Review: Error Correction scheme.

Message "is" points on $P(x)$. (degree $n-1$, $n+2k$ points.)

Channel: Send $P(i)$, receive $R(i)$.

Errors are wrong values at $\le k$ points.Error: $P(i) \ne R(i)$.

Error locator polynomial:
$E(x) = (x-e_1)\cdot(x-e_k) = x^k + b_{k-1}x^{k-1} + \cdots + b_0$.

Find: $Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots + a_0$ and $E(x)$.

Using $n+2k$ equations: $Q(i) = R(i)E(i)$.

$P(x) = Q(x)/E(x)$.

Solving for $Q(x)$ and $E(x)$...and $P(x)$

For all points $1,\ldots,i,n+2k = m$,

$$Q(i) = R(i)E(i) \pmod p$$

Gives $n+2k$ linear equations.

$$\begin{aligned}
a_{n+k-1} + \ldots a_0 &\equiv R(1)(1 + b_{k-1}\cdots b_0) \pmod p\\
a_{n+k-1}(2)^{n+k-1} + \ldots a_0 &\equiv R(2)((2)^k + b_{k-1}(2)^{k-1}\cdots b_0) \pmod p\\
&\vdots\\
a_{n+k-1}(m)^{n+k-1} + \ldots a_0 &\equiv R(m)((m)^k + b_{k-1}(m)^{k-1}\cdots b_0) \pmod p
\end{aligned}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$.

Find $P(x) = Q(x)/E(x)$.

Poll

What are the ideas?

(A) Multiply a incorrect equality by zero makes it correct.
(B) Multiply by non-zero keeps it informative.
(C) A polynomial of degree k, can have exactly k zeros.
(D) Multpliying two polynomials gives a polynomial.
(E) $Q(i) = E(i)R(i)$ is linear in coeffs of Q and E.

(A), (B), (C).
$\implies$ error polynomial.

(D) and (E).
finish up.

Poll

A message of length 4, encoded as $P(x)$ w/packets $P(1),\ldots P(8)$.

Recieved packets $R(1),\ldots R(8)$.

Packets 1 and 4 are corrupted.

(A) $R(1) \ne P(1)$
(B) The degree of $P(x)E(x) = 3+2 = 5$.
(C) The degree of $E(x)$ is 2.
(D) The number of coefficients of $P(x)$ is 4.
(E) The number of coefficients of $P(x)Q(x)$ is 6.

(E) is false.

(A) $E(x) = (x-1)(x-2)$
(B) The number of coefficents in $E(x)$ is 2.
(C) The number of unknown coefficents in $E(x)$ is 2.
(D) $E(x) = (x-1)(x-4)$
(E) $R(4) \ne P(4)$
(F) The degree of $R(x)$ is 5.

(C),(D), (E).
(F) doesn't type check! $R(i)$ is the value one recieves.

Summary. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$
How to encode? With polynomial, $P(x)$.
Of degree? $n-1$
Recover? Reconstruct $P(x)$ with any n points!

Communicate n packets, with k errors.

How many packets? $n+2k$
Why?
k extra "good" packets after k errors.
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
$\le k$ changes ensure
two polynomials "correct on" $n+k$ overlap on n points
Two polynomials of degree $n-1$ mean same polynonmial.
Recover?
Reconstruct error polynomial, $E(X)$, and $P(x)$!
Nonlinear equations.
Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.
Polynomial division! $P(x) = Q(x)/E(x)$!

Reed-Solomon codes. Welsh-Berlekamp Decoding. Perfection!

Cool.

Really Cool!

Probability

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.

For now: Counting!

Later: Probability.

The future in this course.

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. **Chances?**

(A) Red Probability is $3/8$
(B) Blue probability is $3/9$
(C) Yellow Probability is $2/8$
(D) Blue probability is $3/8$

Today: Counting!

Combinatorics.

Outline: basics

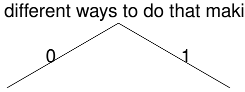
1. Counting.
2. Tree
3. Rules of Counting
4. Sample with/without replacement where order does/doesn't matter.

Count?

How many outcomes possible for k coin tosses?
How many poker hands?
How many handshakes for n people?
How many diagonals in a n sided convex polygon?
How many 10 digit numbers?
How many 10 digit numbers without repetition?
How many ways can I divide up 5 dollars among 3 people?

Using a tree..

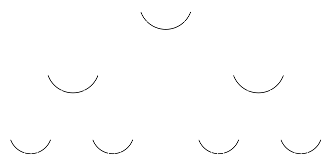
How many 3-bit strings?
How many different sequences of three bits from $\{0,1\}$?
How would you make one sequence?
How many different ways to do that making?



8 leaves which is $2 \times 2 \times 2$. One leaf for each string.
8 3-bit strings! Also recurrence: $B(n) = 2 \times B(n-1)$. $B(0) = 1$.

First Rule of Counting: Product Rule

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



n_1

$\times n_2$

$\times n_3$

In picture, $2 \times 2 \times 3 = 12!$
Also recurrence: $S(i) = n_i \times S(i-1)$, Base: $S(0) = 1$

Poll

What's correct?

(A) $|\text{10 digit numbers}| = 10^{10}$
(B) $|k \text{ coin tosses}| = 2^k$
(C) $|\text{10 digit numbers}| = 9 * 10^9$
(D) $|n \text{ digit base } m \text{ numbers}| = m^n$
(E) $|n \text{ digit base } m \text{ numbers}| = (m-1)m^{n-1}$

(A) or (C)? (D) or (E)? (B) are correct.

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

(Is 09, a two digit number?)

If no. Then $(m-1)m^{n-1}$.

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}

Questions?

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]

Sample of size k from n numbers **without replacement.**

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

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

How many orderings of n objects?

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!

Bijections are permutations.

$f(x) = 2x \pmod 5$

$\{0,1,2,3,4\} \to \{0,2,4,1,3\}$.

Switching around elements.

Number of functions from $\{0,1,2,3,4\}$ to $\{0,1,2,3,4\}$?

5!.

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!"
(The "!" means factorial, not Exclamation.)

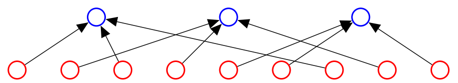
Can write as... $$\frac{52 \times 51 \times 50 \times 49 \times 48}{5!} \qquad \frac{52!}{5! \times 47!}$$

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 deals per hand?
Map each deal to ordered deal: 5!

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

Questions?

..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?

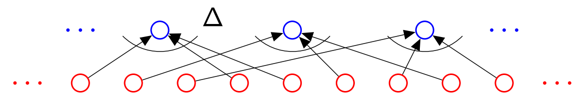
$$\frac{n!}{(n-k)! \times k!}$$

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

Familiar? Questions?

Example: Visualize the proof..

First rule: $n_1 \times n_2 \cdots \times n_3$. **Product Rule.**
Second rule: when order doesn't matter divide...

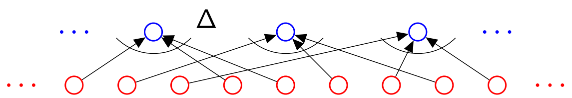


3 card Poker deals: $52 \times 51 \times 50 = \frac{52!}{49!}$. First rule.
Poker hands: Δ?
Hand: Q, K, A.
Deals: Q,K,A : Q,A,K : K,A,Q : K,A,Q : A,K,Q : A,Q,K.
Δ = $3 \times 2 \times 1$ First rule again.
Total: $\frac{52!}{49!3!}$ Second Rule!

Choose k out of n.
Ordered set: $\frac{n!}{(n-k)!}$ Orderings of one hand? $k!$ (By first rule!)
$\implies$ Total: $\frac{n!}{(n-k)!k!}$ Second rule.

Example: Anagram

First rule: $n_1 \times n_2 \cdots \times n_3$. **Product Rule.**
Second rule: when order doesn't matter divide...



Orderings of ANAGRAM?
Ordered Set: 7! First rule.
A's are the same!
What is Δ?
ANAGRAM
$A_1NA_2GRA_3M$, $A_2NA_1GRA_3M$, ...
$\Delta = 3 \times 2 \times 1 = 3!$ First rule!
$\implies \frac{7!}{3!}$ Second rule!

Poll

(A) $|\text{Poker hands}| = \binom{52}{5}$
(B) Orderings of ANAGRAM $= 7!/3!$
(C) Orderings of "CAT" $= 3!$
(D) Orders of MISSISSIPPI $= 11!/4!4!2!$
(E) Orderings of ANAGRAM $= 7!/4!$
(F) Orders of MISSISSIPPI $= 11!/10!$

(A)-(E) are correct.

Some Practice.

How many orderings of letters of CAT?

3 ways to choose first letter, 2 ways for 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 three 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"
$\implies \frac{11!}{4!4!2!}$.

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 (sometimes) can divide...

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.
pause Bijection!

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

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!
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??

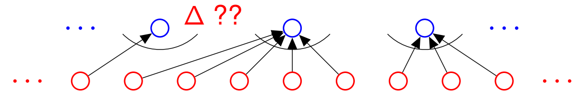
Splitting up some money....

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); ...

"Sorted" way to specify, first Alice's dollars, then Bob's.
(B,B,B,B,B): 1: (B,B,B,B,B)
(A,B,B,B,B): 5: (A,B,B,B,B),(B,A,B,B,B),(B,B,A,B,B),...
(A,A,B,B,B): $\binom{5}{2}$;(A,A,B,B,B),(A,B,A,B,B),(A,B,B,A,B),...
and so on.



Second rule of counting is no good here!

Splitting 5 dollars..

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

Alice gets 3, Bob gets 1, Eve gets 1: (A,A,A,B,E).

Separate Alice's dollars from Bob's and then Bob's from Eve's.

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 "is" a sequence of stars and bars.
Each sequence of stars and bars "is" 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?

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

7 positions in which to place the 2 bars.

– – – – – – –

Alice: 0; Bob 1; Eve: 4
$|\star|\star\star\star\star$.
Bars in first and third position.

Alice: 1; Bob 4; Eve: 0
$\star|\star\star\star\star|$.
Bars in second and seventh position.

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

Stars and Bars.

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.

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

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

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 (sometimes) can divide...

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.
pause Bijection!

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

Poll

Mark whats correct.

(A) ways to split k dollars among n: $\binom{k+n-1}{n-1}$
(B) ways to split n dollars among k: $\binom{n+k-1}{k-1}$
(C) ways to split 5 dollars among 3: $\binom{5+3-1}{3-1}$
(D) ways to split 5 dollars among 3: $\binom{7}{5}$

All correct.

Quick review of the basics.

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: $\binom{k+n-1}{n-1}$.
Distribute k samples (stars) over n poss. ($n-1$ bars group poss..)
Distribute k dollars to n people.

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 (sometimes) can divide...

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.
Bijection!

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