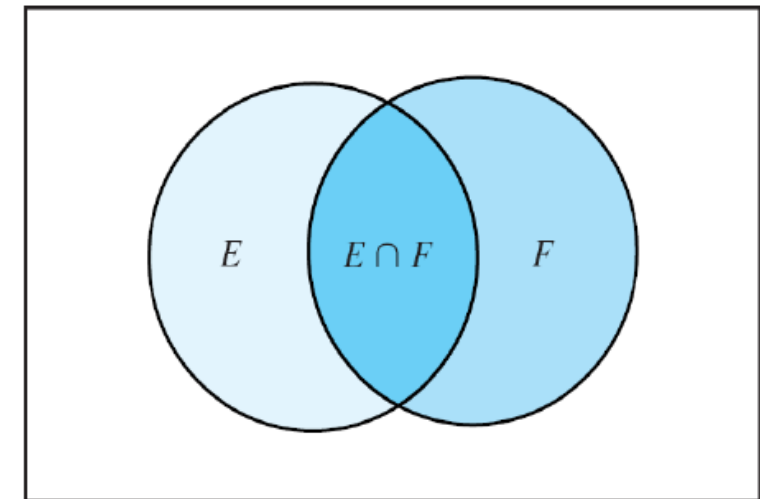
The Inclusion-Exclusion Principle

- The principle is used in counts where the decomposition yields two independent counting tasks with overlapping elements
 - If we use the sum rule, some elements would be counted twice.
- The principle uses a sum rule and then corrects for the overlapping elements.
 - two-set case: $|A \cup B| = |A| + |B| - |A \cap B|$
- Example: How many bit strings of length 8 that start with a '1' bit or end with the two bits '00'?
 - It is easy to count bit strings starting with '1': 2^7
 - It is easy to count bit strings ending with '00': 2^6
 - Deduct the overcounted number of strings starting with '1' and ending with "00": 2^5

The Inclusion-Exclusion Principle

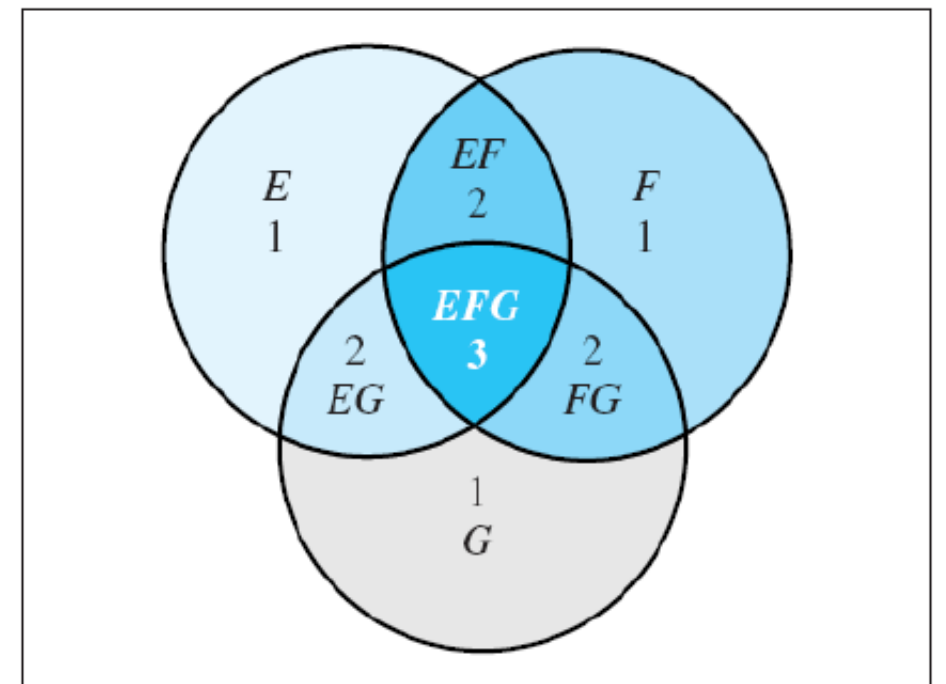
- Two sets:

- $|E \cup F| = |E| + |F| - |E \cap F|$
- $E \cap F$ got counted twice and deducted once



- Three sets:

- $|E \cup F \cup G| = |E| + |F| + |G| - |E \cap F| - |E \cap G| - |F \cap G| + |E \cap F \cap G|$
- EF, EG, FG got counted twice and then deducted once
- $E \cap F \cap G$ got counted three times then deducted three times and finally got counted once



The Inclusion-Exclusion Principle

- **The inclusion-exclusion principle:** Let A_1, A_2, \dots, A_n be finite sets, then

$$|\cup_{i=1}^n E_i| = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k}|$$

- Proof by induction:

- **Basis step:** obviously true for $n = 1, 2$
- **Inductive step:** By the two-set case ($n = 2$), we have

$$|\cup_{i=1}^n E_i| = |\cup_{i=1}^{n-1} E_i| + |E_n| - |(\cup_{i=1}^{n-1} E_i) \cap E_n|$$

Let $G_i = E_i \cap E_n$, by distributive law, we have

$$|(\cup_{i=1}^{n-1} E_i) \cap E_n| = |\cup_{i=1}^{n-1} (E_i \cap E_n)| = |\cup_{i=1}^{n-1} G_i|$$

The proof is concluded by **inductive hypothesis** and noting that

$$-(-1)^{k+1} |G_{i_1} \cap G_{i_2} \cap \dots \cap G_{i_k}| = (-1)^{k+2} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k} \cap E_n|$$

The Inclusion-Exclusion Principle

- **The inclusion-exclusion principle:** Let A_1, A_2, \dots, A_n be finite sets, then

$$|\cup_{i=1}^n E_i| = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k}|$$

- Proof by induction:

- **Basis step:** obviously true for $n = 1, 2$
- **Inductive step:** Let $G_i = E_i \cap E_n$ and we have

$$|\cup_{i=1}^n E_i| = |\cup_{i=1}^{n-1} E_i| + |E_n| - |\cup_{i=1}^{n-1} G_i|$$

By inductive hypothesis, the first union on the right becomes the summation of $(-1)^{k+1} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k}|$ over all lists i_1, i_2, \dots, i_k that do not contain n ; $|E_n|$ and second union on the right becomes the summation over all lists i_1, i_2, \dots, i_k that contain n .

The Number of Onto Functions

- **The inclusion-exclusion principle:** Let A_1, A_2, \dots, A_n be finite sets, then

$$|\cup_{i=1}^n E_i| = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k}|$$

- This can be used to determine the number of onto functions:

- Let A, B be two sets with $|A| = m$ and $|B| = n$.
 - (a) How many onto functions are there from A to B ?
 - (b) How many functions are there from A to B such that at least one element of B has no preimage?

$$\#(a) + \#(b) = n^m$$

- E_i : set of functions such that the i -th element of B has no preimage

$$\begin{aligned} \#(b) &= |\cup_{i=1}^n E_i| = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |E_{i_1} \cap E_{i_2} \cap \dots \cap E_{i_k}| \\ &= \sum_{k=1}^n (-1)^{k+1} \binom{n}{k} (n-k)^m \end{aligned}$$

Solving Linear Recurrence Relations

Linear Recurrence Relations

- **Definition:** A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where c_1, c_2, \dots, c_k are real numbers, and $c_k \neq 0$.

- **linear:** it is a linear combination of previous terms
- **homogeneous:** all terms are multiples of a_j s
- **degree k :** a_n is expressed by the previous k terms
- **constant coefficients:** coefficients are constants
- By induction, such a recurrence relation is uniquely determined by this recurrence relation, and k initial conditions a_0, a_1, \dots, a_{k-1} .

Linear Recurrence Relations

- **Definition:** A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where c_1, c_2, \dots, c_k are real numbers, and $c_k \neq 0$.

- Examples: are these linear homogeneous recurrence relations?
 - $P_n = \pi P_{n-1}$
 - $f_n = f_{n-1} + f_{n-2}$
 - $a_n = a_{n-1} + a_{n-2} \cdot a_{n-2}$
 - $H_n = 2H_{n-1} + 1$
 - $B_n = nB_{n-1}$

Linear Recurrence Relations

- **Definition:** A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where c_1, c_2, \dots, c_k are real numbers, and $c_k \neq 0$.

- Examples: are these linear homogeneous recurrence relations?
 - $P_n = \pi P_{n-1}$ *Yes, of degree 1*
 - $f_n = f_{n-1} + f_{n-2}$ *Yes, of degree 2*
 - $a_n = a_{n-1} + a_{n-2} \cdot a_{n-2}$ *No, not linear*
 - $H_n = 2H_{n-1} + 1$ *No, not homogeneous*
 - $B_n = nB_{n-1}$ *No, coefficients are not constants*

Solving Recurrences of Degree 2

- Consider an arbitrary linear homogeneous relation of degree 2 with constant coefficients:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

The characteristic equation (CE) is:

$$r^2 - c_1 r - c_2 = 0$$

- Theorem:** If this CE has 2 roots $r_1 \neq r_2$, then the sequence $\{a_n\}$ is a solution of the recurrence relation if and only if

$$a_n = a_1 r_1^n + a_2 r_2^n$$

for $n \geq 0$ and constants a_1, a_2 .

- the proof consists of two parts: “if” + “only if”
- see the textbook for more details*

Example

○ Solve the recurrence: $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

○ Solution:

- The characteristic equation (CE) is

$$r^2 - 7r + 10 = 0$$

- Two roots are 2 and 5. So, assume that

$$a_n = a_1 2^n + a_2 5^n$$

- By the two initial conditions, we have

$$a_0 = a_1 + a_2 = 2$$

$$a_1 = 2a_1 + 5a_2 = 1$$

- We get $a_1 = 3$ and $a_2 = -1$. Therefore

$$a_n = 3 \cdot 2^n - 5^n$$

Exercise (5 mins)

- What is the closed-form expression of Fibonacci sequence F_n ?
 - $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

○ Solve the recurrence: $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2, a_1 = 1$

○ Solution:

- The characteristic equation (CE) is

$$r^2 - 7r + 10 = 0$$

- Two roots are 2 and 5. So, assume that

$$a_n = a_1 2^n + a_2 5^n$$

- By the two initial conditions, we have

$$a_0 = a_1 + a_2 = 2$$

$$a_1 = 2a_1 + 5a_2 = 1$$

- We get $a_1 = 3$ and $a_2 = -1$. Therefore

$$a_n = 3 \cdot 2^n - 5^n$$

Solving Recurrences of Degree k

- Consider an arbitrary linear homogeneous relation of degree k with constant coefficients:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$$

The characteristic equation (CE) is:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \dots - c_k = 0$$

- e.g., $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$ with CE: $r^3 - 2r^2 - 5r + 6 = 0$
- Theorem:** If this CE has k distinct roots r_1, r_2, \dots, r_k , then the solutions to the recurrence $\{a_n\}$ is of the form

$$a_n = a_1 r_1^n + a_2 r_2^n + \dots + a_k r_k^n$$

for all $n \geq 0$, where a_1, a_2, \dots, a_k are constants.

- the proof is left as an exercise*

The Case of Degenerate Roots

- **Theorem:** If the CE $r^2 - c_1r - c_2 = 0$ has **only 1** root r_0 , then

$$a_n = a_1 r_0^n + a_2 n r_0^n$$

for all $n \geq 0$ and two constants a_1 and a_2 .

- *the proof is left as an exercise*

- **Theorem:** Suppose the CE $r^k - c_1 r^{k-1} - \dots - c_k = 0$ has t **distinct** roots r_1, \dots, r_t with multiplicities m_1, \dots, m_t . Then

$$a_n = \sum_{i=1}^t \left(\sum_{j=0}^{m_i-1} \alpha_{i,j} n^j \right) r_i^n$$

for all $n \geq 0$ and constants $\alpha_{i,j}$.

- e.g., $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with $a_0 = 1, a_1 = -2, a_2 = -1$
- *the proof is left as an exercise*

Exercise (3 mins)

- Solve the recurrence: $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 0$

○ **Theorem:** If the CE $r^2 - c_1r - c_2 = 0$ has **only 1** root r_0 , then

$$a_n = a_1 r_0^n + a_2 n r_0^n$$

for all $n \geq 0$ and two constants a_1 and a_2 .

Solving Nonhomogeneous Recurrences

- **Theorem:** If $a_n = p(n)$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

Then all its solutions are of the form

$$a_n = p(n) + h(n)$$

where $a_n = h(n)$ is any solution to the associated homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

- *the proof is left as an exercise*

Example

- Solve the recurrence: $a_n = 3a_{n-1} + 2n$ with $a_1 = 3$.
- Solution:
 - The characteristic equation (CE) of the associated linear homogeneous recurrence relation is $r - 3 = 0$.
 - The root is 3. So, assume $a_n = p(n)$ is a particular solution to the original recurrence relation, then all of its solutions are of the form $a_n = a_1 3^n + p(n)$.
 - It is natural to try a degree-1 polynomial, i.e., $p(n) = cn + d$. Then, $cn + d = 3(c(n - 1) + d) + 2n$, i.e., $(2c + 2)n + 2d - 3c = 0$.
 - We get $c = -1$ and $d = -3/2$. Therefore $a_n = a_1 3^n - n - 3/2$.
 - By the initial condition $a_1 = 2a_1 - 1 - 3/2 = 3$, we get $a_1 = 11/4$.

Generating Functions

Generating Functions

- **Definition:** The **generating function** for the sequence $\{a_k\}$ of real numbers is the infinite series

$$G(x) = a_0 + a_1x + \cdots + a_kx^k + \cdots = \sum_{k=0}^{\infty} a_kx^k$$

- We use generating functions to **characterize** sequences:

- $\sum_{k=0}^{\infty} 3x^k$: generating function for the sequence $\{a_k\}$ with $a_k = 3$
- $\sum_{k=0}^{\infty} 2^k x^k$: generating function for the sequence $\{a_k\}$ with $a_k = 2^k$

Generating Functions

- **Definition:** The **generating function** for the sequence $\{a_k\}$ of real numbers is the infinite series

$$G(x) = a_0 + a_1x + \cdots + a_kx^k + \cdots = \sum_{k=0}^{\infty} a_kx^k$$

- We use generating functions to **characterize** sequences:

- $\sum_{k=0}^{\infty} 3x^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n 3x^k = 3 \lim_{n \rightarrow \infty} \frac{1 - x^{n+1}}{1 - x} = \frac{3}{1 - x}$ for $|x| < 1$
- $\sum_{k=0}^{\infty} 2^k x^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n (2x)^k = \lim_{n \rightarrow \infty} \frac{1 - (2x)^{n+1}}{1 - 2x} = \frac{1}{1 - 2x}$ for $|2x| < 1$

Operations of Generating Functions

- **Theorem:** Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$, then

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k \quad \text{and} \quad f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^k a_j b_{k-j} \right) x^k$$

** the proof can be found in a calculus course*

- Example: $f(x) = g(x) = \sum_{k=0}^{\infty} a^k x^k$
 - We know $G(x) = \sum_{k=0}^{\infty} a^k x^k = 1/(1 - ax)$ for $|ax| < 1$
 - Therefore,

$$f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^k a^j a^{k-j} \right) x^k = \sum_{k=0}^{\infty} (k+1) a^k x^k = \frac{1}{(1 - ax)^2}$$

The Case of Finite Sequences

- **Definition:** The generating function for the finite sequence a_0, a_1, \dots, a_n of real numbers is a polynomial of degree n

$$G(x) = a_0 + a_1x + \dots + a_nx^n$$

- A finite sequence a_0, a_1, \dots, a_n can be easily extended to infinity by setting $a_{n+1} = a_{n+2} = \dots = 0$.
- Example: What is the generating function for the finite sequence a_0, a_1, \dots, a_n , with $a_k = C(n, k)$?

$$G(x) = C(n,0) + C(n,1)x + \dots + C(n,n)x^n = (1+x)^n$$

Useful Generating Functions

$$(1 + x)^n = \sum_{k=0}^n C(n, k)x^k$$

$$(1 + ax)^n = \sum_{k=0}^n C(n, k)a^k x^k$$

$$(1 + x^r)^n = \sum_{k=0}^n C(n, k)x^{rk}$$

$$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^n x^k = 1 + x + x^2 + \dots + x^n$$

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

$$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2 x^2 + \dots$$

$$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \dots$$

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

Generating Functions for Counting

- **Example 1:** Find the number of solutions of $x_1 + x_2 + x_3 = 17$, such that x_1, x_2, x_3 are all nonnegative integers and $2 \leq x_1 \leq 5$, $3 \leq x_2 \leq 6$, $4 \leq x_3 \leq 7$.
- Solution: Using generating functions, the number is the coefficient of x^{17} in the expansion of

$$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$$

The answer is 3.

Generating Functions for Counting

- **Example 2:** In how many ways can eight identical cookies be distributed among three distinct children if each child receives at least two and no more than four cookies?
- Solution: Using generating functions, the number of ways is the coefficient of x^8 in the expansion of

$$(x^2 + x^3 + x^4)^3$$

The answer is 6.

Generating Functions for Counting

- **Example 3:** In how many ways can r dollars be paid by coins that are worth 1 dollar, 2 dollar, and 5 dollar each?
- Solution: Using generating functions, the number of ways is the coefficient of x^r in the expansion of the following functions:

- If the order of coins do not matter:

$$(1 + x + x^2 + x^3 + \dots) (1 + x^2 + x^4 + x^6 + \dots) (1 + x^5 + x^{10} + x^{15} + \dots)$$

- If the order matters:

$$1 + (x + x^2 + x^5) + (x + x^2 + x^5)^2 + (x + x^2 + x^5)^3 + \dots$$

Generating Functions for Counting

- **Example 4:** Use **generating functions** to find the number of **k -combinations** of a set with n elements.
- Solution: Each of the n elements in the set contributes one term $(1 + x)$ to the generating function $f(x) = (1 + x)^n = \sum_{k=0}^n a_k x^k$. Then by the **binomial theorem**, we have $a_k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.

r -Combinations with Repetition

- An r -combination with repetition allowed (or a multiset of size r), chosen from a set of n elements, is an unordered selection of r elements from n elements with repetition allowed.

- Example: How many multisets of size 17 from the set $\{1, 2, 3\}$?

- This is equivalent to find the number of nonnegative solutions to

$$x_1 + x_2 + x_3 = 17$$

- The solution is $C(3 + 17 - 1, 17) = C(19, 17) = C(19, 2)$

How many ways one can split 17 balls into 3 groups?

Imagine 19 boxes are aligned in a line, then one just needs to choose 17 boxes and put balls in each of them, with 2 empty boxes splitting the balls into 3 groups.

- This is equal to the coefficient of x^{17} in the generating function:

$$(1 + x + x^2 + \dots)^3 = 1/(1 - x)^3 = \sum_{k=0}^{\infty} C(3 + k - 1, k)x^k$$

Useful Generating Functions (more)

- Hinted from r -combinations with repetition allowed:

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

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

$$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1, k)a^k x^k$$

- Taylor series:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

$$\ln(1+x) = \sum_{k=0}^{\infty} \frac{(-1)^{k+1} x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

Solving Recurrences with $G(x)$

- **Example 1:** Solve $a_k = 3a_{k-1}$ ($k \geq 1$) with $a_0 = 2$.
- Solution: Let $G(x)$ be the generating function of $\{a_k\}$, we have

$$\begin{aligned} G(x) - 3xG(x) &= \sum_{k=0}^{\infty} a_k x^k - \sum_{k=1}^{\infty} 3a_{k-1} x^k \\ &= a_0 + \sum_{k=1}^{\infty} (a_k - 3a_{k-1}) x^k = a_0 = 2 \end{aligned}$$

Then, we know

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

Therefore, the solution is $a_k = 2 \cdot 3^k$ for $k \geq 0$.

Solving Recurrences with $G(x)$

- **Example 2:** Solve $a_n = 8a_{n-1} + 10^{n-1}$ ($n \geq 2$) with $a_1 = 9$.
- Solution: Let $a_0 = 1$, then we have $a_1 = 9 = 8a_0 + 10^0$ holds, so the recurrence relation is consistent with $n \geq 1$. Then, let $G(x)$ be the generating function of $\{a_n\}$ for $n \geq 0$, we have

$$\begin{aligned} G(x) - a_0 &= \sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} (8a_{n-1} x^n + 10^{n-1} x^n) \\ &= 8x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} + x \sum_{n=1}^{\infty} 10^{n-1} x^{n-1} \\ &= 8x \sum_{n=0}^{\infty} a_n x^n + x \sum_{n=0}^{\infty} 10^n x^n \\ &= 8xG(x) + x/(1 - 10x) \end{aligned}$$

Solving Recurrences with $G(x)$

- **Example 2:** Solve $a_n = 8a_{n-1} + 10^{n-1}$ ($n \geq 2$) with $a_1 = 9$.
- Solution: Let $a_0 = 1$, then we have $a_1 = 9 = 8a_0 + 10^0$ holds, so the recurrence relation is consistent with $n \geq 1$. Then, let $G(x)$ be the generating function of $\{a_n\}$ for $n \geq 0$, we have

$$G(x) - a_0 = G(x) - 1 = 8xG(x) + x/(1 - 10x)$$

Solving for $G(x)$ shows that

$$G(x) = \frac{1 - 9x}{(1 - 8x)(1 - 10x)}$$

Solving Recurrences with $G(x)$

- **Example 2:** Solve $a_n = 8a_{n-1} + 10^{n-1}$ ($n \geq 2$) with $a_1 = 9$.
- Solution: Let $a_0 = 1$, then we have $a_1 = 9 = 8a_0 + 10^0$ holds, so the recurrence relation is consistent with $n \geq 1$. Then, let $G(x)$ be the generating function of $\{a_n\}$ for $n \geq 0$, we have

$$\begin{aligned} G(x) &= \frac{1 - 9x}{(1 - 8x)(1 - 10x)} = \frac{1}{2} \left(\frac{1}{1 - 8x} + \frac{1}{1 - 10x} \right) \\ &= \frac{1}{2} \left(\sum_{n=0}^{\infty} 8^n x^n + \sum_{n=0}^{\infty} 10^n x^n \right) = \sum_{n=0}^{\infty} \frac{1}{2} (8^n + 10^n) x^n \end{aligned}$$

Therefore, the solution is $a_n = \frac{1}{2}(8^n + 10^n)$ for $n \geq 0$.

Solving Recurrences with $G(x)$

- Using generating functions to solve recurrence relations:
 - **Step 1:** Based on the given recurrence and its initial conditions, find its generating function $G(x)$ as an explicit formula.

E.g.,
$$G(x) = \frac{1 - 9x}{(1 - 8x)(1 - 10x)}$$

- **Step 2:** Rewrite $G(x)$ as the summation of an infinite (or finite) series.
** this step may be tricky*

E.g.,
$$G(x) = \sum_{n=0}^{\infty} \frac{1}{2}(8^n + 10^n)x^n$$

08 Relations

To be continued...

Announcement

- Quiz 2 will take place in class on Dec 8 and it captures materials from 06 Induction and Recursion to 07 Counting.
- Again, the quiz is open-book:
 - 3~6 questions in 30 minutes
 - bring several pieces of paper to write your answers on
 - no electronic device is allowed during the quiz
 - take photos of your quiz answers and submit them as a single file via Blackboard (you will have 5 minutes after quiz to do this)
 - must attend the quiz in person