Discrete Mathematics for Computer Science

Lecture 13: Counting

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

Combinatorial Proof

Theorem: Let n and r be nonnegative integers with $r \leq n$. Then $C(n, r) = C(n, n-r)$.

Definition: A combinatorial proof of an identity is

- a proof that uses counting arguments to prove that both sides of the identity count the same objects but in different ways
- or a proof that is based on showing that there is a bijection between the sets of objects counted by the two sides of the identity.

These two types of proofs are called double counting proofs and bijective proofs, respectively.

The Binomial Theorem

Let x and y be variables, and let n be a nonnegative integer:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

Proof: The terms in the product when it is expanded are of the form $x^{n-j}y^j$ for $j = 0, 1, 2, ..., n$.

To count the number of terms of the form $x^{n-j}y^j$, it is necessary to choose $n-j$ xs from the n sums (so that the other j terms in the product are ys).

Therefore, the coefficient of $x^{n-j}y^j$ is $\binom{n}{n-j}$, which is $\binom{n}{j}$.

Pascal's Identity

Theorem: Let n and k be positive integers with $n \geq k$. Then,

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

Proof: Suppose that T is a set containing $n+1$ elements.

- let a be an element in T
- let $S = T - a$.

Left-hand side counts the number of subsets of T containing k elements, i.e., $\binom{n+1}{k}$.

Note that a subset of T with k elements either contains a together with $k-1$ elements of S, or contains k elements of S and does not contain a.

Right-hand side counts

- the subsets of $k-1$ elements of S, i.e., $\binom{n}{k-1}$
- the subsets of k elements of T, i.e., $\binom{n}{k}$.

Pascal's Identity

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}$$

Consider $S = \{A, B, C, D, E\}$.

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

Set S_1 of 2-subsets of S can be partitioned into 2 disjoint parts:

- S_2: the 2-subsets that contain E
- S_3: the set of 2-subsets that do not contain E

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

Pascal's Triangle

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$
$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$
$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$
$$\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6}$$
$$\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7}$$
$$\binom{8}{0}\ \binom{8}{1}\ \binom{8}{2}\ \binom{8}{3}\ \binom{8}{4}\ \binom{8}{5}\ \binom{8}{6}\ \binom{8}{7}\ \binom{8}{8}$$
$$\cdots$$

By Pascal's identity:

$$\binom{6}{4} + \binom{6}{5} = \binom{7}{5}$$

$$1$$
$$1 \quad 1$$
$$1 \quad 2 \quad 1$$
$$1 \quad 3 \quad 3 \quad 1$$
$$1 \quad 4 \quad 6 \quad 4 \quad 1$$
$$1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1$$
$$1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$
$$1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1$$
$$1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1$$
$$\cdots$$

Pascal's identity, together with the initial conditions $\binom{n}{0} = \binom{n}{n} = 1$ for all integers n, can be used to recursively define binomial coefficients.

Other Identities Involving Binomial Coefficients

Let n and r be nonnegative integers with $r \leq n$.

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}.$$

Proof: Consider bit strings of length $n+1$.

The left-hand side, $\binom{n+1}{r+1}$, counts the bit strings of length $n+1$ containing $r+1$ ones.
We show that the right-hand side counts the same objects by considering the cases corresponding to the possible locations of the final 1 in a string with $r+1$ ones.

Other Identities Involving Binomial Coefficients

Let n and r be nonnegative integers with $r \leq n$.

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}.$$

Proof: We show that the right-hand side counts the same objects by considering the cases corresponding to the possible locations of the final 1 in a string with $r+1$ ones.

- This final one must occur at position $r+1$, $r+2$, . . . , or $n+1$.
- If the last one is the k-th bit there must be r ones among the first $k-1$ positions. There are $\binom{k-1}{r}$ such bit strings.

Summing over k with $r+1 \leq k \leq n+1$, we find that there are

$$\sum_{k=r+1}^{n+1} \binom{k-1}{r} = \sum_{j=r}^{n} \binom{j}{r}.$$

Labelling and Trinomial Coefficients

Suppose we have k_1 labels of one kind (e.g., red) and $k_2 = n - k_1$ labels of another (e.g., blue). How many different ways to label n distinct objects?

$$C(n, k_1) = \frac{n!}{k_1! k_2!}$$

If we have k_1 labels of one kind (e.g., red), k_2 labels of a second kind (e.g., blue), and $k_3 = n - k_1 - k_2$ labels of a third kind (e.g., green). How many different ways to label n distinct objects?

- There are $\binom{n}{k_1}$ ways to choose the red items
- There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n - k_1$.

Labelling and Trinomial Coefficients

How many different ways to label n distinct objects?

- There are $\binom{n}{k_1}$ ways to choose the red items
- There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n - k_1$.

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

This is called a trinomial coefficient and denote it as

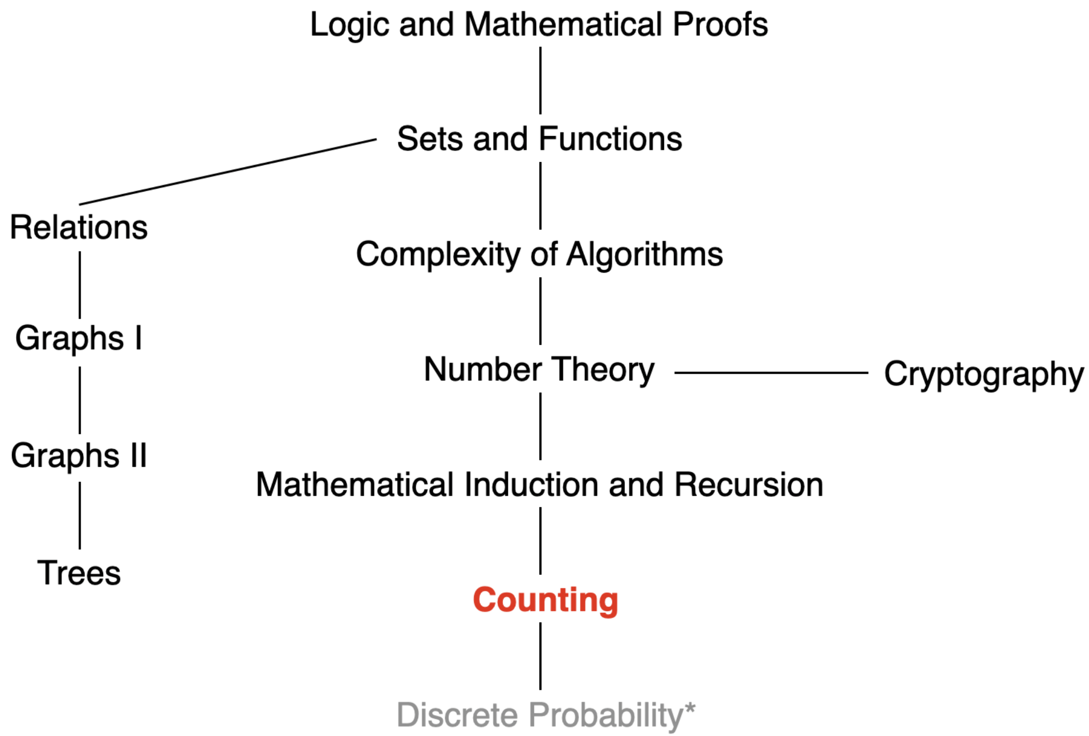
$$\binom{n}{k_1 \quad k_2 \quad k_3} = \frac{n!}{k_1!k_2!k_3!},$$

where $k1 + k2 + k3 = n$.

What is the coefficient of $x^{k_1}y^{k_2}z^{k_3}$ in $(x+y+z)^n$?

SUSTech Southern University of Science and Technology

This Lecture



Counting basis, Permutations and Combinations, Binomial Coefficients, The Birthday Paradox, Solving Linear Recurrence Relations, ...

The Birthday Paradox

Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

It's greater than 1/2! (only need 23).

A_n - "there are n students in a room and at least two of them share a birthday."

We may assume that a year has 365 days and there are no twins in the room.

This will be very similar to the analysis of hashing n keys into a table of size 365.

The Birthday Paradox

A_n - "there are n students in a room and at least two of them share a birthday."

Sample space: $|S| = 365^n$

B_n - "there are n students in a room and none of them share a birthday."

$$\#B_n = 365 \times 364 \times ... \times (365 - (n-1))$$

$$\#A_n + \#B_n = 365^n$$

The Birthday Paradox

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 Paradox

Event A: at least two people in the room have the same birthday
Event B: no two people in the room have the same birthday

$\Pr[A] = 1 - \Pr[B]$

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

$\Pr[A] = 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right)$

"Birthday" Attacks

Given a function f, the goal of the attack is to find two different inputs x_1 and x_2 such that $f(x_1) = f(x_2)$. Such a pair x_1 and x_2 is called a collision.

Collision in Hashing Functions: A good hashing function yields few collisions (i.e., which are mappings of two different keys to the same memory location).

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

"Birthday" Attacks

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

Note that $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$, for $|x| \ll 1$, $e^x \approx 1 + x$.

Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

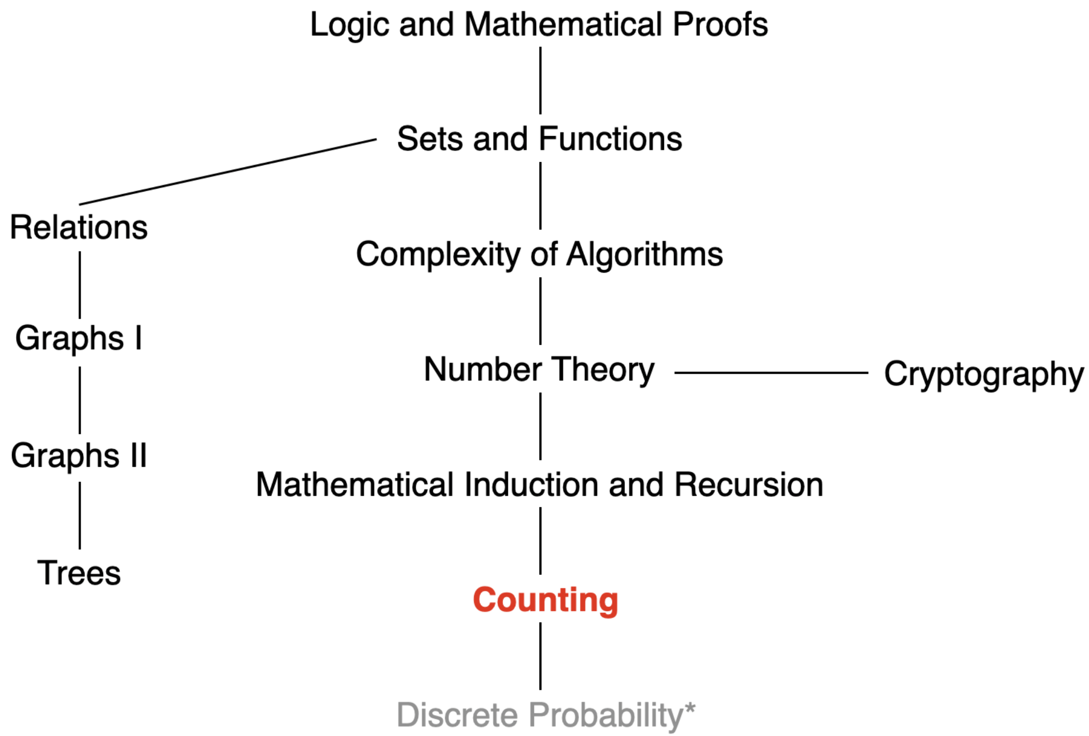
This probability can be approximated as

$$p(n;H) \approx 1 - e^{-n(n-1)/(2H)} \approx 1 - e^{-n^2/(2H)}.$$

Let $n(p;H)$ be the smallest number of values we have to choose, such that the probability for finding a collision is at least p. By inverting the expression above, we have

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

This Lecture



Counting basis, Permutations and Combinations, Binomial Coefficients, The Birthday Paradox, Solving Linear Recurrence Relations, ...

Solving Linear Recurrence Relations

- Linear Homogeneous Recurrence Relations
- Linear Nonhomogeneous Recurrence Relations

Solving Linear Recurrence Relations

One important class of recurrence relations can be explicitly solved in a systematic way.

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

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

where $c_1, c_2, \ldots, c_k$ 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

By induction, such a recurrence relation is uniquely determined by this recurrence relation and k initial conditions $a_0, a_1, \ldots, a_{k-1}$.

Solving Linear Recurrence Relations

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

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

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

Example:

- $P_n = 1.11 \cdot P_{n-1}$ linear homogeneous recurrence relation of degree 1
- $f_n = f_{n-1} + f_{n-2}$ linear homogeneous recurrence relation of degree 2
- $a_n = a_{n-1} + a_{n-2}^2$ NOT linear
- $H_n = 2H_{n-1} + 1$ NOT homogeneous
- $B_n = nB_{n-1}$ coefficients are not constants

Solving Linear Recurrence Relations

Example: Consider the recurrence relation

$$a_n = 2a_{n-1} - a_{n-2},$$

Which of the following are solutions?

- $a_n = 3n$ Yes
- $a_n = 2^n$ No
- $a_n = 5$ Yes

Question: Why not unique?

Question: Any systematic way?

Solving Linear Recurrence Relations

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

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

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

Basic idea: Look for solutions of the form $a_n = r^n$, where r is a constant.

Note that $a_n = r^n$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$ if and only if

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \ldots + c_k r^{n-k}.$$

Divide both sides by r^{n-k},

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \ldots - c_{k-1} r - c_k = 0.$$

Characteristic equation of the recurrence relation.

Solving Linear Recurrence Relations: Degree Two

Theorem: Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2.

Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n \text{ for } n = 0, 1, 2, \ldots,$$

where α_1 and α_2 are constants.

Proof: To show that both $\{a_n\}$ and $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ are the solutions of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ and satisfy the initial conditions.

- $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ is a solution of the recurrence relation.
- For every recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, there exist α_1 and α_2 that satisfy the initial conditions.

Solving Linear Recurrence Relations: Degree Two

Proof: $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ is a solution of the recurrence relation.

Since r_1 and r_2 are roots of $r^2 - c_1 r - c_2 = 0$, it follows that $r_1^2 = c_1 r_1 + c_2$ and $r_2^2 = c_1 r_2 + c_2$.

$$\begin{aligned}
c_1 a_{n-1} + c_2 a_{n-2} &= c_1(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}) + c_2(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2}) \\
&= \alpha_1 r_1^{n-2}(c_1 r_1 + c_2) + \alpha_2 r_2^{n-2}(c_1 r_2 + c_2) \\
&= \alpha_1 r_1^{n-2} r_1^2 + \alpha_2 r_2^{n-2} r_2^2 \\
&= \alpha_1 r_1^n + \alpha_2 r_2^n \\
&= a_n.
\end{aligned}$$

Solving Linear Recurrence Relations: Degree Two

For every recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, there exist α_1 and α_2 that satisfy the initial conditions.

Suppose that $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ is a solution of the recurrence relation, and the initial conditions $a_0 = C_0$ and $a_1 = C_1$ hold.

$$a_0 = C_0 = \alpha_1 + \alpha_2, \qquad a_1 = C_1 = \alpha_1 r_1 + \alpha_2 r_2.$$

Thus,

$$\alpha_1 = \frac{C_1 - C_0 r_2}{r_1 - r_2}, \qquad \alpha_2 = C_0 - \alpha_1 = \frac{C_0 r_1 - C_1}{r_1 - r_2}.$$

α_1 and α_2 exist since $r_1 \neq r_2$.

Solving Linear Recurrence Relations: Degree Two

Proof: To show that both $\{a_n\}$ and $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ are the solutions of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ and satisfy the initial conditions.

- $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ is a solution of the recurrence relation.
- For every recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, there exist α_1 and α_2 that satisfy the initial conditions.

Note that there is a unique solution of a linear homogeneous recurrence relation of degree two with two initial conditions.

The two solutions $\{a_n\}$ and $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ must be the same.

Solving Linear Recurrence Relations: Degree Two

Theorem: Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c2 = 0$ has two distinct roots r_1 and r_2.

Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n \text{ for } n = 0, 1, 2, ...,$$

where α_1 and α_2 are constants.

Solve Linear Recurrence Relations:

- Solve r_1 and r_2 with $r^2 - c_1 r - c2 = 0$.
- Solve α_1 and α_2 with the initial conditions.

Example 1: Fibonacci number

Fibonacci number: $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

What is the closed-form expression of F_n?

To solve r_1 and r_2, consider $r^n = r^{n-1} + r^{n-2}$, i.e., $r^2 - r - 1 = 0$. There are two different roots:

$$r_1 = \frac{1+\sqrt{5}}{2}, \qquad r_2 = \frac{1+\sqrt{5}}{2}$$

Consider the form of $F_n = \alpha_1 r_1^n + \alpha_2 r_2^n$. To solve α_1 and α_2, by $F_0 = 0$ and $F_1 = 1$, we have $\alpha_1 + \alpha_2 = 0$ and $\alpha_1 r_1 + \alpha_1 r_2 = 1$.

Thus, $\alpha_1 = 1/\sqrt{5}$ and $\alpha_2 = -\alpha_1$. Hence,

$$F_n = \alpha_1 r_1^n + \alpha_2 r_2^n = \frac{r_1^n - r_2^n}{\sqrt{5}}.$$

SUSTech Southern University of Science and Technology

Example 2

$a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$, $a_1 = 7$.

The characteristic equation is

$$r^2 - r - 2 = 0.$$

The two roots are 2 and -1. So, assume that

$$a_n = \alpha_1 2^n + \alpha_2 (-1)^n.$$

By the two initial conditions, we have

$$a_0 = \alpha_1 + \alpha_2 = 2, \qquad a_1 = 2\alpha_1 - \alpha_2 = 7.$$

We get $\alpha_1 = 3$ and $\alpha_2 = -1$. Thus,

$$a_n = 3 \cdot 2^n - (-1)^n.$$

Example 3

$a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

The characteristic equation is

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

Two roots are 2 and 5. So, assume that

$$a_n = \alpha_1 2^n + \alpha_2 5^n.$$

By the two initial conditions, we have

$$a_0 = \alpha_1 + \alpha_2 = 2, \qquad a_1 = 2\alpha_1 + 5\alpha_2 = 1.$$

We get $\alpha_1 = 3$ and $\alpha_2 = -1$. Thus,

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

Solving Linear Recurrence Relations of Degree k

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

$$a_n = \sum_{i-1}^{k} c_i a_{n-i}.$$

The characteristic equation (CE) is:

$$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

Theorem: If this CE has k distinct roots r_i, then the solutions to the recurrence are of the form

$$a_n = \sum_{i=1}^{k} \alpha_i r_i^n$$

for all $n \geq 0$, where the α_i's are constants.

Example

$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ with the initial conditions $a_0 = 2$, $a_1 = 5$, and $a_2 = 15$.

The characteristic equation is

$$r^3 - 6r^2 + 11r - 6 = 0.$$

The characteristic roots are $r = 1$, $r = 2$, and $r = 3$, because $r^3 - 6r^2 + 11r - 6 = (r-1)(r-2)(r-3)$. So, assume that

$$a_n = \alpha_1 \cdot 1^n + \alpha_2 \cdot 2^n + \alpha_3 \cdot 3^n.$$

By the three initial conditions, we have $a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3$, $\quad a_1 = 5 = \alpha_1 + \alpha_2 \cdot 2 + \alpha_3 \cdot 3$, $\quad a_2 = 15 = \alpha_1 + \alpha_2 \cdot 4 + \alpha_3 \cdot 9$.

We get $\alpha_1 = 1$, $\alpha_2 = -1$, and $\alpha_3 = 2$. Thus,

$$a_n = 1 - 2^n + 2 \cdot 3^n.$$

The Case of Degenerate Roots: Degree Two

Theorem: If the $r^2 - c_1 r - c_2 = 0$ has only 1 root r_0, then

$$a_n = (\alpha_1 + \alpha_2 n) r_0^n,$$

for all $n \geq 0$ and two constants α_1 and α_2.

Example

$a_n = 4a_{n-1} - 4a_{n-2}$ with $a_0 = 1$ and $a_1 = 0$

The characteristic equation is

$$r^2 - 4r + 4 = 0.$$

The only root is 2. So, assume that

$$a_n = (\alpha_1 + \alpha_2 n)2^n.$$

By the three initial conditions, we have

$$a_0 = \alpha_1 = 1, \qquad a_1 = 2 \cdot (\alpha_1 + \alpha_2) = 0.$$

We get $\alpha_1 = 1$, $\alpha_2 = -1$. Thus,

$$a_n = (1 - n)2^n.$$

The Case of Degenerate Roots: Degree k

Theorem: Suppose that there are t roots $r_1, \ldots, r_t$ with multiplicities $m_1, \ldots, m_t$. 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 $\alpha_{i,j}$.

$$\begin{aligned} a_n = {} & (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n \\ & + \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n \end{aligned}$$

Example

$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with $a_0 = 1$, $a_1 = -2$, $a_2 = -1$.

The characteristic equation is

$$r^3 + 3r^2 + 3r + 1 = 0.$$

There is a single root $r = -1$ of multiplicity three of the characteristic equation. Thus, assume that

$$a_n = (\alpha_{1,0} + \alpha_{1,1} n + \alpha_{1,2} n^2)(-1)^n.$$

By the three initial conditions, we have ...

We get $\alpha_{1,0} = 1$, $\alpha_{1,1} = 3$, $\alpha_{1,2} = -2$. Thus, $a_n = (1 + 3n - 2n^2)(-1)^n$.

Solving Linear Recurrence Relations

- Linear Homogeneous Recurrence Relations
- Linear Nonhomogeneous Recurrence Relations

Linear Nonhomogeneous Recurrence Relations

Definition: A linear nonhomogeneous relation with constant coefficients may contain some terms $F(n)$ that depend only on n

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

The recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$ is called the associated homogeneous recurrence relation.

Example:

- $a_n = a_{n-1} + 2^n$ $\quad a_n = a_{n-1}$
- $a_n = a_{n-1} + a_{n-2} + n^2 + n + 1$ $\quad a_n = a_{n-1} + a_{n-2}$
- $a_n = 3a_{n-1} + n3^n$ $\quad a_n = 3a_{n-1}$
- $a_n = a_{n-1} + a_{n-2} + a_{n-3} + n!$ $\quad a_n = a_{n-1} + a_{n-2} + a_{n-3}$

Linear Nonhomogeneous Recurrence Relations

Every solution is the sum of a particular solution and a solution of the associated linear homogeneous recurrence relation.

Theorem: If $\{a_n^{(p)}\}$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

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

Then all its solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)},$$

where $\{a_n^{(h)}\}$ is any solution to the associated homogeneous recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$.

Linear Nonhomogeneous Recurrence Relations

Proof: Suppose $\{a_n^{(p)}\}$ is a particular solution of the nonhomogeneous recurrence relation,

$$a_n^{(p)} = c_1 a_{n-1}^{(p)} + c_2 a_{n-2}^{(p)} + \ldots + c_k a_{n-k}^{(p)} + F(n).$$

Now suppose that $\{b_n\}$ is a second solution of the nonhomogeneous recurrence relation,

$$b_n = c_1 b_{n-1} + c_2 b_{n-2} + \ldots + c_k b_{n-k} + F(n).$$

Subtracting the first of these two equations from the second shows that

$$b_n - a_n^{(p)} = c_1(b_{n-1} - a_{n-1}^{(p)}) + \ldots + c_k(b_{n-k} - a_{n-k}^{(p)}).$$

It follows that $\{b_n - a_n^{(p)}\}$ is a solution of the associated homogeneous linear recurrence, say, $\{a_n^{(h)}\}$.
Consequently, $b_n = a_n^{(p)} + a_n^{(h)}$ for all n.

Linear Nonhomogeneous Recurrence Relations

Theorem: If $\{a_n^{(p)}\}$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

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

Then all its solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)},$$

where $\{a_n^{(h)}\}$ is any solution to the associated homogeneous recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$.

The key is to find the particular solution to the linear nonhomogeneous relation. However, there is no general method for finding such a solution.

SUSTech Southern University of Science and Technology

Example 1

There are techniques that work for certain types of functions $F(n)$, such as polynomials and powers of constants.

Example 1: $a_n = 3a_{n-1} + 2n$. What is the solution with $a_1 = 3$?

- Compute $a_n^{(h)}$
- Compute $a_n^{(p)}$
- Initial condition

Example 1

To compute $a_n^{(h)}$:
The characteristic equation is

$$r^2 - 3r = 0.$$

The roots are $r_1 = 3$ and $r_2 = 0$. By So, assume that

$$a_n^{(h)} = \alpha 3^n.$$

To compute $a_n^{(p)}$: Try $a_n^{(p)} = cn + d$. Thus,

$$cn + d = 3(c(n-1) + d) + 2n.$$

We get $c = -1$ and $d = -3/2$. Thus, $a_n^{(p)} = -n - 3/2$.

Example 1

To compute $a_n^{(h)}$: $a_n^{(h)} = \alpha 3^n$.

To compute $a_n^{(p)}$: $a_n^{(p)} = -n - 3/2$.

Initial condition:

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha 3^n - n - 3/2.$$

Base on the initial condition $a_1 = 3$. We have $3 = -1 - 3/2 + 3\alpha$, which implies $\alpha = 11/6$. Thus, $a_n = -n - 3/2 + (11/6)3^n$.

Example 2

Find all solutions of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$. (Since we do not provide the initial conditions, obtain the general form would be sufficient.)

Solution:

- $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$
- Try $a_n^{(p)} = C \cdot 7^n$:

$$C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n.$$

Thus, $C = 49/20$, and $a_n^{(p)} = (49/20)7^n$.

$$a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n.$$

Linear Nonhomogeneous Recurrence Relations

For previous two examples, we made a guess that there are solutions of a particular form. This was not an accident.

Suppose that $\{a_n\}$ satisfies the linear nonhomogeneous recurrence relation

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

where $c_1, c_2, \ldots, c_k$ are real numbers, and

$$F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n,$$

where $b_0, b_1, \ldots, b_t$ and s are real numbers. When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

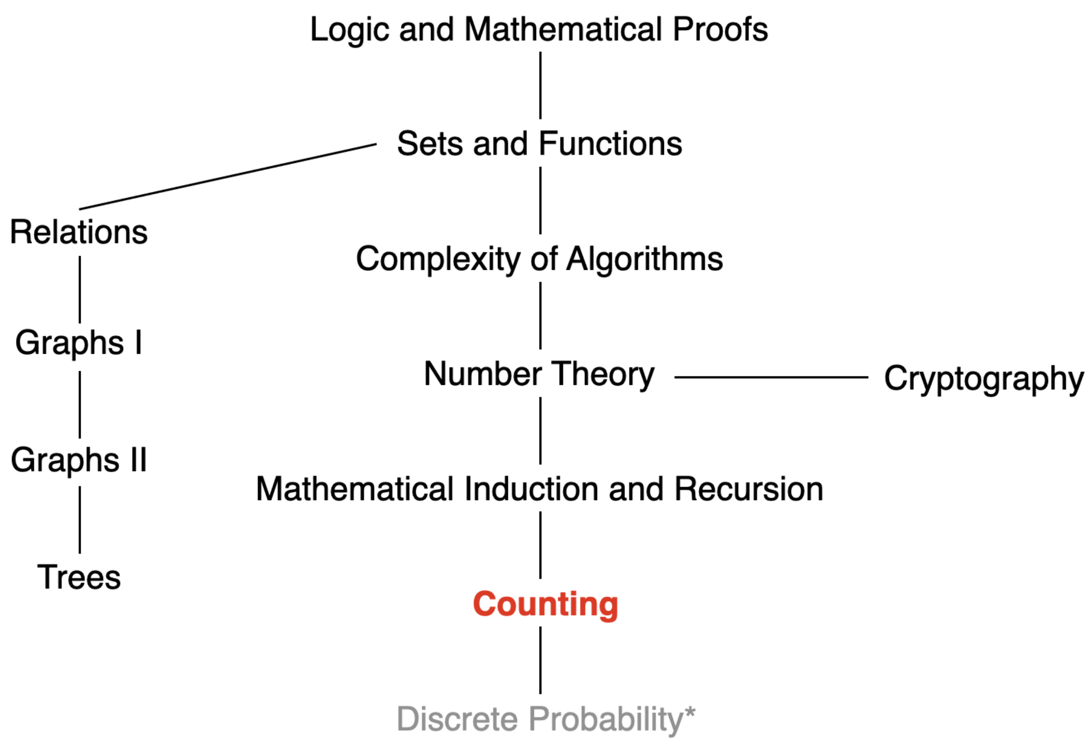
$$(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

When s is a root of this characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

Southern University of Science and Technology

This Lecture



Counting basis, Permutations and Combinations, Binomial Coefficients, The Birthday Paradox, Solving Linear Recurrence Relations, Generating Function, ...

Generating Function

The generating function for the sequence $a_0, a_1, \ldots, a_k, \ldots$ of real numbers is the infinite series

$$G(x) = a_0 + a_1 x + \ldots + a_k x^k + \ldots = \sum_{k=0}^{\infty} a_k x^k.$$

Example:

- The sequence $\{a_k\}$ with $a_k = 3$

$$\sum_{k=0}^{\infty} 3x^k$$

- The sequence $\{a_k\}$ with $a_k = 2^k$

$$\sum_{k=0}^{\infty} 2^k x^k$$

Generating Function: Finite Series

A finite sequence $a_0, a_1, \ldots, a_n$ can be easily extended by setting $a_{n+1} = a_{n+2} = \ldots = 0$.

The generating function $G(x)$ of this infinite sequence $\{a_n\}$ is a polynomial of degree n, i.e.,

$$G(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Example: What is the generating function for the sequence $a_0, a_1, \ldots,$ a_m, with $a_k = C(m, k)$?

$$G(x) = C(m, 0) + C(m, 1)x + C(m, 2)x^2 + \ldots + C(m, m)x^m.$$

Based on binomial theorem, $G(x) = (1 + x)^m$.

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

Useful Facts

- For $|x| < 1$, function $G(x) = 1/(1-x)$ is the generating function of the sequence 1, 1, 1, 1, . . . ,

$$1/(1-x) = 1 + x + x^2 + \ldots$$

- For $|ax| < 1$, function $G(x) = 1/(1-ax)$ is the generating function of the sequence 1, a, a^2, a^3, . . . ,

$$1/(1-ax) = 1 + ax + a^2x^2 + \ldots$$

- For $|x| < 1$, $G(x) = 1/(1-x)^2$ is the generating function of the sequence 1, 2, 3, 4, 5, . . .

$$1/(1-x)^2 = 1 + 2x + 3x^2 + \ldots$$

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,

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

$$f(x)g(x) = \sum_{k=0}^{\infty} (\sum_{j=0}^{k} a_j b_{k-j}) x^k$$

Example 1: To obtain the corresponding sequence of $G(x) = 1/(1-x)^2$: Consider $f(x) = 1/(1-x)$ and $g(x) = 1/(1-x)$. Since the sequence of $f(x)$ and $g(x)$ corresponds to 1, 1, 1, ..., we have

$$G(x) = f(x)g(x) = \sum_{k=0}^{\infty} (k+1) x^k.$$

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,

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

$$f(x)g(x) = \sum_{k=0}^{\infty} (\sum_{j=0}^{k} a_j b_{k-j}) x^k$$

Example 2: To obtain the corresponding sequence of $G(x) = 1/(1 - ax)^2$ for $|ax| < 1$:

Consider $f(x) = 1/(1 - ax)$ and $g(x) = 1/(1 - ax)$. Since the sequence of $f(x)$ and $g(x)$ corresponds to 1, a, a^2, ..., we have

$$G(x) = f(x)g(x) = \sum_{k=0}^{\infty} (k + 1) a^k x^k.$$

Extended Binomial Coefficient

Let u be a real number and k a nonnegative integer. Then the extended binomial coefficient $\binom{n}{k}$ is defined by

$$\binom{u}{k} = \begin{cases} u(u-1)\cdots(u-k+1)/k! & \text{if } k > 0, \\ 1 & \text{if } k = 0. \end{cases}$$

Here, u cannot any real number, e.g., negative integers, non-integers, ...

Extended Binomial Coefficient

$$\binom{u}{k} = \begin{cases} u(u-1)\cdots(u-k+1)/k! & \text{if } k > 0, \\ 1 & \text{if } k = 0. \end{cases}$$

Example: Find the extended binomial coefficients $\binom{-2}{3}$ and $\binom{1/2}{3}$.

Taking $u = -2$ and $k = 3$

$$\binom{-2}{3} = \frac{(-2)(-3)(-4)}{3!} = -4.$$

Taking $u = 1/2$ and $k = 3$

$$\begin{aligned} \binom{1/2}{3} &= \frac{(1/2)(1/2-1)(1/2-2)}{3!} \\ &= (1/2)(-1/2)(-3/2)/6 \\ &= 1/16. \end{aligned}$$

Extended Binomial Coefficient

When u is a negative integer:

$$\begin{aligned}
\binom{-n}{r} &= \frac{(-n)(-n-1)\cdots(-n-r+1)}{r!} \\
&= \frac{(-1)^r n(n+1)\cdots(n+r-1)}{r!} \\
&= \frac{(-1)^r (n+r-1)(n+r-2)\cdots n}{r!} \\
&= \frac{(-1)^r (n+r-1)!}{r!(n-1)!} \\
&= (-1)^r \binom{n+r-1}{r} \\
&= (-1)^r C(n+r-1, r).
\end{aligned}$$

SUSTech Southern University of Science and Technology

Extended Binomial Theorem

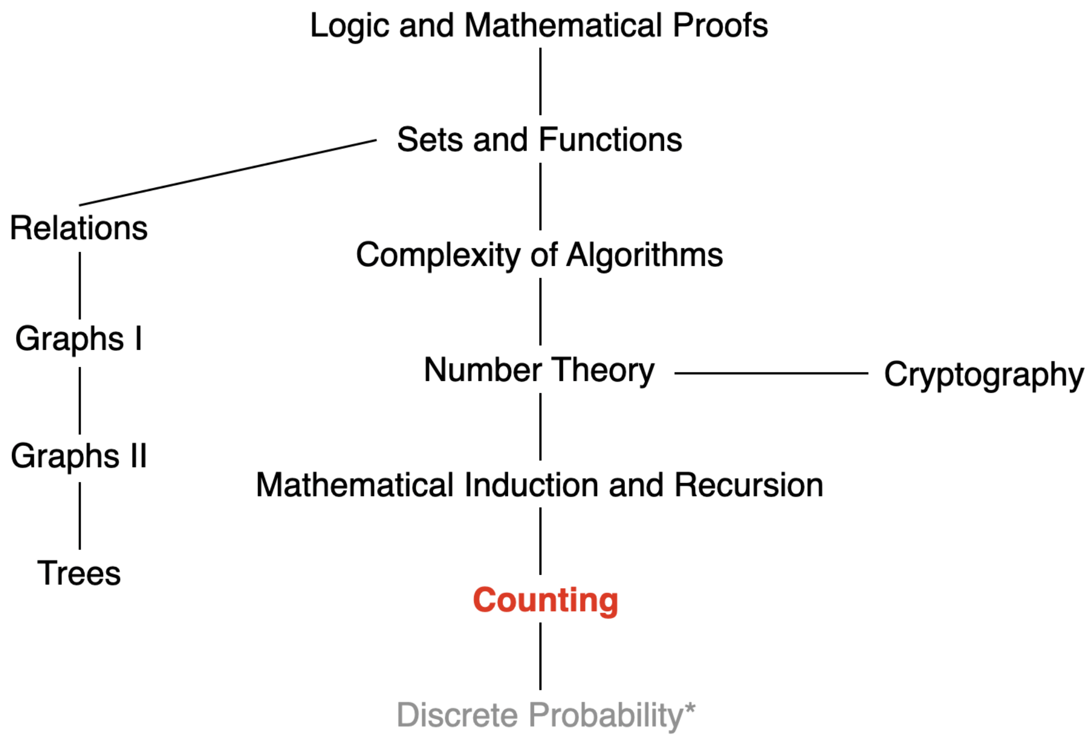
Theorem: Let x be a real number with $|x| < 1$ and let u be a real number. Then,

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k.$$

Example:

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

Next Lecture



Counting basis, Permutations and Combinations, Binomial Coefficients, The Birthday Paradox, Solving Linear Recurrence Relations, Generating Function, ...