Discrete Mathematics for Computer Science

Lecture 12: Counting

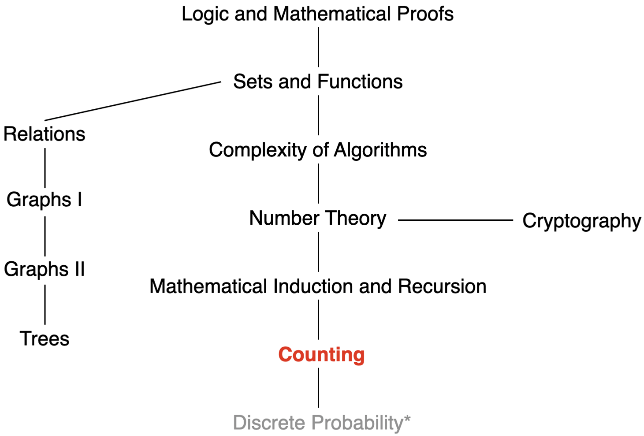
Dr. Ming Tang

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

Pigeonhole principle: Example

Let (x_i, y_i, z_i), $i = 1, 2, 3, 4, 5, 6, 7, 8, 9$ be a set of nine distinct points with integer coordinates in xyz space. Show that the midpoint of at least one pair of these points has integer coordinates.

This Lecture



Counting basis, Permutations, Combinations, ...

Combinations

An r-combination of elements of a set is an unordered selection of r elements from the set.

The number of r-combinations of a set with n distinct elements is denoted by $C(n, r)$.

Note that $C(n, r)$ is also denoted by $\binom{n}{r}$ and is called a binomial coefficient.

Example: The 2-combinations of $\{a, b, c, d\}$ are the six subsets $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, and $\{c, d\}$. Thus, $C(4, 2) = 6$.

Binomial Coefficient

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

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

Proof: The $P(n,r)$ r-permutations of the set can be obtained by

- forming the $C(n,r)$ r-combinations of the set.
- ordering the elements in each r-combination, which can be done in $P(r,r)$ ways.

By the product rule,

$$P(n,r) = C(n,r)P(r,r).$$

Some Properties of Binomial Coefficients

- $C(n, 0) = 1$: one set of size 0.
- $C(n, n) = 1$: one set of size n.
- $C(n, r) = C(n, n - r)$

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

$$C(n, n-r) = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{r!(n-r)!}$$

Any other ideas to prove?

We will address this later.

Combinations: Example

Example 1: How many ways are there to select five players from a 10-member tennis team to make a trip to a match at another school?

$C(10,5) = \frac{10!}{5!5!} = 252.$

Example 2: There are 9 faculty members in the mathematics department and 11 in the computer science department.

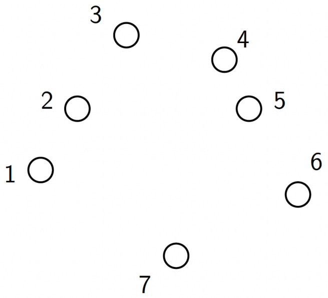
How many ways are there to form a committee with 3 faculty members from the mathematics department and 4 from the computer science department?

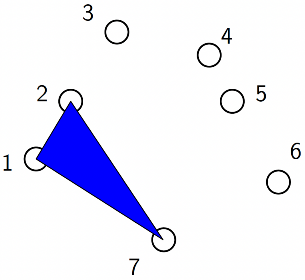
$C(9,3) \cdot C(11,4) = \frac{9!}{3!6!} \cdot \frac{11!}{4!7!} = 27,720.$

Example: Counting Triangle

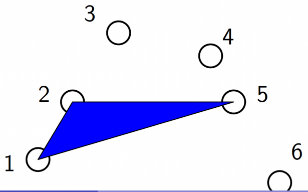
Design an algorithm to count the number of triangles formed by n points in the plane:

- 3 points form a triangle if and only if they are non-collinear





1 — 2 — 7: yes



1 — 2 — 7: yes

1 — 2 — 5: yes

Example: Counting Triangle

The following loop is a part of the program to determine the number of triangles formed by *n* points in the plane:

```
(1) trianglecount = 0
(2)   for i = 1 to n
(3)     for j = i+1 to n
(4)       for k = j+1 to n
(5)         if points i, j, k are not collinear
(6)           trianglecount = trianglecount + 1
```

Question: Among all iterations of line 5, what is the total number of times this line checks three points to see if they are collinear?

This corresponds to the total number of combinations. Why?

Example: Counting Triangle

```
(1) trianglecount = 0
(2)   for i = 1 to n
(3)     for j = i+1 to n
(4)       for k = j+1 to n
(5)         if points i, j, k are not collinear
(6)           trianglecount = trianglecount + 1
```

- First loop begins with $i = 1$ and i increases up to n.
- Second loop begins with $j = i + 1$ and j increases up to n.
- Third loop begins with $k = j + 1$ and k increases up to n.

Thus each triple i, j, k with $i < j < k$ is examined exactly once.

For example, if $n = 4$, then triples (i, j, k) used by algorithm are $(1, 2, 3)$, $(1, 2, 4)$, $(1, 3, 4)$, and $(2, 3, 4)$.

Example: Counting Triangle

Want to compute the number of increasing triples (i, j, k) with $1 \leq i < j < k \leq n$.

Claim: The number of increasing triples is exactly the same as the number of 3-combinations from $\{1, 2, ..., n\}$. Why?

- X: set of increasing triples
- Y: set of 3-combinations from $\{1, 2, ..., n\}$

Define: $f : X \to Y$ by $f((i, j, k)) = \{i, j, k\}$

Claim: f is a bijection, so $|X| = |Y|$.

Example: Counting Triangle

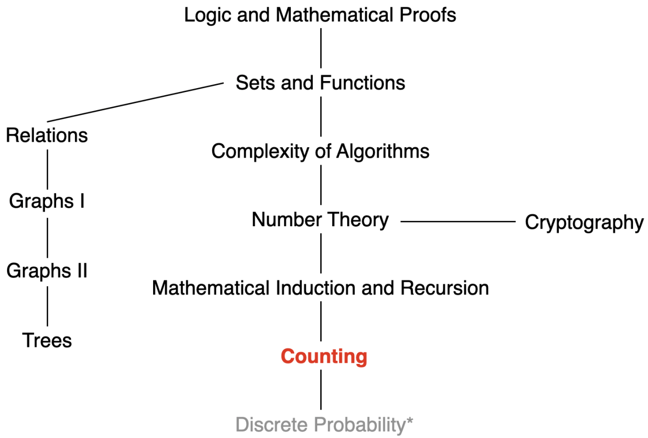
- X: set of increasing triples
- Y: set of 3-combinations from $\{1, 2, ..., n\}$

Define: $f : X \to Y$ by $f((i, j, k)) = \{i, j, k\}$

Claim: f is a bijection, so $|X| = |Y|$.

- One-to-one: if $f((i, j, k)) = f((i', j', k'))$, then $(i, j, k) = (i', j', k')$.
- Onto: for any $\{i, j, k\}$, there exists a (i, j, k) such that $f((i, j, k)) = \{i, j, k\}$.

This Lecture



Counting basis, Permutations and Combinations, Binomial Coefficients, ...

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.

Combinatorial Proof: Bijective Proof

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

Bijective Proof: Suppose that S is a set with n elements.

The function that maps a subset A of S to $\bar{A}$ is a bijection between subsets of S with r elements and subsets with $n - r$ elements.

- X: the set of all possible A, where $|X| = C(n, r)$
- Y: the set of all possible $\bar{A}$, where $|Y| = C(n, n - r)$
- $f : X \to Y$ is defined as $f(A) = \bar{A}$
  - One-to-one: if $f(A_1) = f(A_2)$, then $A_1 = A_2$.
  - Onto: for any $\bar{A}$, there exists an A such that $f(A) = \bar{A}$.

Since there is a bijection between two finite sets X and Y, they must have the same number of elements. Thus, $C(n, r) = C(n, n - r)$.

Combinatorial Proof: Double Counting Proof

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

Double Counting Proof:

- Left-hand side $C(n,r)$: The number of subsets A of S with r elements.
- Right-hand side $C(n,n-r)$: The number of subsets $\bar{A}$ (i.e., the complement of A) of S with $n-r$ elements.

Each subset A of S is also determined by specifying which elements are not in A, so are in $\bar{A}$. Thus, both sides count the same thing

It follows that $C(n,r) = C(n,n-r)$.

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 $\binom{n}{j}$.

The Binomial Theorem: Example

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

Example 1: What is the expansion of $(x+y)^4$?

$$\begin{aligned}(x+y)^4 &= \sum_{j=0}^{4} \binom{4}{j} x^{4-j} y^j \\ &= \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} x y^3 + \binom{4}{4} y^4 \\ &= x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4.\end{aligned}$$

The Binomial Theorem: Example

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

Example 2: What is the coefficient of $x^{12}y^{13}$ in the expansion of $(2x-3y)^{25}$?

First, note that this expression equals $(2x+(-3y))^{25}$

$$(2x+(-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j.$$

The coefficient of $x^{12}y^{13}$ in the expansion is obtained when $j=13$:

$$\binom{25}{13} 2^{12} (-3)^{13} = -\frac{25!}{13!\,12!} 2^{12} 3^{13}.$$

The Binomial Theorem

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

Corollary: Let n be a nonnegative integer,

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

This is proven by substituting $x = 1$ and $y = 1$.
Any other ideas to prove?

The Binomial Theorem

Corollary: Let n be a nonnegative integer,

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

Double Counting Proof: Let P denote the set of all subsets of $\{1, 2, ..., n\}$.

- Left-hand side: Let S_k be the set of all subsets of $\{1, 2, ..., n\}$ with k elements.

$$|P| = \sum_{k=0}^{n} |S_k| = \sum_{k=0}^{n} \binom{n}{k}$$

- Right-hand side: A set with n elements has a total of 2^n different subsets, i.e., $|P| = 2^n$.

SUSTech Southern University of Science and Technology

The Binomial Theorem

Corollary: Let n be a nonnegative integer,

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

Bijective Proof: Let P denote the set of all subsets of $\{1, 2, ..., n\}$. Let S_k be the set of all subsets of $\{1, 2, ..., n\}$ with k elements.

$$|P| = \sum_{i=0}^{n} |S_k| = \sum_{i=0}^{n} \binom{n}{k}$$

Consider $L = L_1 L_2 ... L_n$ be a list of size n from $\{0, 1\}$. Let $\mathcal{L}$ be the set of all such lists, we have $|\mathcal{L}| = 2^n$.

Objective: there is a bijection between $\mathcal{L}$ and P, so $|P| = |\mathcal{L}| = 2^n$.

The Binomial Theorem

Define the following function $f : \mathcal{L} \to P$

- If $L \in \mathcal{L}$, then $f(L)$ is the set $S \subset \{1, 2, ..., n\}$ defined by

$$i \in S, \text{for } L_i = 1$$

f is a bijection between $\mathcal{L}$ and P.

- one-to-one: If $f(L_1) = f(L_2)$, then $L_1 = L_2$
- onto: for any S, there exists an L such that $f(L) = S$

The Binomial Theorem

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

Corollary: Let n be a positive integer.

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

This is proven by substituting $x = -1$ and $y = 1$.

Corollary: Let n be a nonnegative integer.

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$$

This is proven by substituting $x = 1$ and $y = 2$.

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., $\binom{n}{k}$.

SUSTech Southern University of Science and Technology

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

$$
\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0}\ \binom{1}{1} \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} \\
\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5} \\
\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6} \\
\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7} \\
\binom{8}{0}\ \binom{8}{1}\ \binom{8}{2}\ \binom{8}{3}\ \binom{8}{4}\ \binom{8}{5}\ \binom{8}{6}\ \binom{8}{7}\ \binom{8}{8} \\
\cdots
\end{array}
$$

By Pascal's identity:

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

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1 \\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \\
\cdots
\end{array}
$$

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

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

Combinatorial Proof: Example

$$\sum_{k=1}^{n} k \binom{n}{k} = n2^{n-1}.$$

Hint: Consider a set of people, and count the number of ways to select a committee and select one leader within the committee.

- Left-hand side: Suppose there are k people in a committee.
  - First select k people from the n people to form a committee.
  - Then, given the people in the committee, select a leader from the committee, i.e., k ways.

  Thus, there are a total of $\sum_{k=1}^{n} k \binom{n}{k}$ ways.
- Right-hand side:
  - There are n ways to choose a leader.
  - Then, each person other than the leader can be either in the committee or not, i.e., 2^{n-1} ways.

  Hence, using product rule, there are $n2^{n-1}$ ways.

Combinatorial Proof: Example

Use combinatorial proof to show that when integer $n \geq 2$, then

$$\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} 1 = \binom{n}{2}.$$

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 $n - k_1$.

$$\begin{aligned}\binom{n}{k_1}\binom{n-k_1}{k_2} &= \frac{n!}{k_1!(n-k_1)!}\frac{(n-k_1)!}{(k_2)!(n-k_1-k_2)!} \\ &= \frac{n!}{k_1!k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!}\end{aligned}$$

This is called a trinomial coefficient and denote it as

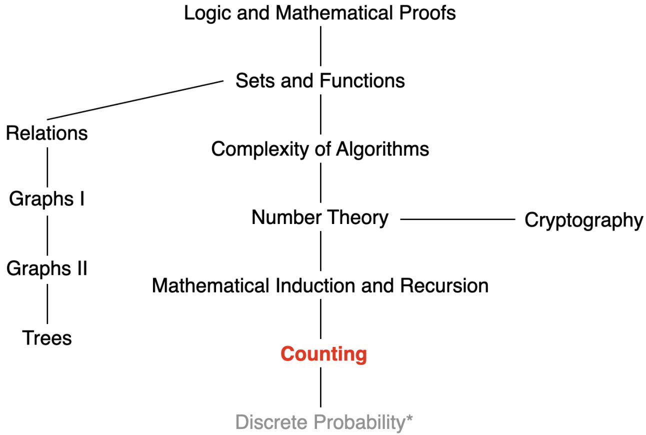
$$\binom{n}{k_1 \quad k_2 \quad k_3} = \frac{n!}{k_1!k_2!k_3!},$$

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

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

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

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

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

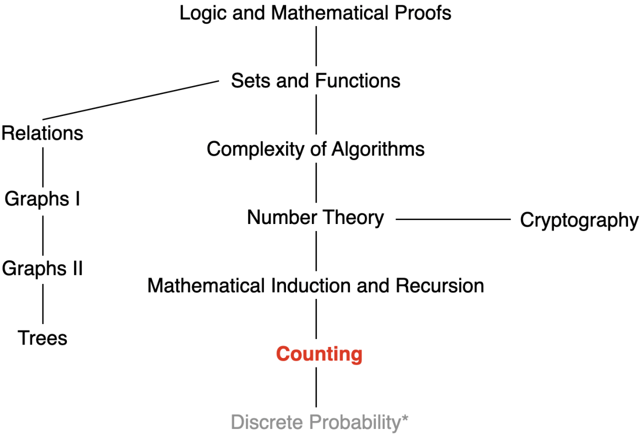
This probability can be approximated as

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

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

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

Next Lecture



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

Use strong induction to prove that $\sqrt{2}$ is irrational.

- To prove the above, we need to first consider the statement $P(n)$ that we need to prove. Write this statement $P(n)$: ____________
- Prove the above statement using strong induction. Suppose we know $\sqrt{2} > 1$.

Solution:

- $P(n)$: there is no positive integer b such that $\sqrt{2} = n/b$.
- Basic step: $P(1)$ is true, because $\sqrt{2} > 1 > 1/b$.
- Inductive step: Suppose $P(j)$ is true for all $j \leq k$, where k is an arbitrary positive integer. We prove that $P(k+1)$ is true by contradiction.

Mathematical Induction

Use strong induction to prove that $\sqrt{2}$ is irrational.

- $P(n)$: there is no positive integer b such that $\sqrt{2} = n/b$
- Prove the above statement using strong induction. Suppose we know $\sqrt{2} > 1$.

Solution:

- Inductive step: Suppose $P(j)$ is true for all $j \leq k$, where k is an arbitrary positive integer. We prove that $P(k+1)$ is true by contradiction.

  Suppose $P(k+1)$ is false. Then, there exists a b such that $\sqrt{2} = (k+1)/b$. Thus, $2b^2 = (k+1)^2$, so $(k+1)^2$ must be even, and hence $k+1$ must be even. This implies $k+1 = 2t$ for some positive integer t. Substituting $k+1$, we have $2b^2 = 4t^2$, so $b = 2s$ for some positive integer s. This implies that $\sqrt{2} = (k+1)/b = 2t/(2s) = t/s$. That is, when $n = t$, there exists an s such that $\sqrt{2} = t/s$. However, since $t < k+1$, this statement is contradict with $P(t)$ is true.

Mathematical Induction

Suppose there are n people in a group, each aware of a secrete no one else in the group knows about. These people communicate by telephone; when two people in the group talk, they share information about all secrete each knows about. For example, consider three people A, B, C with secrete S_A, S_B, S_C, respectively:

- On the first call, A and B communicate. Then, both A and B know about secrets $\{S_A, S_B\}$.
- On the second call, A and C communicate. Then, both A and C knows about secrets $\{S_A, S_B, S_C\}$.

The gossip problem asks for $G(n)$, the minimum number of telephone calls that are needed for **all** n **people** to learn about **all the secrete**.

(a) Find $G(1)$, $G(2)$, $G(3)$, and $G(4)$.

(b) Use mathematical induction to prove that $G(n) \leq 2n - 4$ for all $n \geq 4$.

Mathematical Induction

Solution:

(a) $G(1) = 0,\ G(2) = 1,\ G(3) = 3,\ G(4) = 4.$

(b) Let $P(n)$: $G(n) \leq 2n - 4$ for all $n \geq 4$.

- Basic Step: $G(4) = 4 \leq 2 \times 4 - 4 = 4$.
- Inductive Step: Suppose $G(n) \leq 2n - 4$ for all $n \geq 4$. Now consider $n + 1$ people. Let $\mathcal{N}$ denote a set of n people, and let r denote the remaining one person. Let k denote an arbitrary person in set $\mathcal{N}$.
  - ★ r and k communicate by telephone: takes 1 calls; k knows the secret of S_r
  - ★ the people in set $\mathcal{N}$ communicate: by inductive hypothesis, takes $G(n) \leq 2n - 4$ calls; everyone in set $\mathcal{N}$ knows every secrete of $\{S_i \mid i \in \mathcal{N} \cup \{r\}\}$
  - ★ r and k communicate by telephone: takes 1 calls; r knows the secret of $\{S_i \mid i \in \mathcal{N} \cup \{r\}\}$

  In total, it takes $G(n+1) \leq 2n - 4 + 2 = 2(n+1) - 4$ calls. The proof completes.