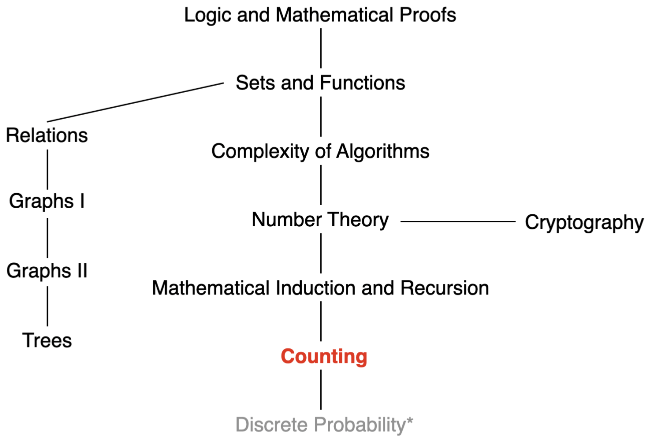
Discrete Mathematics for Computer Science

Lecture 13: Counting

Dr. Ming Tang

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

This Lecture



Counting basis, Permutations, Combinations, ...

The Binomial Theorem

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

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

$$(x+y)^n = \underbrace{(x+y)(x+y)(x+y)\cdots(x+y)}_{\text{a total of } n\ (x+y)\text{'s}}$$

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

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 $\binom{n}{j}$.

Counting and functions ...

- Using counting to expand functions
- Using functions to count $\rightarrow$ generating function

Binomial and Trinomial Coefficients

Binomial coefficient:

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

where $k_1 + k_2 = n$.

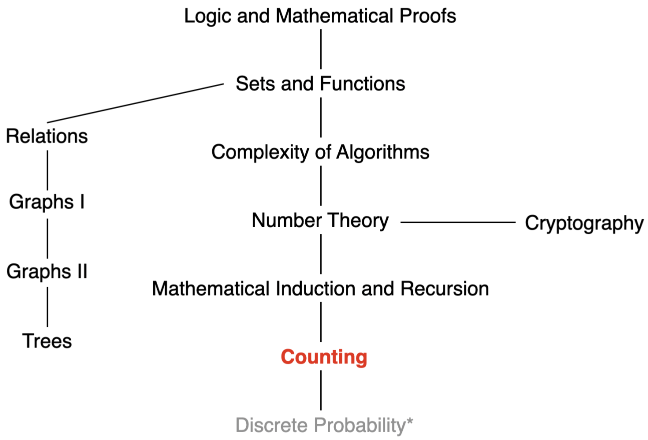
Trinomial coefficient:

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

where $k1 + k2 + k3 = n$.

SUSTech Southern University of Science and Technology

This Lecture



Counting basis, Permutations and Combinations, Binomial Coefficients, The Birthday Paradox, Generalized Permutations and Combinations, Generating Function, 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).
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

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

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

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

Southern University of Science and Technology

"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).

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

- H: the number of available hash values
- n: the number of values we generate using a hash function $f(x)$

Goal: find the minimum n such that the probability of collision is larger than a predefined value.

"Birthday" Attacks

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

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 $e^{-i/H} \approx 1 - \frac{i}{H}$.

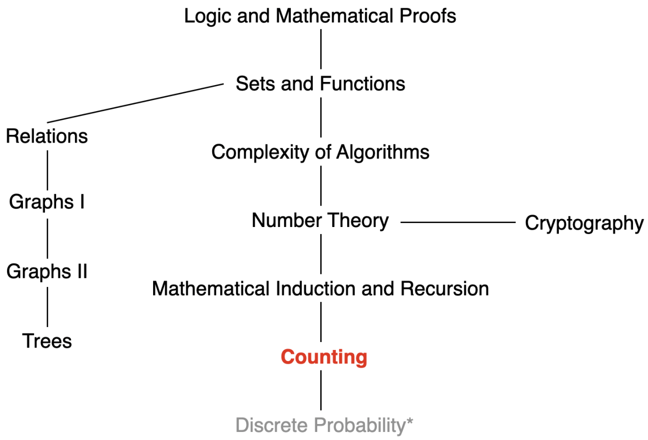
This probability can be approximated as

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

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, Generalized Permutations and Combinations, Generating Function, Solving Linear Recurrence Relations , ...

Generalized Permutations and Combinations

- Permutations with repetition
- Permutations with indistinguishable objects
- Combinations with repetition

Repetition: Distinct objects; each object can be selected multiple times

Indistinguishable objects: E.g., "SUCCESS"

Permutations with Repetition

Example: How many strings of length r can be formed from the uppercase letters of the English alphabet? 26^r

Theorem: The number of r-permutations of a set of n objects with repetition allowed is n^r.

Permutations with Indistinguishable Objects

Example: How many different strings can be made by reordering the letters of the word SUCCESS?

Solution:

- The three S's can be placed among the seven positions in $C(7,3)$ different ways.
- The two C's can be placed in $C(4,2)$ ways.
- The U can be placed in $C(2,1)$ ways.
- The E can be placed in $C(1,1)$ way.

From the product rule,

$$C(7,3)C(4,2)C(2,1)C(1,1) = \frac{7!}{3!2!1!1!} = 420.$$

Permutations with Indistinguishable Objects

Theorem: The number of different permutations of n objects, where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, . . . , and n_k indistinguishable objects of type k, is

$$C(n, n_1)(n - n_1, n_2) \cdots C(n - n_1 - \cdots n_{k-1}, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

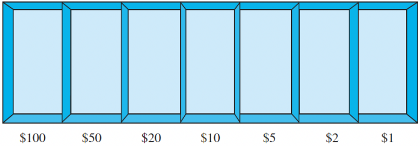
Combinations with Repetition

Example: How many ways are there to select five bills from a cash box containing \$1 bills, \$2 bills, \$5 bills, \$10 bills, \$20 bills, \$50 bills, and \$100 bills?

Assume that the order in which the bills are chosen does not matter, that the bills of each denomination are indistinguishable, and that there are at least five bills of each type.

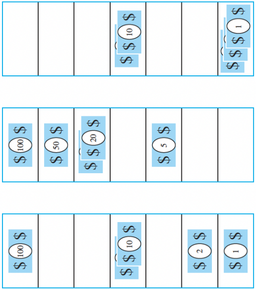
Combinations with Repetition

Solution: Suppose that a cash box has seven compartments, one to hold each type of bill.



- These compartments are separated by six dividers
- The choice of five bills corresponds to placing five markers in the compartments holding different types of bills.

Combinations with Repetition



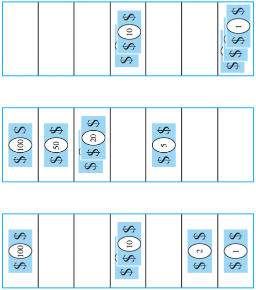
$$\mid\ \mid\ \mid \ast\ast \mid\ \mid\ \mid \ast\ast\ast$$

$$\ast \mid \ast \mid \ast\ast \mid\ \mid \ast \mid\ \mid$$

$$\ast \mid\ \mid\ \mid \ast\ast \mid\ \mid \ast \mid \ast$$

The number of ways to select five bills corresponds to the number of ways to arrange six bars and five stars in a row with a total of 11 positions.

Combinations with Repetition



$| \; | \; | \; * \; * \; | \; | \; | \; * \; * \; *$

$* \; | \; * \; | \; * \; * \; | \; | \; * \; | \; |$

$* \; | \; | \; | \; * \; * \; | \; | \; * \; | \; *$

Consequently, the number of ways to select the five bills is the number of ways to select the positions of the five stars from the 11 positions.

$$C(11, 5) = \frac{11!}{5!6!} = 462$$

Combinations with Repetition

Theorem: There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set with n elements when repetition of elements is allowed.

In the previous example:

- Selecting five bills: $r = 5$
- Seven types of bills: $n = 7$

Combinations with Repetition: Example

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?

Solution: This is equivalent to finding the number of ways of selecting 11 items from three types of items, so that x_1 items of type one, x_2 items of type two, and x_2 items of type three:

$$C(3 + 11 - 1, 11) = 78$$

Combinations with Repetition: Example

How many solutions does the equation

$$x_1 + x_2 + x_3 = 11$$

have, where $x_1 \geq 1$, $x_2 \geq 2$, and $x_3 \geq 3$ are nonnegative integers?

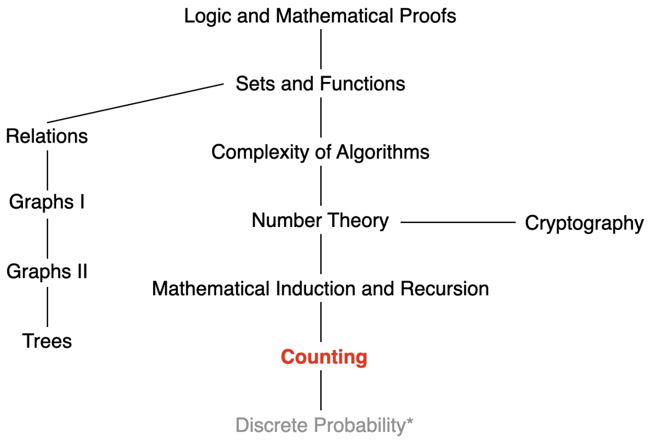
Solution: A solution corresponds to a selection of 11 items with x_1 items of type one, x_2 items of type two, and x_3 items of type three:

- At least one item of type one, two items of type two, and three items of type three.

A solution corresponds to a choice of one item of type one, two of type two, and three of type three, together with a choice of five additional items of any type.

$$C(3+5-1, 5) = 21$$

This Lecture



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

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 $a_k = 2^k$

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

SUSTech Southern University of Science and Technology

Generating Function

Generating function can be written in simpler forms:

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

$$1/(1 - x) = 1 + x + x^2 + ...$$

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

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

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

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

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 sequence $\{a_n\}$ is a polynomial of degree n, i.e.,

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

Generating Function: Example

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

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

Based on binomial theorem, this generating function has a simpler form: $G(x) = (1+x)^m = C(m,0) + C(m,1)x + C(m,2)x^2 + ... + C(m,m)x^m$.

Example: Generating function of 1,1,1,1,1,1?

$$1 + x^2 + x^3 + x^4 + x^5.$$

Based on the summation of geometric sequence,

$$1 + x^2 + x^3 + x^4 + x^5 = \frac{x^6 - 1}{x - 1}.$$

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,

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

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

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

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

SUSTech Southern University of Science and Technology

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

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

Useful Generating Functions

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

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

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

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

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

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

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

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

Useful Generating Functions

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

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

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

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 can be 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:

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

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:

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

Generating Function

Generating function and counting ...

Generating Function and Combinations with Repetitions

Recall the following example:

How many solutions does the equation

$$x_1 + x_2 + x_3 = 11$$

have, where $x_1 \geq 1$, $x_2 \geq 2$, and $x_3 \geq 3$ are nonnegative integers?

This type of counting problem can be solved with generating function.

Generating Function and Combinations with Repetitions

Formally, generating functions can also be used to solve counting problems of the following type:

$$e_1 + e_2 + \cdots + e_n = C,$$

where C is a constant and each e_i is a nonnegative integer that may be subject to a specified constraint.

SUSTech Southern University of Science and Technology

Example 1

Find the number of solutions of

$$e_1 + e_2 + e_3 = 17,$$

where e_1, e_2, and e_3 are nonnegative integers with $2 \leq e_1 \leq 5$, $3 \leq e_2 \leq 6$, and $4 \leq e_3 \leq 7$.

Solution: The number of solutions with the indicated constraints is the coefficient of x^{17} in the expansion of

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

By enumerating all possibilities, we have that the coefficient of x^{17} in this product is 3.

Example 2

In how many different ways can eight identical cookies be distributed among three distinct children if each child receives at least two cookies and no more than four cookies?

Solution: This corresponds to the coefficient of x^8 of expansion

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

This coefficient equals 6.

Example 3

Use generating functions to determine the number of ways to insert tokens worth \$1, \$2, and \$5 into a vending machine to pay for an item that costs r dollars in the cases

- Case 1: when the order does not matter

  E.g., three \$1 tokens; one \$1 token and a \$2 token

- Case 2: when the order does matter

  E.g., three \$1 tokens; a \$1 token and then a \$2 token; a \$2 token and then a \$1 token

Example 3

Case 1: when the order does not matter
The answer is the coefficient of x^r in the generating function

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

Case 2: when the order does matter
The number of ways to insert exactly n tokens to produce a total of r dollars is the coefficient of x^r in

$$(x + x^2 + x^5)^n$$

Because any number of tokens may be inserted,

$$1 + (x + x^2 + x^5) + (x + x^2 + x^5)^2 + \cdots = \frac{1}{1 - (x + x^2 + x^5)}$$

Example 4

Use generating functions to find the number of r-combinations of a set with n elements.

Solution: The answer is the coefficient of x^r in generating function

$$(1+x)^n$$

But by the binomial theorem, we have

$$f(x) = \sum_{r=0}^{n} \binom{n}{r} x^r.$$

Thus, $\binom{n}{r}$ is the answer.

Example 5

Use generating functions to find the number of r-combinations from a set with n elements when repetition of elements is allowed.

Solution: The answer is the coefficient of x^r in generating function

$$G(x) = (1 + x + x^2 + \cdots)^n.$$

As long as $|x| < 1$, we have $1 + x + x^2 + \cdots = 1/(1 - x)$, so

$$G(x) = 1/(1 - x)^n = (1 - x)^{-n}.$$

Applying the extended binomial theorem

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

Hence, the coefficient of x^r equals $\binom{-n}{r}(-1)^r = C(n + r - 1, r)$.

Example 6

Use generating functions to find the number of ways to select r objects of n different kinds if we must select at least one object of each kind.

Solution: The answer is the coefficient of x^r in generating function

$$G(x) = (x + x^2 + x^3 + \cdots)^n = x^n(1 + x + x^2 + \cdots)^n = x^n/(1-x)^n.$$

$$\begin{aligned} G(x) &= x^n/(1-x)^n \\ &= x^n \cdot (1-x)^{-n} \\ &= x^n \sum_{r=0}^{\infty} \binom{-n}{r} (-x)^r \\ &= x^n \sum_{r=0}^{\infty} (-1)^r C(n+r-1, r)(-1)^r x^r \end{aligned} \qquad \begin{aligned} &= \sum_{r=0}^{\infty} C(n+r-1, r) x^{n+r} \\ &= \sum_{t=n}^{\infty} C(t-1, t-n) x^t \\ &= \sum_{r=n}^{\infty} C(r-1, r-n) x^r. \end{aligned}$$

Hence, there are $C(r-1, r-n)$ ways to select r objects of n different kinds if we must select at least one object of each kind.

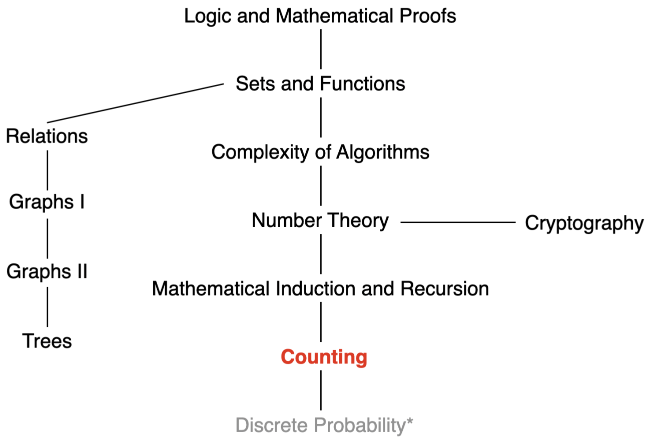
Generating Function and Combinations with Repetitions

- Based on the combination problem, transfer the problem as finding the coefficient of x^r of a generating function, e.g.,

$$G(x) = (1 + x + x^2 + x^3 + \cdots)^n$$

- Find the coefficient of x^r
  - Enumerate all possibilities or
  - Use useful generating functions

Next Lecture



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