

Combinatorics

Slides by Christopher M. Bourke
Instructor: Berthe Y. Choueiry

Fall 2007

Computer Science & Engineering 235
Introduction to Discrete Mathematics
Sections 5.1-5.6 & 7.5-7.6 of Rosen
cse235@cse.unl.edu

Combinatorics I

Introduction

Combinatorics is the study of collections of objects. Specifically, *counting* objects, arrangement, derangement, etc. of objects along with their mathematical properties.

Counting objects is important in order to analyze algorithms and compute discrete probabilities.

Originally, combinatorics was motivated by gambling: counting configurations is essential to elementary probability.

Combinatorics II

Introduction

A simple example: How many arrangements are there of a deck of 52 cards?

In addition, combinatorics can be used as a proof technique.

A *combinatorial proof* is a proof method that uses counting arguments to prove a statement.

Product Rule

If two events are not mutually exclusive (that is, we do them separately), then we apply the product rule.

Theorem (Product Rule)

Suppose a procedure can be accomplished with two disjoint subtasks. If there are n_1 ways of doing the first task and n_2 ways of doing the second, then there are

$$n_1 \cdot n_2$$

ways of doing the overall procedure.

Sum Rule I

If two events are mutually exclusive, that is, they cannot be done at the same time, then we must apply the sum rule.

Theorem (Sum Rule)

If an event e_1 can be done in n_1 ways and an event e_2 can be done in n_2 ways and e_1 and e_2 are mutually exclusive, then the number of ways of both events occurring is

$$n_1 + n_2$$

Sum Rule II

There is a natural generalization to any sequence of m tasks; namely the number of ways m mutually exclusive events can occur is

$$n_1 + n_2 + \cdots + n_{m-1} + n_m$$

We can give another formulation in terms of sets. Let A_1, A_2, \dots, A_m be pairwise *disjoint* sets. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|$$

In fact, this is a special case of the general *Principle of Inclusion-Exclusion*.

Principle of Inclusion-Exclusion (PIE) I

Introduction

Say there are two events, e_1 and e_2 for which there are n_1 and n_2 possible outcomes respectively.

Now, say that only *one* event can occur, not both.

In this situation, we cannot apply the sum rule? Why?

Principle of Inclusion-Exclusion (PIE) II

Introduction

We cannot use the sum rule because we would be *over counting* the number of possible outcomes.

Instead, we have to count the number of possible outcomes of e_1 and e_2 *minus* the number of possible outcomes in common to both; i.e. the number of ways to do both "tasks".

If again we think of them as sets, we have

$$|A_1| + |A_2| - |A_1 \cap A_2|$$

Principle of Inclusion-Exclusion (PIE) III

Introduction

More generally, we have the following.

Lemma

Let A, B be subsets of a finite set U . Then

1. $|A \cup B| = |A| + |B| - |A \cap B|$
2. $|A \cap B| \leq \min\{|A|, |B|\}$
3. $|A \setminus B| = |A| - |A \cap B| \geq |A| - |B|$
4. $|\bar{A}| = |U| - |A|$
5. $|A \oplus B| = |A \cup B| - |A \cap B| = |A| + |B| - 2|A \cap B| = |A \setminus B| + |B \setminus A|$
6. $|A \times B| = |A| \times |B|$

Principle of Inclusion-Exclusion (PIE) I

Theorem

Theorem

Let A_1, A_2, \dots, A_n be finite sets, then

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_i |A_i| \\ &\quad - \sum_{i < j} |A_i \cap A_j| \\ &\quad + \sum_{i < j < k} |A_i \cap A_j \cap A_k| \\ &\quad - \dots \\ &\quad + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned}$$

Principle of Inclusion-Exclusion (PIE) II

Theorem

Each summation is over all i , pairs i, j with $i < j$, triples i, j, k with $i < j < k$ etc.

Principle of Inclusion-Exclusion (PIE) III

Theorem

To illustrate, when $n = 3$, we have

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| \\ &\quad - [|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|] \\ &\quad + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

Principle of Inclusion-Exclusion (PIE) IV

Theorem

To illustrate, when $n = 4$, we have

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4| &= |A_1| + |A_2| + |A_3| + |A_4| \\ &\quad - \left[|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| \right. \\ &\quad \left. + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4| \right] \\ &\quad + \left[|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \right. \\ &\quad \left. + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \right] \\ &\quad - |A_1 \cap A_2 \cap A_3 \cap A_4| \end{aligned}$$

Principle of Inclusion-Exclusion (PIE) I

Example I

Example

How many integers between 1 and 300 (inclusive) are

1. Divisible by at least one of 3, 5, 7?
2. Divisible by 3 and by 5 but not by 7?
3. Divisible by 5 but by neither 3 nor 7?

Let

$$\begin{aligned} A &= \{n \mid 1 \leq n \leq 300 \wedge 3 \mid n\} \\ B &= \{n \mid 1 \leq n \leq 300 \wedge 5 \mid n\} \\ C &= \{n \mid 1 \leq n \leq 300 \wedge 7 \mid n\} \end{aligned}$$

Principle of Inclusion-Exclusion (PIE) II

Example I

How big are each of these sets? We can easily use the floor function;

$$\begin{aligned} |A| &= \lfloor 300/3 \rfloor = 100 \\ |B| &= \lfloor 300/5 \rfloor = 60 \\ |C| &= \lfloor 300/7 \rfloor = 42 \end{aligned}$$

For (1) above, we are asked to find $|A \cup B \cup C|$.

Principle of Inclusion-Exclusion (PIE) III

Example I

By the principle of inclusion-exclusion, we have that

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad - \left[|A \cap B| + |A \cap C| + |B \cap C| \right] \\ &\quad + |A \cap B \cap C| \end{aligned}$$

It remains to find the final 4 cardinalities.

All three divisors, 3, 5, 7 are relatively prime. Thus, any integer that is divisible by *both* 3 and 5 must simply be divisible by 15.

Principle of Inclusion-Exclusion (PIE) IV

Example I

Using the same reasoning for all pairs (and the triple) we have

$$\begin{aligned} |A \cap B| &= \lfloor 300/15 \rfloor = 20 \\ |A \cap C| &= \lfloor 300/21 \rfloor = 14 \\ |B \cap C| &= \lfloor 300/35 \rfloor = 8 \\ |A \cap B \cap C| &= \lfloor 300/105 \rfloor = 2 \end{aligned}$$

Therefore,

$$|A \cup B \cup C| = 100 + 60 + 42 - 20 - 14 - 8 + 2 = 162$$

Principle of Inclusion-Exclusion (PIE) V

Example I

For (2) above, it is enough to find

$$|(A \cap B) \setminus C|$$

By the definition of set-minus,

$$|(A \cap B) \setminus C| = |A \cap B| - |A \cap B \cap C| = 20 - 2 = 18$$

Principle of Inclusion-Exclusion (PIE) VI

Example I

For (3) above, we are asked to find

$$|B \setminus (A \cup C)| = |B| - |B \cap (A \cup C)|$$

By distributing B over the intersection, we get

$$\begin{aligned} |B \cap (A \cup C)| &= |(B \cap A) \cup (B \cap C)| \\ &= |B \cap A| + |B \cap C| - |(B \cap A) \cap (B \cap C)| \\ &= |B \cap A| + |B \cap C| - |B \cap A \cap C| \\ &= 20 + 8 - 2 = 26 \end{aligned}$$

So the answer is $|B| - 26 = 60 - 26 = 34$.

Principle of Inclusion-Exclusion (PIE) I

Example II

The principle of inclusion-exclusion can be used to count the number of onto (surjective) functions.

Theorem

Let A, B be non-empty sets of cardinality m, n with $m \geq n$. Then there are

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \dots + (-1)^{n-1} \binom{n}{n-1} 1^m$$

i.e. $\sum_{i=0}^{n-1} (-1)^i \binom{n}{i} (n-i)^m$ onto functions $f: A \rightarrow B$.

See textbook page 509.

Principle of Inclusion-Exclusion (PIE) II

Example II

Example

How many ways of giving out 6 pieces of candy to 3 children if each child must receive at least one piece?

This can be modeled by letting A represent the set of candies and B be the set of children.

Then a function $f: A \rightarrow B$ can be interpreted as giving candy a_i to child c_j .

Since each child must receive at least one candy, we are considering only onto functions.

Principle of Inclusion-Exclusion (PIE) III

Example II

To count how many there are, we apply the theorem and get (for $m = 6, n = 3$),

$$3^6 - \binom{3}{1}(3-1)^6 + \binom{3}{2}(3-2)^6 = 540$$

Derangements I

Consider the hatcheck problem.

- ▶ An employee checks hats from n customers.
- ▶ However, he forgets to tag them.
- ▶ When customer's check-out their hats, they are given one at random.

What is the probability that no one will get their hat back?

Derangements II

This can be modeled using *derangements*: permutations of objects such that no element is in its original position.

For example, 21453 is a derangement of 12345, but 21543 is not.

Theorem

The number of derangements of a set with n elements is

$$D_n = n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right]$$

See textbook page 510.

Derangements III

Thus, the answer to the hatcheck problem is

$$\frac{D_n}{n!}$$

Its interesting to note that

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \dots$$

So that the probability of the hatcheck problem converges;

$$\lim_{n \rightarrow \infty} \frac{D_n}{n!} = e^{-1} = .368 \dots$$

The Pigeonhole Principle I

The *pigeonhole principle* states that if there are more pigeons than there are roosts (pigeonholes), for at least one pigeonhole, more than two pigeons must be in it.

Theorem (Pigeonhole Principle)

If $k + 1$ or more objects are placed into k boxes, then there is at least one box containing two or more objects.

This is a fundamental tool of elementary discrete mathematics. It is also known as the *Dirichlet Drawer Principle* or *Dirichlet Box Principle*.

The Pigeonhole Principle II

It is *seemingly* simple, but *very* powerful.

The difficulty comes in where and how to apply it.

Some simple applications in Computer Science:

- ▶ Calculating the probability of Hash functions having a collision.
- ▶ Proving that there can be *no* lossless compression algorithm compressing all files to within a certain ratio.

Lemma

For two finite sets A, B there exists a bijection $f : A \rightarrow B$ if and only if $|A| = |B|$.

Generalized Pigeonhole Principle I

Theorem

If N objects are placed into k boxes then there is at least one box containing at least

$$\left\lceil \frac{N}{k} \right\rceil$$

Example

In any group of 367 or more people, at least two of them must have been born on the same date.

Generalized Pigeonhole Principle II

A probabilistic generalization states that if n objects are randomly put into m boxes with uniform probability (each object is placed in a given box with probability $1/m$) then at least one box will hold more than one object with probability,

$$1 - \frac{m!}{(m-n)!m^n}$$

Generalized Pigeonhole Principle III

Example

Among 10 people, what is the probability that two or more will have the same birthday?

Here, $n = 10$ and $m = 365$ (ignore leapyears). Thus, the probability that two will have the same birthday is

$$1 - \frac{365!}{(365-10)!365^{10}} \approx .1169$$

So less than a 12% probability!

Pigeonhole Principle I

Example I

Example

Show that in a room of n people with certain acquaintances, some pair must have the same number of acquaintances.

Note that this is equivalent to showing that any symmetric, irreflexive relation on n elements must have two elements with the same number of relations.

We'll show by contradiction using the pigeonhole principle.

Assume to the contrary that every person has a different number of acquaintances; $0, 1, \dots, n-1$ (we cannot have n here because it is irreflexive). Are we done?

Pigeonhole Principle II

Example I

No, since we only have n people, this is okay (i.e. there are n possibilities).

We need to use the fact that acquaintanceship is a symmetric, irreflexive relation.

In particular, some person knows 0 people while another knows $n-1$ people.

In other words, someone knows everyone, but there is also a person that knows no one.

Thus, we have reached a contradiction. \square

Pigeonhole Principle I

Example II

Example

Show that in any list of ten nonnegative integers, A_0, \dots, A_9 , there is a string of consecutive items of the list a_i, a_{i+1}, \dots whose sum is divisible by 10.

Consider the following 10 numbers.

$$\begin{aligned} &a_0 \\ &a_0 + a_1 \\ &a_0 + a_1 + a_2 \\ &\vdots \\ &a_0 + a_1 + a_2 + \dots + a_9 \end{aligned}$$

If any one of them is divisible by 10 then we are done.

Pigeonhole Principle II

Example II

Otherwise, we observe that each of these numbers must be in one of the congruence classes

$$1 \bmod 10, 2 \bmod 10, \dots, 9 \bmod 10$$

By the pigeonhole principle, at least two of the integers above must lie in the same congruence class. Say a, a' lie in the congruence class $k \bmod 10$.

Then

$$(a - a') \equiv k - k \pmod{10}$$

and so the difference $(a - a')$ is divisible by 10. \square

Pigeonhole Principle I

Example III

Example

Say 30 buses are to transport 2000 Cornhusker fans to Colorado. Each bus has 80 seats. Show that

1. One of the buses will have 14 empty seats.
2. One of the buses will carry at least 67 passengers.

For (1), the total number of seats is $30 \cdot 80 = 2400$ seats. Thus there will be $2400 - 2000 = 400$ empty seats total.

Pigeonhole Principle II

Example III

By the generalized pigeonhole principle, with 400 empty seats among 30 buses, one bus will have at least

$$\left\lceil \frac{400}{30} \right\rceil = 14$$

empty seats.

For (2) above, by the pigeonhole principle, seating 2000 passengers among 30 buses, one will have at least

$$\left\lceil \frac{2000}{30} \right\rceil = 67$$

passengers.

Permutations I

A *permutation* of a set of distinct objects is an *ordered* arrangement of these objects. An ordered arrangement of r elements of a set is called an r -*permutation*.

Theorem

The number of r permutations of a set with n distinct elements is

$$P(n, r) = \prod_{i=0}^{r-1} (n-i) = n(n-1)(n-2) \cdots (n-r+1)$$

Permutations II

It follows that

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

In particular,

$$P(n, n) = n!$$

Again, note here that *order is important*. It is necessary to distinguish in what cases order is important and in which it is not.

Permutations

Example I

Example

How many pairs of dance partners can be selected from a group of 12 women and 20 men?

The first woman can be partnered with any of the 20 men. The second with any of the remaining 19, etc.

To partner all 12 women, we have

$$P(20, 12)$$

Permutations

Example II

Example

In how many ways can the English letters be arranged so that there are exactly ten letters between a and z ?

The number of ways of arranging 10 letters between a and z is $P(24, 10)$. Since we can choose either a or z to come first, there are $2P(24, 10)$ arrangements of this 12-letter block.

For the remaining 14 letters, there are $P(15, 15) = 15!$ arrangements. In all, there are

$$2P(24, 10) \cdot 15!$$

Permutations

Example III

Example

How many permutations of the letters a, b, c, d, e, f, g contain neither the pattern bge nor caf ?

The number of total permutations is $P(7, 7) = 7!$.

If we fix the pattern bge , then we can consider it as a single block. Thus, the number of permutations with this pattern is $P(5, 5) = 5!$.

Permutations

Example III - Continued

Fixing the pattern caf we have the same number, $5!$.

Thus we have

$$7! - 2(5!)$$

Is this correct?

No. We have taken away too many permutations: ones containing *both* caf and bge .

Here there are two cases, when caf comes first and when bge comes first.

Permutations

Example III - Continued

$ea f$ cannot come before bge , so this is not a problem.

If bge comes first, it must be the case that we have $bgeaf$ as a single block and so we have 3 blocks or $3!$ arrangements.

Altogether we have

$$7! - 2(5!) + 3! = 4806$$

Combinations I

Definition

Whereas permutations consider order, *combinations* are used when *order does not matter*.

Definition

An k -combination of elements of a set is an unordered selection of k elements from the set. A combination is simply a subset of cardinality k .

Combinations II

Definition

Theorem

The number of k -combinations of a set with cardinality n with $0 \leq k \leq n$ is

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

Note: the notation, $\binom{n}{k}$ is read, " n choose k ". In \TeX use $\{n$ choose $k\}$ (with the forward slash).

Combinations III

Definition

A useful fact about combinations is that they are symmetric.

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

$$\binom{n}{2} = \binom{n}{n-2}$$

etc.

Combinations IV

Definition

This is formalized in the following corollary.

Corollary

Let n, k be nonnegative integers with $k \leq n$, then

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

Combinations I

Example I

Example

In the Powerball lottery, you pick five numbers between 1 and 55 and a single "powerball" number between 1 and 42. How many possible plays are there?

Order here doesn't matter, so the number of ways of choosing five regular numbers is

$$\binom{55}{5}$$

Combinations II

Example I

We can choose among 42 power ball numbers. These events are not mutually exclusive, thus we use the product rule.

$$42 \binom{55}{5} = 42 \frac{55!}{(55-5)!5!} = 146,107,962$$

So the odds of winning are

$$\frac{1}{146,107,962} < .000000006845$$

Combinations I

Example II

Example

In a sequence of 10 coin tosses, how many ways can 3 heads and 7 tails come up?

The number of ways of choosing 3 heads out of 10 coin tosses is

$$\binom{10}{3}$$

Combinations II

Example II

However, this is the same as choosing 7 tails out of 10 coin tosses;

$$\binom{10}{3} = \binom{10}{7} = 120$$

This is a perfect illustration of the previous corollary.

Combinations I

Example III

Example

How many possible committees of five people can be chosen from 20 men and 12 women if

1. if exactly three men must be on each committee?
2. if at least four women must be on each committee?

Combinations II

Example III

For (1), we must choose 3 men from 20 then two women from 12. These are not mutually exclusive, thus the product rule applies.

$$\binom{20}{3} \binom{12}{2}$$

Combinations III

Example III

For (2), we consider two cases; the case where four women are chosen and the case where five women are chosen. These two cases are mutually exclusive so we use the addition rule.

For the first case we have

$$\binom{20}{1} \binom{12}{4}$$

Combinations IV

Example III

And for the second we have

$$\binom{20}{0} \binom{12}{5}$$

Together we have

$$\binom{20}{1} \binom{12}{4} + \binom{20}{0} \binom{12}{5} = 10,692$$

Binomial Coefficients I

Introduction

The number of r -combinations, $\binom{n}{r}$ is also called a *binomial coefficient*.

They are the coefficients in the expansion of the expression (multivariate polynomial), $(x + y)^n$. A *binomial* is a sum of two terms.

Binomial Coefficients II

Introduction

Theorem (Binomial Theorem)

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

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

Binomial Coefficients III

Introduction

Expanding the summation, we have

$$(x + y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \dots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$$

For example,

$$\begin{aligned} (x + y)^3 &= (x + y)(x + y)(x + y) \\ &= (x + y)(x^2 + 2xy + y^2) \\ &= x^3 + 3x^2y + 3xy^2 + y^3 \end{aligned}$$

Binomial Coefficients I

Example

Example

What is the coefficient of the term x^8y^{12} in the expansion of $(3x + 4y)^{20}$?

By the Binomial Theorem, we have

$$(3x + 4y)^n = \sum_{j=0}^n \binom{n}{j} (3x)^{n-j} (4y)^j$$

So when $j = 12$, we have

$$\binom{20}{12} (3x)^8 (4y)^{12}$$

so the coefficient is $\frac{20!}{12!8!} 3^8 4^{12} = 13866187326750720$.

Binomial Coefficients I

More

Many useful identities and facts come from the Binomial Theorem.

Corollary

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} &= 2^n \\ \sum_{k=0}^n (-1)^k \binom{n}{k} &= 0 \quad n \geq 1 \\ \sum_{k=0}^n 2^k \binom{n}{k} &= 3^n \end{aligned}$$

Binomial Coefficients II

More

Check textbook for proofs, which are based on: $2^n = (1 + 1)^n$,
 $0 = 0^n = ((-1) + 1)^n$, $3^n = (1 + 2)^n$.

Binomial Coefficients III

More

Most of these can be proven by either induction or by a combinatorial argument.

Theorem (Vandermonde's Identity)

Let m, n, r be nonnegative integers with r not exceeding either m or n . Then

$$\binom{m+n}{r} = \sum_{k=0}^r \binom{m}{r-k} \binom{n}{k}$$

Binomial Coefficients IV

More

Taking $n = m = r$ in the Vandermonde's identity.

Corollary

If n is a nonnegative integer, then

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

Corollary

Binomial Coefficients V

More

Let n, r be nonnegative integers, $r \leq n$. Then

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

Binomial Coefficients I

Pascal's Identity & Triangle

The following is known as Pascal's Identity which gives a useful identity for efficiently computing binomial coefficients.

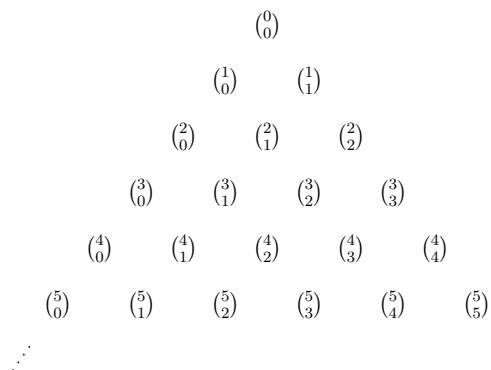
Theorem (Pascal's Identity)

Let $n, k \in \mathbb{Z}^+$ with $n \geq k$. Then

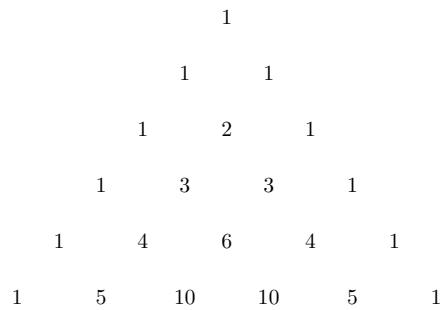
$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

Pascal's Identity forms the basis of a geometric object known as Pascal's Triangle.

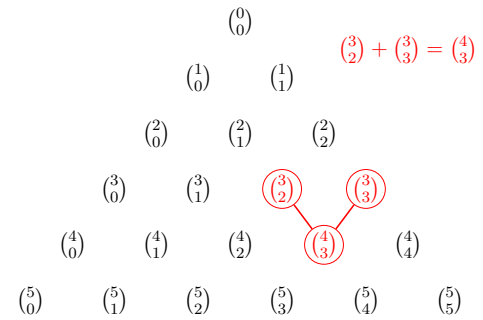
Pascal's Triangle



Pascal's Triangle



Pascal's Triangle



Generalized Combinations & Permutations I

Sometimes we are concerned with permutations and combinations in which *repetitions* are allowed.

Theorem

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

Easily obtained by the product rule.

Generalized Combinations & Permutations II

Theorem

There are

$$\binom{n+r-1}{r}$$

r -combinations from a set with n elements when repetition of elements is allowed.

Generalized Combinations & Permutations III

Example

There are 30 varieties of donuts from which we wish to buy a dozen. How many possible ways to place your order are there?

Here $n = 30$ and we wish to choose $r = 12$. Order does not matter and repetitions are possible, so we apply the previous theorem to get that there are

$$\binom{30+12-1}{12}$$

possible orders.

Generalized Combinations & Permutations IV

Theorem

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

$$\frac{n!}{n_1!n_2! \cdots n_k!}$$

An equivalent way of interpreting this theorem is the number of ways to distribute n distinguishable objects into k distinguishable boxes so that n_i objects are placed into box i for $i = 1, 2, \dots, k$.

Generalized Combinations & Permutations V

Example

How many permutations of the word "Mississippi" are there?

"Mississippi" contains 4 distinct letters, M , i , s and p ; with 1, 4, 4, 2 occurrences respectively.

Therefore there are

$$\frac{11!}{1!4!4!2!}$$

permutations.

Generating Permutations & Combinations I

Introduction

In general, it is inefficient to solve a problem by considering all permutations or combinations since there are an exponential number of such arrangements.

Nevertheless, for many problems, *no better approach is known*. When exact solutions are needed, *back-tracking* algorithms are used.

Generating permutations or combinations are sometimes the basis of these algorithms.

Generating Permutations & Combinations II

Introduction

Example (Traveling Sales Person Problem)

Consider a salesman that must visit n different cities. He wishes to visit them in an order such that his overall distance traveled is minimized.

Generating Permutations & Combinations III

Introduction

This problem is one of hundreds of NP-complete problems for which no known efficient algorithms exist. Indeed, it is believed that *no* efficient algorithms exist. (Actually, Euclidean TSP is not even known to be in NP!)

The only known way of solving this problem *exactly* is to try all $n!$ possible routes.

We give several algorithms for generating these combinatorial objects.

Generating Combinations I

Recall that combinations are simply all possible subsets of size r . For our purposes, we will consider generating subsets of

$$\{1, 2, 3, \dots, n\}$$

The algorithm works as follows.

- ▶ Start with $\{1, \dots, r\}$
- ▶ Assume that we have $a_1 a_2 \dots a_r$, we want the next combination.
- ▶ Locate the last element a_i such that $a_i \neq n - r + i$.
- ▶ Replace a_i with $a_i + 1$.
- ▶ Replace a_j with $a_i + j - i$ for $j = i + 1, i + 2, \dots, r$.

Generating Combinations II

The following is pseudocode for this procedure.

Algorithm (Next r -Combination)

```
INPUT      : A set of  $n$  elements and an  $r$ -combination,  $a_1 \dots a_r$ .
OUTPUT     : The next  $r$ -combination.
1   $i = r$ 
2  WHILE  $a_i = n - r + i$  DO
3     $i = i - 1$ 
4  END
5   $a_i = a_i + 1$ 
6  FOR  $j = (i + 1) \dots r$  DO
7     $a_j = a_i + j - i$ 
8  END
```

Generating Combinations III

Example

Find the next 3-combination of the set $\{1, 2, 3, 4, 5\}$ after $\{1, 4, 5\}$

Here, $a_1 = 1, a_2 = 4, a_3 = 5, n = 5, r = 3$.

The last i such that $a_i \neq 5 - 3 + i$ is 1.

Thus, we set

$$\begin{aligned}a_1 &= a_1 + 1 = 2 \\a_2 &= a_1 + 2 - 1 = 3 \\a_3 &= a_1 + 3 - 1 = 4\end{aligned}$$

So the next r -combination is $\{2, 3, 4\}$.

Generating Permutations

The text gives an algorithm to generate permutations in lexicographic order. Essentially the algorithm works as follows.

Given a permutation,

- ▶ Choose the left-most pair a_j, a_{j+1} where $a_j < a_{j+1}$.
- ▶ Choose the least item to the right of a_j greater than a_j .
- ▶ Swap this item and a_j .
- ▶ Arrange the remaining (to the right) items in order.

Generating Permutations

Lexicographic Order

Algorithm (Next Permutation (Lexicographic Order))

```
INPUT      : A set of  $n$  elements and an  $r$ -permutation,  $a_1 \dots a_r$ .
OUTPUT     : The next  $r$ -permutation.
1   $j = n - 1$ 
2  WHILE  $a_j > a_{j+1}$  DO
3     $j = j - 1$ 
4  END
   //  $j$  is the largest subscript with  $a_j < a_{j+1}$ 
5   $k = n$ 
6  WHILE  $a_j > a_k$  DO
7     $k = k - 1$ 
8  END
   //  $a_k$  is the smallest integer greater than  $a_j$  to the right of  $a_j$ 
9  swap( $a_j, a_k$ )
10  $r = n$ 
11  $s = j + 1$ 
12 WHILE  $r > s$  DO
13   swap( $a_r, a_s$ )
14
```

Generating Permutations I

Often there is no reason to generate permutations in lexicographic order. Moreover, even though generating permutations is inefficient in itself, lexicographic order induces even *more* work.

An alternate method is to *fix* an element, then recursively permute the $n - 1$ remaining elements.

Johnson-Trotter algorithm has the following attractive properties. Not in your textbook, not on the exam, just for your reference/culture.

- ▶ It is bottom-up (non-recursive).
- ▶ It induces a *minimal-change* between each permutation.

Generating Permutations II

The algorithm is known as the *Johnson-Trotter algorithm*.

We associate a direction to each element, for example:

$$\begin{array}{ccccc} & \leftarrow & & \leftarrow & \\ 3 & 2 & 4 & 1 & \end{array}$$

A component is *mobile* if its direction points to an adjacent component that is *smaller* than itself. Here 3 and 4 are mobile and 1 and 2 are not.

Generating Permutations III

Algorithm (JohnsonTrotter)

```
INPUT      : An integer  $n$ .
OUTPUT     : All possible permutations of  $(1, 2, \dots, n)$ .
1   $\pi = \overline{1} \overline{2} \dots \overline{n}$ 
2  WHILE There exists a mobile integer  $k \in \pi$  DO
3     $k =$  largest mobile integer
4    swap  $k$  and the adjacent integer  $k$  points to
5    reverse direction of all integers  $> k$ 
6    Output  $\pi$ 
7  END
```

More Examples

As always, the best way to learn new concepts is through practice and examples.

Example I I

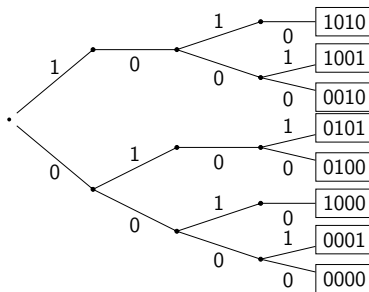
Example

How many bit strings of length 4 are there such that 11 never appears as a substring?

We can represent the set of string graphically using a diagram tree.

See textbook page 343.

Example I II



Therefore, the number of such bit string is 8.

Example: Counting Functions I I

Example

Let S, T be sets such that $|S| = n, |T| = m$. How many functions are there mapping $f : S \rightarrow T$? How many of these functions are one-to-one (injective)?

A function simply maps each s_i to some t_j , thus for each n we can choose to send it to *any* of the elements in T .

Example: Counting Functions I II

Each of these is an independent event, so we apply the multiplication rule;

$$\underbrace{m \times m \times \cdots \times m}_{n \text{ times}} = m^n$$

If we wish f to be one-to-one (injective), we must have that $n \leq m$, otherwise we can easily answer 0.

Now, each s_i must be mapped to a *unique* element in T . For s_1 , we have m choices. However, once we have made a mapping (say t_j), we cannot map subsequent elements to t_j again.

Example: Counting Functions I III

In particular, for the second element, s_2 , we now have $m - 1$ choices. Proceeding in this manner, s_3 will have $m - 2$ choices, etc. Thus we have

$$m \cdot (m - 1) \cdot (m - 2) \cdots (m - (n - 2)) \cdot (m - (n - 1))$$

An alternative way of thinking about this problem is by using the choose operator: we need to choose n elements from a set of size m for our mapping;

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

Example: Counting Functions I IV

Once we have chosen this set, we now consider all permutations of the mapping, i.e. $n!$ different mappings for this set. Thus, the number of such mappings is

$$\frac{m!}{(m-n)!n!} \cdot n! = \frac{m!}{(m-n)!}$$

Example: Counting Functions II

Recall this question from the midterm exam:

Example

Let $S = \{1, 2, 3\}$, $T = \{a, b\}$. How many onto functions are there mapping $S \rightarrow T$? How many one-to-one (injective) functions are there mapping $T \rightarrow S$?

See Theorem 1, page 509.

Example: Counting Primes I

Example

Give an estimate for how many 70 bit primes there are.

Recall that the number of primes not more than n is about

$$\frac{n}{\ln n}$$

See slides on Number Theory, page 15.

Using this fact, the number of primes not exceeding 2^{70} is

$$\frac{2^{70}}{\ln 2^{70}}$$

Example: Counting Primes II

However, we have over counted—we've counted 69-bit, 68-bit, etc primes as well.

The number of primes not exceeding 2^{69} is about

$$\frac{2^{69}}{\ln 2^{69}}$$

Thus the difference is

$$\frac{2^{70}}{\ln 2^{70}} - \frac{2^{69}}{\ln 2^{69}} \approx 1.19896 \times 10^{19}$$

Example: More sets I

Example

How many integers in the range $1 \leq k \leq 100$ are divisible by 2 or 3?

Let

$$\begin{aligned} A &= \{x \mid 1 \leq x \leq 100, 2 \mid x\} \\ B &= \{y \mid 1 \leq x \leq 100, 3 \mid y\} \end{aligned}$$

Clearly, $|A| = 50$, $|B| = \lfloor \frac{100}{3} \rfloor = 33$, so is it true that $|A \cup B| = 50 + 33 = 83$?

Example: More sets II

No; we've over counted again—any integer divisible by 6 will be in both sets. How much did we over count?

The number of integers between 1 and 100 divisible by 6 is $\lfloor \frac{100}{6} \rfloor = 16$, so the answer to the original question is

$$|A \cup B| = (50 + 33) - 16 = 67$$