CS70: Lecture 17.

Brief Comment.

Math and Computer Science Theory.

E.g.
There is a multiplicative inverse modulo a prime.
Existence: pigeonhole principle and divisibility argument.
Does not give efficient method to find inverse.
Extended GCD gives inverse.
and proof of existence.

E.g.
There is a way to recover from k errors in $n+2k$ packets.
Unique reconstruction that is consistent with $n+k$ points.
Does not give efficient method to reconstruct.
Berlekamp-Welsh: Error Locator polynomials!
Efficient reconstruction.

It's all math, done by mathematicians!

Efficient methods to construct objectes important in CS.

Lecture 17

What's to come? Probability.

A bag contains:

What is the chance that a ball taken from the bag is blue?

Count blue. Count total. Divide.

Today: Counting!

Later: Probability. Professor Walrand.

Outline

1. Counting.
2. Tree
3. Rules of Counting
4. Sample with/without replacement where order does/doesn't matter.

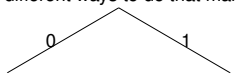
Probability is soon..but first let's count.

Count?

How many outcomes possible for k coin tosses?
How many poker hands?
How many handshakes for n people?
How many diagonals in a convex polygon?
How many 10 digit numbers?
How many 10 digit numbers without repetition?

Using a tree..

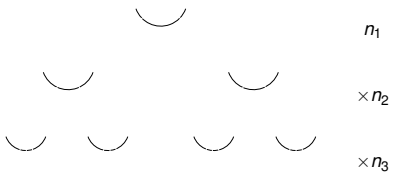
How many 3-bit strings?
How many different sequences of three bits from $\{0,1\}$?
How would you make one sequence?
How many different ways to do that making?



8 leaves which is $2 \times 2 \times 2$. One leaf for each string.
8 3-bit srings!

First Rule of Counting: Product Rule

Objects made by choosing from n_1, then n_2, ..., then n_k
the number of objects is $n_1 \times n_2 \cdots \times n_k$.



In picture, $2 \times 2 \times 3 = 12$!

Using the first rule..

How many outcomes possible for k coin tosses?

2 ways for first choice, 2 ways for second choice, ...
$2 \times 2 \cdots \times 2 = 2^k$

How many 10 digit numbers?

10 ways for first choice, 10 ways for second choice, ...
$10 \times 10 \cdots \times 10 = 10^k$

How many n digit base m numbers?

m ways for first, m ways for second, ...
m^n

Functions, polynomials.

How many functions f mapping S to T?

$|T|$ ways to choose for $f(s_1)$, $|T|$ ways to choose for $f(s_2)$, ...

....$|T|^{|S|}$

How many polynomials of degree d modulo p?

p ways to choose for first coefficient, p ways for second, ...
...p^{d+1}

p values for first point, p values for second, ...
...p^{d+1}

Permutations.

How many 10 digit numbers **without repeating a digit**?

10 ways for first, 9 ways for second, 8 ways for third, ...

... $10 * 9 * 8 \cdots * 1 = 10!$.[1]

How many different samples of size k from n numbers **without replacement.**

n ways for first choice, $n-1$ ways for second,
$n-2$ choices for third, ...

... $n*(n-1)*(n-2)\cdot*(n-k) = \frac{n!}{(n-k)!}$.

How many orderings of n objects are there?
Permutations of n objects.

n ways for first, $n-1$ ways for second,
$n-2$ ways for third, ...

... $n*(n-1)*(n-2)\cdot*1 = n!$.

[1] By definition: 0! = 1.

One-to-One Functions.

How many one-to-one functions from $|S|$ to $|S|$.

$|S|$ choices for $f(s_1)$, $|S|-1$ choices for $f(s_2)$, ...

So total number is $|S| \times |S|-1 \cdots 1 = |S|!$
A one-to-one function is a permutation!

Counting sets..when order doesn't matter.

How many poker hands?

$52 \times 51 \times 50 \times 49 \times 48$???

Are $A, K, Q, 10, J$ of spades
and $10, J, Q, K, A$ of spades the same?
Second Rule of Counting: If order doesn't matter count ordered objects and then divide by number of orderings.[2]

Number of orderings for a poker hand: 5!.

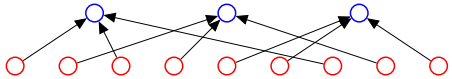
Can write as...
$$\frac{52 \times 51 \times 50 \times 49 \times 48}{5!}$$
$$\frac{52!}{5! \times 47!}$$

Generic: ways to choose 5 out of 52 possibilities.

[2] When each unordered object corresponds equal numbers of ordered objects.

Ordered to unordered.

Second Rule of Counting: If order doesn't matter count ordered objects and then divide by number of orderings.



How many red nodes (ordered objects)? 9.

How many red nodes mapped to one blue node? 3.

How many blue nodes (unordered objects)? $\frac{9}{3} = 3$.

How many poker deals? $52 \cdot 51 \cdot 50 \cdot 49 \cdot 48$.

How many poker hands per deal? Map each deal to ordered deal. 5!

How many poker hands? $\frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5!}$

..order doesn't matter.

Choose 2 out of n?

$$\frac{n \times (n-1)}{2} = \frac{n!}{(n-2)! \times 2}$$

Choose 3 out of n?

$$\frac{n \times (n-1) \times (n-2)}{3!} = \frac{n!}{(n-3)! \times 3!}$$

Choose k **out of** n?

$$\frac{n!}{(n-k)! \times k!}$$

Notation: $\binom{n}{k}$ **and pronounced "n choose k."**

Simple Practice.

How many orderings of letters of CAT?

3 ways to choose first letter, 2 ways to choose second, 1 for last.

$\implies 3 \times 2 \times 1 = 3!$ orderings

How many orderings of the letters in ANAGRAM?

Ordered, except for A!

total orderings of 7 letters. 7!
total "extra counts" or orderings of two A's? 3!

Total orderings? $\frac{7!}{3!}$

How many orderings of MISSISSIPPI?

4 S's, 4 I's, 2 P's.
11 letters total!
11! ordered objects!
$4! \times 4! \times 2!$ ordered objects per "unordered object"

$\implies \frac{11!}{4!4!2!}$.

Sampling...

Sample k items out of n

Without replacement:
Order matters: $n \times n-1 \times n-2 \ldots \times n-k+1 = \frac{n!}{(n-k)!}$
Order does not matter:
Second Rule: divide by number of orders – "$k!$"
$\implies \frac{n!}{(n-k)!k!}$.
"n choose k"

With Replacement.
Order matters: $n \times n \times \ldots n = n^k$
Order does not matter: Second rule ???

Problem: depends on how many of each item we chose!
So different number of unordered elts map to each unordered elt.

Unordered elt: $1,2,3$ 3! ordered elts map to it.
Unordered elt: $1,2,2$ $\frac{3!}{2!}$ ordered elts map to it.

How do we deal with this mess?!?!

Stars and bars....

How many ways can Bob and Alice split 5 dollars?
For each of 5 dollars pick Bob or Alice(2^5), divide out order ???

5 dollars for Bob and 0 for Alice:
one ordered set: (B,B,B,B,B).

4 for Bob and 1 for Alice:
5 ordered sets: (A,B,B,B,B) ; (B,A,B,B,B); ...

Well, we can list the possibilities.
$0+5$, $1+4$,$2+3$, $3+2$, $4+1$, $5+0$.

For 2 numbers adding to k, we get $k+1$.

For 3 numbers adding to k?

Stars and Bars.

How many ways to add up n numbers to equal k?

Or: k choices from set of n possibilities with replacement.
Sample with replacement where order just doesn't matter.

How many ways can Alice, Bob, and Eve split 5 dollars.

Five dollars are five stars: $\star\star\star\star\star$.

Alice: 2, Bob: 1, Eve: 2.
Stars and Bars: $\star\star|\star|\star\star$.

Alice: 0, Bob: 1, Eve: 4.
Stars and Bars: $|\star|\star\star\star\star$.

Each split $\implies$ a sequence of stars and bars.
Each sequence of stars and bars $\implies$ a split.

Counting Rule: if there is a one-to-one mapping between two sets they have the same size!

Stars and Bars.

How many different 5 star and 2 bar diagrams?

7 positions in which to place the 2 bars.

$\binom{7}{2}$ ways to do so and $\binom{7}{2}$ ways to split 5$ among 3 people.

Ways to add up n numbers to sum to k? or

" k from n with replacement where order doesn't matter."

In general, k stars $n-1$ bars.

$$\star\star|\star|\cdots|\star\star.$$

$n+k-1$ positions from which to choose $n-1$ bar positions.

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

Summary.

First rule: $n_1 \times n_2 \cdots \times n_3$**.**

k Samples with replacement from n items: n^k.
Sample without replacement: $\frac{n!}{(n-k)!}$

Second rule: when order doesn't matter divide..when possible.

Sample without replacement and order doesn't matter: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.
"n choose k"

One-to-one rule: equal in number if one-to-one correspondence.

Sample with replacement and order doesn't matter: $\binom{k+n-1}{n}$.

See you on Friday.