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.

\[
\begin{align*}
        a_n &+ a_0 = R(1)(1 + b_0 + \cdots + b_0) \quad \pmod p \\
   a_{n-k} &+ \cdots + a_0 = R(2)(2^k + b_0 + \cdots + b_0) \quad \pmod p \\
   &\vdots \\
   a_{n-1} &+ \cdots + a_0 = R(m)(m^k + b_0 + \cdots + b_0) \quad \pmod p
\end{align*}
\]

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

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

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

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 $\leq k$ points.
Error locator polynomial:
$E(x) = (x - e_1)(x - e_2)\cdots(x - e_n) = x^k + b_k + \cdots + b_0$.
Find: $Q(x) = E(x)P(x) = a_n + \cdots + a_0$ and $E(x)$.
Using $n + 2k$ equations: $Q(i) = R(i)E(i)$.

Poll

Say you sent a message of length 4, encoded as $P(x)$ where one sends packets $P(1),\ldots,P(8)$.
You receive packets $R(1),\ldots,R(8)$.

Poll

What are the ideas?

(A) Multiply a wrong equation 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) Multiplying two polynomials gives a polynomial.
(E) $Q(i) = E(i)R(i)$ is linear in coeffs of $Q$ and $E$.

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? 


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!

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!
**First Rule of Counting: Product Rule**

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

In picture, \( 2 \times 2 \times 3 = 12! \)

**Functions, polynomials.**

How many functions \( f \) mapping \( S \) to \( T \)?
- \( |T| \) ways to choose for \( f(s_1) \), \( |T| \) ways to choose for \( f(s_2) \), ...
- \( \cdots |T|^{\left|S\right|^{\left|T\right|}} \)

How many polynomials of degree \( d \) modulo \( p \)?
- \( p \) ways to choose for first coefficient, \( p \) ways for second, ...
- \( \cdots p^{d+1} \)
- \( p \) values for first point, \( p \) values for second, ...
- \( \cdots p^{d+1} \)

Questions?

**Poll**

Mark what's correct.
- (A) \(|10 \text{ digit numbers}| = 10^{10} \)
- (B) \(|k \text{ coin tosses}| = 2^k \)
- (C) \(|10 \text{ digit numbers}| = 9 \times 10^9 \)
- (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.

**Permutations.**

- How many 10 digit numbers without repeating a digit?
- \( 10 \) ways for first, \( 9 \) ways for second, \( 8 \) ways for third, ...
- \( \cdots 10 \times 9 \times 8 = 10! \).\(^1\)
- How many different samples of size \( k \) from \( n \) numbers without replacement.
- \( n \) ways for first choice, \( n − 1 \) ways for second, ...
- \( \cdots n \times (n − 1) \times (n − 2) \times \cdots 1 = n! \)

- How many orderings of \( n \) objects are there?
- **Permutations of \( n \) objects.**
- \( n \) ways for first, \( n − 1 \) ways for second, ...
- \( \cdots n \times (n − 1) \times (n − 2) \times 1 = n! \).

\(^1\)By definition: \( 0! = 1 \).

**Using the first rule.**

- How many outcomes possible for \( k \) coin tosses?
- 2 ways for first choice, 2 ways for second choice, ...
- \( 2 \times 2 \times 2 = 2^k \)
- How many 10 digit numbers?
- \( 10 \) ways for first choice, \( 10 \) ways for second choice, ...
- \( 10 \times 10 \times \cdots 10 = 10^k \)
- 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 \( (m − 1)m^{n−1} \).

**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 × 51 × 50 × 49 × 48 ???

Are A, K, Q, 10, J of spades and 10, J, Q, K 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...
\[
\frac{52!}{51!} \times \frac{50!}{49!} \times \frac{48!}{47!}
\]

Generic: ways to choose 5 out of 52 possibilities.

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

---

### Example: Visualize the proof.

**First rule:** \( n_1 \times n_2 \times \cdots \times n_k \). **Product Rule.**

**Second rule:** when order doesn’t matter divide...

3 card Poker deals: \( 52 \times 51 \times 50 = \frac{51!}{48!} \). **First rule.**

Poker hands: \( \Delta \)?

**Hand:** Q, K, A.

**Deals:** Q, K, A: Q, A, K: K, A, Q: K, Q, A: A, Q, K.

\( \Delta = 3 \times 2 \times 1 \). **First rule again.**

**Total:** \( \frac{52!}{48!} \). **Second Rule!**

Choose k out of n.

**Ordered set:** \( \frac{n!}{(n-k)!} \). **First rule!**

\( \Delta \) \( \frac{n!}{(n-k)!} \). **Second rule!**

---

### Example: Anagram

**First rule:** \( n_1 \times n_2 \times \cdots \times n_k \). **Product Rule.**

**Second rule:** when order doesn’t matter divide...

Orderings of ANAGRAM?

Ordered Set: 7!

A’s are the same!

What is \( \Delta \)?

**ANAGRAM**

A₁NA₂GRA₁M, A₂NA₁GRA₂M, ...

\( \Delta = 3 \times 2 \times 1 = 3! \). **First rule!**

\( \Rightarrow \frac{7!}{3!} \). **Second rule!**

---

### 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? \( 52 \times 51 \times 49 \times 48 \).
- How many poker deals per hand?
  - Map each deal to ordered deal: 5!
  - How many poker hands? \( \frac{52 \times 51 \times 49 \times 48}{5!} \)

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.”

Questions?

---

### Poll

Mark what’s correct.

(A) (Poker hands) \( \frac{52!}{51! \times 48!} \)
(B) Orderings of ANAGRAM \( \frac{7!}{3!} \)
(C) Orderings of “CAT” \( \frac{3!}{3!} \)
(D) Orders of MISSISSIPPI \( \frac{11!}{4!4!2!} \)
(E) Orderings of ANAGRAM \( \frac{7!}{3!} \)
(F) Orders of MISSISSIPPI \( \frac{11!}{10!} \)

(A)-(E) are correct.
Split 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: (B,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) ,...
and so on.

How many different 5 star and 2 bar diagrams?
| ⋆ | ⋆ ⋆ ⋆ ⋆ .

7 positions in which to place the 2 bars.

Second rule of counting is no good here!

Summary.

First rule: \( n_1 \times n_2 \cdots \times n_3 \).

k Samples with replacement from n items: \( n^k \).

Second rule: when order doesn’t matter (sometimes) can divide...

Sample without replacement: \( \binom{n}{k} \)

Second rule: when order doesn’t matter (sometimes) can divide...

Sample without replacement and order doesn’t matter: \( \binom{n}{k} \times \frac{k!}{(n-k)!} \).

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: \( \binom{n+k-1}{k} \).

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: \( 1,2,2 \) 2! ordered elts map to it.

How do we deal with this mess??

Session Practice.

How many orderings of letters of CAT?
3 ways to choose first letter, 2 ways for second, 1 for last.

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! x 4! x 2! ordered objects per “unordered object”

\( \frac{11!}{(4!)^2 \times 2!} \)

Second rule of counting is no good here!

How do we deal with this mess??

Splitting 5 dollars...

How many ways can Alice, Bob, and Eve split 5 dollars.
Alice gets 3, Bob gets 1, Eve gets 1: ...

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!

Sampling...

Sample k items out of n

Without replacement:

Order matters: \( n \times n-1 \times n-2 \cdots \times n-k+1 = \frac{n!}{(n-k)!} \)

Order does not matter:

Second Rule: divide by number of orders “k!”

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

“n choose k”

With Replacement.

Order matters: \( n \times n \times \cdots \times n = n^k \)

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: \( 1,2,2 \) 2! ordered elts map to it.

How do we deal with this mess??

Stars and Bars.

How many different 5 star and 2 bar diagrams?

| ⋆ | ⋆ ⋆ ⋆ ⋆ .

7 positions in which to place the 2 bars.

| ⋆ | ⋆ ⋆ ⋆ ⋆ |

Bars in first and third position.

| ⋆ | ⋆ ⋆ ⋆ ⋆ |

Bars in second and seventh position.

\( \binom{5}{2} \) ways to do so and \( \binom{5}{2} \) 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.

\[ \binom{n+k-1}{n-1} \]

\( n+k-1 \) positions from which to choose \( n-1 \) bar positions.

Or: \( k \) unordered choices from set of \( n \) possibilities with replacement. Sample with replacement where order doesn’t matter.

Quick review of the basics.

First rule: \( n_1 \times n_2 \times \cdots \times n_3 \).

\( k \) Samples with replacement from \( n \) items: \( n^k \).

Sample without replacement: \( \frac{n^k}{k!} \).

Second rule: when order doesn’t matter divide

"\( n \) choose \( k \)"

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

Distribute \( k \) dollars to \( n \) people.

Summary.

First rule: \( n_1 \times n_2 \times \cdots \times n_3 \).

\( k \) Samples with replacement from \( n \) items: \( n^k \).

Sample without replacement: \( \frac{n^k}{k!} \).

Second rule: when order doesn’t matter (sometimes) can divide...

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

"\( n \) 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: \( \binom{n+k-1}{n-1} \).

Poll

Mark what’s 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.

Sampling...

Sample \( k \) items out of \( n \)

Without replacement:

Order matters: \( n \times n-1 \times n-2 \times \cdots \times n-k+1 = \frac{n!}{(n-k)!} \)

Order does not matter:

Second Rule: divide by number of orders – \( "k!" \)

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

"\( n \) choose \( k \)"

With Replacement:

Order matters: \( n \times n \times \cdots \times n = n^k \)

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 \( 3 \) 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.
(A, B, B, B, B): 5 ordered sets: (A, B, B, B, B), (B, A, B, B, B), ...
(A, A, B, B, B): 3 ordered sets: (A, A, B, B, B), (A, B, A, B, 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, B, B, E).
Separate Alice’s dollars from Bob’s and then Bob’s from Eve’s.
Five dollars are five stars: ******.
Alice: 2, Bob: 1, Eve: 2.
Stars and Bars: *|*|*|*|*.
Alice: 0, Bob: 1, Eve: 4.
Stars and Bars: |*|*|*|*|*.
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.

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.

|***|*|*|*|

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.