CSCE 222
Discrete Structures for Computing

Counting

Dr. Hyunyoung Lee

Based on slides by Andreas Klappenecker

Counting

The art of counting is known as enumerative combinatorics. One tries to count the number of elements in a set (or, typically, simultaneously count the number of elements in a series of sets).

For example, let S_1, S_2, S_3, ... be sets with 1, 2, 3, ... elements, respectively. Then the number of subsets of S_i is given by $f(i)=|P(S_i)|=2^i$.

The basic principles are extremely simple, but counting is a nontrivial task.

The Product Rule

Suppose that a task can be broken down into a sequence of two subtasks. If there are n_1 ways to solve subtask 1 and n_2 ways to solve subtask 2, then there must be $n_1 n_2$ ways to solve the task.

Let S_1 and S_2 be sets describing the ways of the first and second subtasks, so $n_1 = |S_1|$ and $n_2 = |S_2|$.

Then $|S_1 \times S_2| = n_1 n_2$.

Product Rule: Example 1

How many different license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits (and no sequence of letters are prohibited).

There are 26 choices for each of the three uppercase letters, and 10 choices for each of the three digits. Thus,

26 x 26 x 26 x 10 x 10 x 10 = 17,576,000

possible license plates. Since Texas has already a population of 29,366,479, this is perhaps not a good choice here.

Product Rule: Example 2

How many functions are there from a set with m elements to a set with n elements?

For each of the m elements in the domain, we can choose any element from the codomain as a function value. Hence, by the product rule, we get

$$n \times n \times \ldots \times n = n^m$$

different functions.

Product Rule: Example 3

How many injective functions are there from a set with m elements to a set with n elements?

If $m > n$, then there are 0 injective functions.

If $m \le n$, then there are n ways to choose the value for the first element in the domain, n-1 ways to choose the value for the second element (as one has to avoid the previously chosen value), n-2 for the third element of the domain and so forth. Thus, we have $n(n-1)\ldots(n-m+1)$ injective functions in this case.

Sum Rule

If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Let S_1 and S_2 be disjoint sets with $n_1=|S_1|$ and $n_2=|S_2|$. Then $|S_1 \cup S_2| = n_1+n_2$.

Sum Rule: Example 1

A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one lists. How many possible projects are there to choose from?

There are 23+15+19=57 projects to choose from.

Sum Rule: Example 2

How many sequences of 1s and 2s sum to n?

Let us call the answer to this question a_n.

$a_0 = 1$ { one sequence, namely the empty sequence () }

$a_1 = 1$ { one sequence, namely (1) }

$a_2 = 2$ { the sequences (1,1) and (2) }

$a_3 = 3$ { the sequences (1,1,1), (1,2), and (2,1) }

$a_4 = 5$ { the sequences (1,1,1,1), (1,1,2), (1,2,1), (2,1,1), and (2,2) }

Sum Rule: Example 2 (Cont.)

How many sequences of 1s and 2s sum to n?

Let us call the answer to this question a_n.

$a_0 = 1$, $a_1 = 1$

$a_n = a_{n-1} + a_{n-2}$ for $n >= 2$

Indeed, there are

- a_{n-1} sequences starting with 1 (remaining seq. summing to n-1)
- a_{n-2} sequences starting with 2 (remaining seq. summing to n-2)

Thus, by the sum rule $a_n = a_{n-1} + a_{n-2}$

Defining $a_{-1}=0$, we get $a_n=f_{n+1}$ where f_n is the Fibonacci sequence.

IPv4 Address Example

Computer addresses belong to one of the following 3 types:

- Class A: address contains a 7-bit “netid” $\neq 1^7$, and a 24-bit “hostid”
- Class B: address has a 14-bit netid and a 16-bit hostid.
- Class C: address has 21-bit netid and an 8-bit hostid.

Bit Number	0	1	2	3	4	8	16	24	31
Class A	0	netid				hostid			
Class B	1	0	netid				hostid		
Class C	1	1	0	netid				hostid	

Hostids that are all 0s or all 1s are not allowed.

How many valid computer addresses are there?

IPv4 Address Example (Cont.)

- (# addrs) = (# class A) + (# class B) + (# class C)

  (by sum rule)
- # class A = (# valid netids)·(# valid hostids)

  (by product rule)
- (# valid class A netids) = $2^7 - 1 = 127$.
- (# valid class A hostids) = $2^{24} - 2 = 16,777,214$.

Continuing in this fashion we find the answer is:
3,737,091,842 (3.7 billion IP addresses)

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 is common to the two different ways.

Principle of Inclusion-and-Exclusion:

Let S_1 and S_2 be sets. Then

$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|$

Subtraction Rule: Example 1

How many bit strings of length 8 either start with a 1 bit or end with the last two bits equal to 00 ?

Let S_1 be the set of bit strings of length 8 that start with 1.

Then $|S_1| = 2^7 = 128$.

Let S_2 be the set of bit strings of length 8 that end with 00.

Then $|S_2| = 2^6 = 64$.

Furthermore, the set of bit strings of length 8 that start with bit 1 and end with bits 00 has cardinality $|S_1 \cap S_2| = 2^5 = 32$.

Thus, the answer is $|S_1 \cup S_2|=|S_1|+|S_2|-|S_1 \cap S_2|=128+64-32=160$.

Subtraction Rule: Example 2

Let us consider some (slightly simplified) rules for passwords:

Passwords must be 2 characters long.

Each character must be

a) a letter [a-z],

b) a digit [0-9], or

c) one of the 10 special characters [!@#$%^&*()].

Each password must contain at least 1 digit or special character.

Subtraction Rule: Example 2 (Cont.)

A legal password has a digit or a special character in position 1 or position 2.

These cases overlap, so the subtraction rule applies.

(# of passwords with valid symbol in position #1) =

$$(10+10)\cdot(10+10+26) = 20\cdot 46$$

(# of passwords with valid symbol in position #2) = $20\cdot 46$

(# of passwords with valid symbols in both places) = $20\cdot 20$

Answer: $920+920-400 = 1{,}440$

Pigeonhole Principle

If k+1 objects are assigned to k places, then at least one place must be assigned at least two objects.

Generalized Pigeonhole Principle

Theorem: If N > k objects are assigned to k places, then at least one place must be assigned at least $\lceil N/k \rceil$ objects.

Proof: Seeking a contradiction, suppose every place has less than $\lceil N/k \rceil$ objects; so at most ≤ $\lceil N/k \rceil - 1$ objects per place.

Then the total number of objects is at most

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k} + 1\right) - 1\right) = k\,(N/k) = N$$

Thus, there are fewer than N objects total, contradicting our assumption on the total number of objects.

Pigeonhole Principle: Example 1

Suppose that there are 90 students in a class X. Then there must exist a week during which

$$\lceil 90/52 \rceil = 2$$

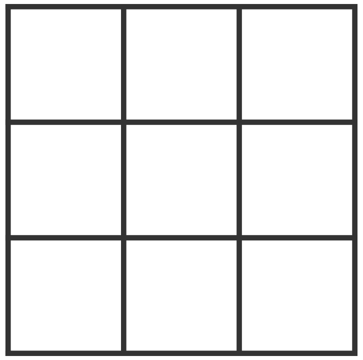
students of class X have a birthday.

Pigeonhole Principle: Example 2

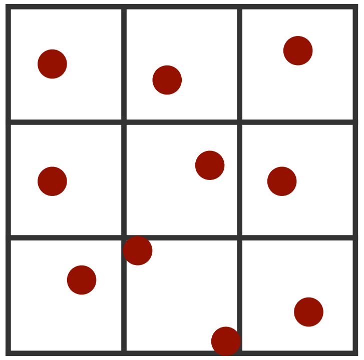
Ten points are given within a square of unit size. Then there are two points that are closer to each other than 0.48.

Proof: Let us partition the square into nine squares of side length 1/3, see Figure (a) below.

(a)



(b)



By the pigeonhole principle, one square must contain at least 2 points, see Figure (b). The distance of two points within a square of side length 1/3 is at most $(2/9)^{1/2}$ by Pythagoras' theorem. The claim follows, since $(2/9)^{1/2} < 0.471405 < 0.48$.

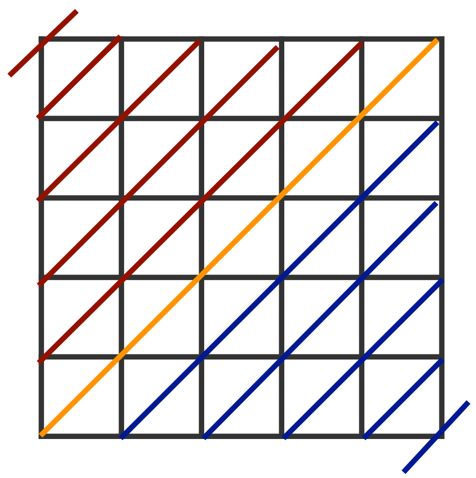
Counting in Two Different Ways Rule

When two different formulas enumerate the same set, then they must be the same.

[In other words, you count the elements of the set in two different ways.]

Double Counting: Example

Take an array of (n+1) x (n+1) dots. Thus, it contains $(n+1)^2$ dots.



Counting the points on the main diagonal, the upper diagonals, and the lower diagonals, we get

$$(n+1)^2 = (n+1) + \sum_{i=1}^{n} i + \sum_{i=1}^{n} i$$

$$\Longrightarrow n(n+1) = (n+1)^2 - (n+1) = 2\sum_{i=1}^{n} i$$

$$\Longrightarrow \frac{n(n+1)}{2} = \sum_{i=1}^{n} i$$

Permutations and Combinations

Permutations

Let S be a set with n elements. An ordered arrangement of r elements of S is called an r-permutation of S. A permutation of S is an n-permutation.

The number of r-permutations of a set with n elements is denoted by P(n,r).

Example: S = {1,2,3,4}. Then (2,4,3) and (4,3,2) are two distinct 3-permutations of S. Order matters here!

Number of r-Permutations

Theorem: Let n and r be positive integers, r <= n.

Then $P(n,r) = n(n-1) \dots (n-r+1)$.

Proof: Let S be a set with n elements. The first element of the permutation can be chosen in n ways, the second in n-1 ways, ..., the r-th element can be chosen in (n-r+1) ways. The claim follows by the product rule.

Number of r-Permutations

Corollary: Let n be a positive integer, and r an integer in the range $0 <= r <= n$.

Then $P(n,r) = n!/(n-r)!$

Proof: For r in the range $1 <= r <= n$, this follows from the previous theorem and the fact that

$n!/(n-r)! = n(n-1) \ldots (n-r+1)$.

For r=0, we have $P(n,0)=1$, which equals $n!/(n-0)! = n!/n! = 1$.

Permutation Example

How many permutations of the letters ABCDEFGH contain the string ABC?

Let us regard ABC, D, E, F, G, and H as blocks. Any permutation of these six blocks will yield a valid permutation containing ABC, and there are no others. Therefore, we have 6!=720 permutations of the letters ABCDEFGH that contain ABC as a block.

Combinations

Let S be a set of n elements. An r-combination of S is a subset of r elements from S.

The number of r-combinations of a set S with n elements is denoted by

C(n,r) or $\binom{n}{r}$.

Number of r-Combinations

Theorem: The number of r-combinations of a set with n elements is given by

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

Proof. We can form all r-permutations of a set with n elements by first choosing an r-combination and then ordering the r elements in all possible ways. Thus, P(n,r)=C(n,r)P(r,r).

Hence, C(n,r)=P(n,r)/P(r,r)=n!/(n-r)!/r!/(r-r)!.

Since (r-r)!=0!=1, this yields our claim.

Binomial Coefficient Identity

Corollary: We have $\binom{n}{r} = \binom{n}{n-r}$

Proof: Let S be a set with n elements. Each subset A of S is determined by its complement A^c, which specifies the elements of S that are not contained in A. Therefore, we can use double counting:

The number C(n,r) of subsets of cardinality r of S corresponds to the number of "complements of subsets of cardinality r in S". Since $|A|=r$ iff $|A^c|=n-r$, the complements of subsets of cardinality r of S correspond to subsets of cardinality n-r of S.

Thus, C(n,r) = # of r-subsets of S

= # of complements of r-subsets of S = C(n,n-r), as claimed.

Counting Subset Identity

Theorem: For any nonnegative integer n, we have

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

Proof: Let S be a set with n elements. The number of subsets of S is 2^n. The number of subsets with 0, 1, 2,..., n elements is given by

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}$$

Since subsets of S need to have between 0 and n elements, the claim of the theorem follows.

Binomial Theorem

Theorem: Let x and y be variables. Let n be a nonnegative integer. Then

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

Proof: Let us expand the left hand side. The terms of the product in expanded form are $x^k y^{n-k}$ for $0 <= k <= n$.

To obtain the term $x^k y^{n-k}$ one must choose k x's from the n (x+y) terms. There are $\binom{n}{k}$ ways to do that.

Another Binomial Coefficient Identity

Corollary: Let n be a positive integer. Then

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

Proof: We have $0 = 0^n = (-1+1)^n$. Expanding the right hand side with the help of the binomial theorem, we obtain the claim.

[This implies that the number of subsets with an even number of elements is equal to the number of subsets with an odd number of elements.]

Pascal's Identity (1)

Theorem: Let n and k be positive integers with n>=k. Then

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

Proof: We are going to prove this by counting the number of subsets with k elements of a set T with n+1 elements in two different ways.

First way of counting:

The set T clearly contains $\binom{n+1}{k}$ subsets of size k.

Pascal's Identity (2)

Second way of counting:

Recall that T is a set with n+1 elements. Let us consider an element t of T. We will count the subsets of T of size k that (a) contain the element t, and (b) do not contain the element t.

(a) There are $\binom{n}{k-1}$ subsets of T that contain t, since t is already chosen, but the remaining k-1 elements need to be chosen from T - {t}, a set of size n.

(b) There are $\binom{n}{k}$ subsets of T not containing t, since one can choose any k elements from the set T - {t} with n elements.

Since the two cases are exhaustive, C(n+1,k) = C(n,k-1) + C(n,k).

Pascal's Identity (3)

The first way of counting yields the LHS, and the second way of counting (using the sum rule) yields the RHS of the following formula:

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