Today.

Finish Welsh-Berlekamp.
Countability.
The Scheme.

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.

**Reed-Solomon Code:**

1. Make a polynomial, $P(x)$ of degree $n - 1$, that encodes message.
   - $P(1) = m_1, \ldots, P(n) = m_n$.
   - Comment: could encode with packets as coefficients.

2. Send $P(1), \ldots, P(n + 2k)$.

**After noisy channel:** Recieve values $R(1), \ldots, R(n + 2k)$.

**Properties:**

(1) $P(i) = R(i)$ for at least $n + k$ points $i$,
(2) $P(x)$ is unique degree $n - 1$ polynomial that contains $\geq n + k$ received points.
Slow solution.

**Brute Force:**
For each subset of $n+k$ points
   - Fit degree $n-1$ polynomial, $Q(x)$, to $n$ of them.
   - Check if consistent with $n+k$ of the total points.
   - If yes, output $Q(x)$.

▶ For subset of $n+k$ pts where $R(i) = P(i)$, method will reconstruct $P(x)$!

▶ For any subset of $n+k$ pts,
   1. there is unique degree $n-1$ polynomial $Q(x)$ that fits $n$ of them
   2. and where $Q(x)$ is consistent with $n+k$ points
      $\implies P(x) = Q(x)$.

Reconstructs $P(x)$ and only $P(x)$!!
Error Locater Polynomial.

\[
E(1)(p_{n-1} + \cdots + p_0) \equiv R(1)E(1) \pmod{p} \\
\vdots \\
E(i)(p_{n-1}i^{n-1} + \cdots + p_0) \equiv R(i)E(i) \pmod{p} \\
\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots + p_0) \equiv R(m)E(m) \pmod{p}
\]

...so satisfied, I’m on my way.

\(m = n + 2k\) satisfied equations, \(n + k\) unknowns. But nonlinear!

We have

\[Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots + a_0.\]

and

\[E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.\]

Equations:

\[Q(i) = R(i)E(i).\]

and linear in \(a_i\) and coefficients of \(b_j\)!
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

$$E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.$$  

$\implies k$ (unknown) coefficients. Leading coefficient is 1.

- $Q(x) = P(x)E(x)$ has degree $n + k - 1$ ...

$$Q(x) = a_{n+k-1}x^{n+k-1} + a_{n+k-2}x^{n+k-2} + \cdots a_0$$  

$\implies n + k$ (unknown) coefficients.

Number of unknown coefficients: $n + 2k$. 


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.

$$a_{n+k-1} + \ldots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$

$$a_{n+k-1}(2)^{n+k-1} + \ldots a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}$$

$$a_{n+k-1}(m)^{n+k-1} + \ldots a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}$$

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

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

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

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

\[
\begin{align*}
  a_3 + a_2 + a_1 + a_0 & \equiv 3(1 - b_0) \pmod{7} \\
  a_3 + 4a_2 + 2a_1 + a_0 & \equiv 1(2 - b_0) \pmod{7} \\
  6a_3 + 2a_2 + 3a_1 + a_0 & \equiv 6(3 - b_0) \pmod{7} \\
  a_3 + 2a_2 + 4a_1 + a_0 & \equiv 0(4 - b_0) \pmod{7} \\
  6a_3 + 4a_2 + 5a_1 + a_0 & \equiv 3(5 - b_0) \pmod{7}
\end{align*}
\]

$a_3 = 1, a_2 = 6, a_1 = 6, a_0 = 5$ and $b_0 = 2.$

$Q(x) = x^3 + 6x^2 + 6x + 5.$

$E(x) = x - 2.$
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c}
\begin{array}{cccc}
& 1 & x^2 & + & 1 & x & + & 1 \\
\hline
x - 2) & x^3 & + & 6x^2 & + & 6x & + & 5 \\
x^3 & - & 2x^2 & & & & & \\
\hline
\end{array}
\end{array}
\]

\[
\begin{array}{c}
\begin{array}{cccc}
& 1 & x^2 & + & 6x & + & 5 \\
\hline
1 & x^2 & - & 2x & & & & \\
\hline
\end{array}
\end{array}
\]

\[
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
x + 5 \\
x - 2 \\
\hline
0
\end{array}
\end{array}
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]

Message is \( P(1) = 3, P(2) = 0, P(3) = 6. \)

What is \( \frac{x - 2}{x - 2} \)? 1

Except at \( x = 2 \)? Hole there?
Error Correction: Berlekamp-Welsh

Message: $m_1, \ldots, m_n$.

Sender:
1. Form degree $n-1$ polynomial $P(x)$ where $P(i) = m_i$.
2. Send $P(1), \ldots, P(n+2k)$.

Receiver:
1. Receive $R(1), \ldots, R(n+2k)$.
2. Solve $n+2k$ equations, $Q(i) = E(i)R(i)$ to find $Q(x) = E(x)P(x)$ and $E(x)$.
3. Compute $P(x) = Q(x)/E(x)$.
4. Compute $P(1), \ldots, P(n)$. 
You have error locator polynomial!
Where oh where have my packets gone **wrong**?
Factor? Sure.
Check all values? Sure.
Efficiency? Sure. Only $n + 2k$ values.
   See where it is 0.
Hmmm...

Is there one and only one $P(x)$ from Berlekamp-Welsh procedure?  

**Existence:** there is a $P(x)$ and $E(x)$ that satisfy equations.
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$  \hspace{1cm} (1)

**Proof:**

We claim

$$Q'(x)E(x) = Q(x)E'(x)$$ on $n + 2k$ values of $x$.  \hspace{1cm} (2)

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n + 2k - 1$

and agree on $n + 2k$ points

$E(x)$ and $E'(x)$ have at most $k$ zeros each.

Can cross divide at $n$ points.

$$\implies \frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)}$$ equal on $n$ points.

Both degree $\leq n \implies$ Same polynomial!
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof: Construction implies that

$$Q(i) = R(i)E(i)$$
$$Q'(i) = R(i)E'(i)$$

for $i \in \{1, \ldots n + 2k\}$.

If $E(i) = 0$, then $Q(i) = 0$. If $E'(i) = 0$, then $Q'(i) = 0$.

$$\implies Q(i)E'(i) = Q'(i)E(i)$$

holds when $E(i)$ or $E'(i)$ are zero.

When $E'(i)$ and $E(i)$ are not zero

$$\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = R(i).$$

Cross multiplying gives equality in fact for these points.

Points to polynomials, have to deal with zeros!

Example: dealing with $\frac{x-2}{x-2}$ at $x = 2$. 


Berlekamp-Welsh algorithm decodes correctly when $k$ errors!
Communication $n$ 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!

Communication $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- 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!
Next up: how big is infinity.

- Countable
- Countably infinite.
- Enumeration
How big are the reals or the integers?

Infinite!

Is one bigger or smaller?
Same size?

Make a function $f : \text{Circles} \rightarrow \text{Squares}$.

- $f(\text{red circle}) = \text{red square}$
- $f(\text{blue circle}) = \text{blue square}$
- $f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

**One to One:** For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

Onto. Each square mapped to from some circle.

**Onto:** For all $s \in R$, $\exists c \in D$, $s = f(c)$.

**Isomorphism principle:** If there is $f : D \rightarrow R$ that is one to one and onto, then, $|D| = |R|$. 

Same number?
Isomorphism principle.

Given a function, \( f : D \rightarrow R \).

**One to One:**
For all \( \forall x, y \in D, x \neq y \implies f(x) \neq f(y) \).

or
\( \forall x, y \in D, f(x) = f(y) \implies x = y \).

**Onto:** For all \( y \in R, \exists x \in D, y = f(x) \).

\( f(\cdot) \) is a **bijection** if it is one to one and onto.

**Isomorphism principle:**
If there is a bijection \( f : D \rightarrow R \) then \( |D| = |R| \).
How to count?
0, 1, 2, 3, ...

The Counting numbers. 
The natural numbers! $N$

Definition: $S$ is **countable** if there is a bijection between $S$ and some subset of $N$.

If the subset of $N$ is finite, $S$ has finite **cardinality**.

If the subset of $N$ is infinite, $S$ is **countably infinite**.
Where's 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$

Bijection! $\implies |\mathbb{Z}^+| = |\mathbb{N}|$.

But.. but Where’s zero? “Comes from 1.”
A bijection is a bijection.

Notice that there is a bijection between $N$ and $Z^+$ as well.

$f(n) = n + 1$. $0 \rightarrow 1, 1 \rightarrow 2, \ldots$

Bijection from $A$ to $B \implies$ a bijection from $B$ to $A$.

Inverse function!

Can prove equivalence either way.

Bijection to or from natural numbers implies countably infinite.
More large sets.

$E$ - Even natural numbers?

$f : N \rightarrow E.$

$f(n) \rightarrow 2n.$

Onto: $\forall e \in E, f(e/2) = e.$ $e/2$ is natural since $e$ is even
One-to-one: $\forall x, y \in N, x \neq y \implies 2x \neq 2y.$ $\equiv f(x) \neq f(y)$

Evens are countably infinite.
Evens are same size as all natural numbers.
All integers?

What about Integers, $\mathbb{Z}$?
Define $f : \mathbb{N} \to \mathbb{Z}$.

$$f(n) = \begin{cases} 
\frac{n}{2} & \text{if } n \text{ even} \\
-(n+1)/2 & \text{if } n \text{ odd}.
\end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd, then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if $x$ is even and $y$ is even, then $x/2 \neq y/2 \implies f(x) \neq f(y)$

$\ldots$

Onto: For any $z \in \mathbb{Z}$,
if $z \geq 0$, $f(2z) = z$ and $2z \in \mathbb{N}$.
if $z < 0$, $f(2|z| - 1) = z$ and $2|z| + 1 \in \mathbb{N}$.

Integers and naturals have same size!


Listings

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>\ldots</td>
<td>\ldots</td>
</tr>
</tbody>
</table>

Notice that: A listing “is” a bijection with a subset of natural numbers.
Function \( \equiv \) “Position in list.”
If finite: bijection with \( \{0, \ldots, |S| - 1\} \)
If infinite: bijection with \( \mathbb{N} \).
Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, 2, -2, \ldots\}$
$Z = \{\{0, 1, 2, \ldots,\} \text{ and then } \{-1, -2, \ldots\}\}$

When do you get to $-1$? at infinity?

Need to be careful.

61A — streams!
Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$,
output only if $x \in T$.

Implications:
$\mathbb{Z}^+$ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.

All countably infinite sets have the same cardinality.
Enumeration example.

All binary strings.
\[ B = \{0, 1\}^\ast. \]
\[ B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}. \]
\( \phi \) is empty string.

For any string, it appears at some position in the list. If \( n \) bits, it will appear before position \( 2^{n+1} \).

Should be careful here. 
\[ B = \{\phi; , \, 0, 00, 000, 0000, \ldots\} \]
Never get to 1.