Today.

Finish Welsh-Berlekamp.

Today.

Finish Welsh-Berlekamp.

Countability.

The Scheme.

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

The Scheme.

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

Reed-Solomon Code:

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.
   - $P(1) = m_1, \ldots, P(n) = m_n$.

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.

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

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

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,

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

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

Slow solution.

Brute Force:
For each subset of $n+k$ points
Fit degree $n-1$ polynomial, $Q(x)$, to n of them.

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.

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 $Q(x)$.

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 $P(x)$!

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,

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

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

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
     $\implies P(x) = Q(x)$.

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.

$$\begin{aligned}
(p_{n-1} + \cdots p_0) &\equiv R(1) \pmod{p} \\
&\vdots \\
(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i) \pmod{p} \\
&\vdots \\
(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m) \pmod{p}
\end{aligned}$$

Error Locater Polynomial.

$$
\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}
$$

...so satisfied, I'm on my way.

Error Locater Polynomial.

$$\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}$$

...so satisfied, I'm on my way.

$m = n + 2k$ satisfied equations,

Error Locater Polynomial.

$$\begin{aligned} E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\ &\vdots \\ E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\ &\vdots \\ E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p} \end{aligned}$$

...so satisfied, I'm on my way.

$m = n+2k$ satisfied equations, $n+k$ unknowns.

Error Locater Polynomial.

$$\begin{aligned} E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\ &\vdots \\ E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\ &\vdots \\ E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p} \end{aligned}$$

...so satisfied, I'm on my way.

$m = n + 2k$ satisfied equations, $n + k$ unknowns. But nonlinear!

Error Locater Polynomial.

$$
\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}
$$

...so satisfied, I'm on my way.

$m = n+2k$ satisfied equations, $n+k$ unknowns. But nonlinear!

We have

Error Locater Polynomial.

$$\begin{aligned} E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\ &\vdots \\ E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\ &\vdots \\ E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p} \end{aligned}$$

...so satisfied, I'm on my way.

$m = n + 2k$ satisfied equations, $n + k$ unknowns. But nonlinear!

We have

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

Error Locater Polynomial.

$$
\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}
$$

...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

Error Locater Polynomial.

$$
\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}
$$

...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

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

Error Locater Polynomial.

$$
\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}
$$

...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:

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

Error Locater Polynomial.

$$
\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}
$$

...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:

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

Error Locater Polynomial.

$$\begin{aligned}
E(1)(p_{n-1}+\cdots p_0) &\equiv R(1)E(1) \pmod{p}\\
&\vdots\\
E(i)(p_{n-1}i^{n-1}+\cdots p_0) &\equiv R(i)E(i) \pmod{p}\\
&\vdots\\
E(m)(p_{n-1}(n+2k)^{n-1}+\cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}$$

...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:

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

Error Locater Polynomial.

$$\begin{aligned}
E(1)(p_{n-1} + \cdots p_0) &\equiv R(1)E(1) \pmod{p} \\
&\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) &\equiv R(i)E(i) \pmod{p} \\
&\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) &\equiv R(m)E(m) \pmod{p}
\end{aligned}$$

...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 $E(x)$?

Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree k

Finding $Q(x)$ and $E(x)$?

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

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

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.

Finding $Q(x)$ and $E(x)$?

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

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

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

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 $n+k-1$

Finding $Q(x)$ and $E(x)$?

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

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

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

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

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

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.

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:

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 $E(x)$...

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

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

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

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

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

Gives $n+2k$ linear equations.

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

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

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

Gives $n+2k$ linear equations.

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

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

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

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

Gives $n+2k$ linear equations.

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

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

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

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

Gives $n+2k$ linear equations.

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

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

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 $E(x)$!

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

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 $E(x)$.

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 $E(x)$.

$$\text{Find } P(x) = Q(x)/E(x).$$

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

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

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

Example.

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

Example.

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

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

Example.

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

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

$E(x) = x - b_0$

Example.

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

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

$E(x) = x - b_0$

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

Example.

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

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

$E(x) = x - b_0$

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

$$a_3 + a_2 + a_1 + a_0 \equiv 3(1 - b_0) \pmod 7$$

Example.

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

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

$E(x) = x - b_0$

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

$$\begin{aligned} a_3 + a_2 + a_1 + a_0 &\equiv 3(1 - b_0) \pmod{7} \\ a_3 + 4a_2 + 2a_1 + a_0 &\equiv 1(2 - b_0) \pmod{7} \end{aligned}$$

Example.

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

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

$E(x) = x - b_0$

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

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

Example.

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

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

$E(x) = x - b_0$

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

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

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

Example.

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

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

$E(x) = x - b_0$

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

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

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

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

Example.

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

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

$E(x) = x - b_0$

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

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

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

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

$E(x) = x - 2$.

Example: finishing up.

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

Example: finishing up.

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

Example: finishing up.

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

```
          _________________
x - 2 )   x^3  + 6 x^2 + 6 x + 5
```

Example: finishing up.

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

```
                  1 x^2
            -----------------
x - 2 ) x^3  + 6 x^2 + 6 x + 5
        x^3  - 2 x^2
```

Example: finishing up.

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

```
                 1 x^2
          -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                 1 x^2 + 6 x + 5
```

Example: finishing up.

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

```
                 1 x^2 + 1 x
          -----------------
x - 2 ) x^3  + 6 x^2 + 6 x + 5
        x^3  - 2 x^2
        ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
```

Example: finishing up.

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

```
                 1 x^2 + 1 x
          -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
                 ---------------
                         x + 5
```

Example: finishing up.

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

```
                 1 x^2 + 1 x + 1
         -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
                 ---------------
                           x + 5
                           x - 2
```

Example: finishing up.

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

```
                1 x^2 + 1 x + 1
         -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                1 x^2 + 6 x + 5
                1 x^2 - 2 x
                ---------------
                          x + 5
                          x - 2
                          -----
                              0
```

Example: finishing up.

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

```
                 1 x^2 + 1 x + 1
          -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
                 ---------------
                           x + 5
                           x - 2
                           -----
                               0
```

$P(x) = x^2 + x + 1$

Example: finishing up.

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

```
                 1 x^2 + 1 x + 1
        -----------------
x - 2 ) x^3  + 6 x^2 + 6 x + 5
          x^3  - 2 x^2
          ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
                 ---------------
                           x + 5
                           x - 2
                           -----
                               0
```

$P(x) = x^2 + x + 1$
Message is $P(1) = 3, P(2) = 0, P(3) = 6.$

Example: finishing up.

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

```
                1 x^2 + 1 x + 1
         ----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                1 x^2 + 6 x + 5
                1 x^2 - 2 x
                ---------------
                        x + 5
                        x - 2
                        -----
                            0
```

$P(x) = x^2 + x + 1$
Message is $P(1) = 3, P(2) = 0, P(3) = 6.$

What is $\frac{x-2}{x-2}$?

Example: finishing up.

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

```
                 1 x^2 + 1 x + 1
           ----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
                 ---------------
                         x + 5
                         x - 2
                         -----
                             0
```

$P(x) = x^2 + x + 1$
Message is $P(1) = 3, P(2) = 0, P(3) = 6.$

What is $\frac{x-2}{x-2}$? 1

Example: finishing up.

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

```
                 1 x^2 + 1 x + 1
         -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                 1 x^2 + 6 x + 5
                 1 x^2 - 2 x
                 ---------------
                           x + 5
                           x - 2
                           -----
                               0
```

$P(x) = x^2 + x + 1$
Message is $P(1) = 3, P(2) = 0, P(3) = 6.$

What is $\frac{x-2}{x-2}$? 1
Except at $x = 2$?

Example: finishing up.

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

```
                1 x^2 + 1 x + 1
          -----------------
x - 2 )  x^3  + 6 x^2 + 6 x + 5
         x^3  - 2 x^2
         ----------
                1 x^2 + 6 x + 5
                1 x^2 - 2 x
                ---------------
                          x + 5
                          x - 2
                          -----
                              0
```

$P(x) = x^2 + x + 1$
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 $P(1), \ldots, P(n)$.

Check your undersanding.

You have error locator polynomial!

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor?

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor? Sure.

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor? Sure.
Check all values?

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor? Sure.
Check all values? Sure.

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor? Sure.
Check all values? Sure.

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor? Sure.
Check all values? Sure.

Efficiency?

Check your undersanding.

You have error locator polynomial!

Where oh where have my packets gone wrong?

Factor? Sure.
Check all values? Sure.

Efficiency? Sure.

Check your undersanding.

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.

Check your undersanding.

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?

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

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

Unique solution for $P(x)$

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

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

Proof:

Unique solution for $P(x)$

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

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

Proof:
We claim

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

Equation 2 implies 1:

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

Equation 2 implies 1:

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

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

Equation 2 implies 1:

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

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

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.

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

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.

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

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.

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

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 $\leq n$

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

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!

Unique solution for $P(x)$

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

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

Proof:
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \tag{2}$$

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! $\square$

Last bit.

Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n+2k$ values of x.

Last bit.

Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n+2k$ values of x.

Proof:

Last bit.

Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n+2k$ values of x.

Proof: Construction implies that

Last bit.

Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n+2k$ values of x.

Proof: Construction implies that

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

Last bit.

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

Last bit.

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 $Q(i) = 0$.

Last bit.

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 $Q'(i) = 0$.

Last bit.

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.

Last bit.

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

Last bit.

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

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

Last bit.

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.

Last bit.

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. □

Last bit.

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!

Last bit.

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 $x = 2$.

Yaaay!!!!

Berlekamp-Welsh algorithm decodes correctly when k errors!

Quick Check. Error Correction.

Communicate n packets, with k erasures.

Quick Check. Error Correction.

Communicate n packets, with k erasures.

How many packets?

Quick Check. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$

Quick Check. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$
How to encode?

Quick Check. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$
How to encode? With polynomial, $P(x)$.

Quick Check. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$
How to encode? With polynomial, $P(x)$.
Of degree?

Quick Check. Error Correction.

Communicate n packets, with k erasures.

How many packets? $n+k$
How to encode? With polynomial, $P(x)$.
Of degree? $n-1$

Quick Check. 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?

Quick Check. 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!

Quick Check. 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.

Quick Check. 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?

Quick Check. 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? $n+2k$

Quick Check. 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?

Quick Check. 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 changes to make diff. messages overlap

Quick Check. 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 changes to make diff. messages overlap
How to encode?

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree?

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?
Reconstruct error polynomial, $E(X)$, and $P(x)$!

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?
Reconstruct error polynomial, $E(X)$, and $P(x)$!
Nonlinear equations.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?
Reconstruct error polynomial, $E(X)$, and $P(x)$!
Nonlinear equations.
Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
Recover?
Reconstruct error polynomial, $E(X)$, and $P(x)$!
Nonlinear equations.
Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
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!

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
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! $P(x) = Q(x)/E(x)$!

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
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.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
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.

Quick Check. 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 changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n-1$.
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.

Next up: how big is infinity.

- Countable
- Countably infinite.
- Enumeration

How big are the reals or the integers?

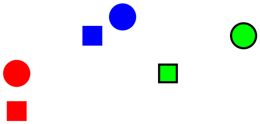
Infinite!

How big are the reals or the integers?

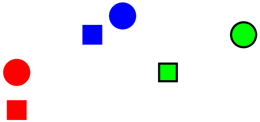
Infinite!

Is one bigger or smaller?

Same size?

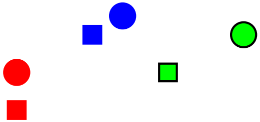


Same size?



Same number?

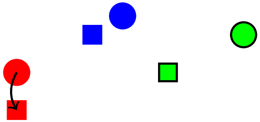
Same size?



Same number?

Make a function f : Circles $\to$ Squares.

Same size?

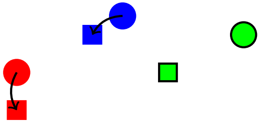


Same number?

Make a function f : Circles $\to$ Squares.

f(red circle) $=$ red square

Same size?



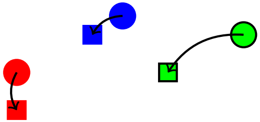
Same number?

Make a function f : Circles $\to$ Squares.

f(red circle) $=$ red square

f(blue circle) $=$ blue square

Same size?



Same number?

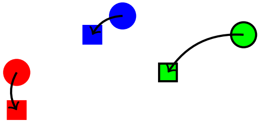
Make a function f : Circles $\rightarrow$ Squares.

f(red circle) $=$ red square

f(blue circle) $=$ blue square

f(circle with black border) $=$ square with black border

Same size?



Same number?

Make a function f : Circles $\rightarrow$ Squares.

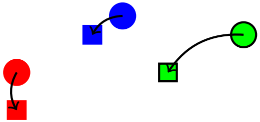
f(red circle) $=$ red square

f(blue circle) $=$ blue square

f(circle with black border) $=$ square with black border

One to one.

Same size?



Same number?

Make a function f : Circles $\rightarrow$ Squares.

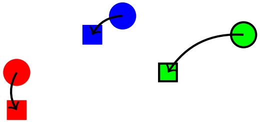
f(red circle) $=$ red square

f(blue circle) $=$ blue square

f(circle with black border) $=$ square with black border

One to one. Each circle mapped to different square.

Same size?



Same number?

Make a function f : Circles $\to$ Squares.

f(red circle) $=$ red square

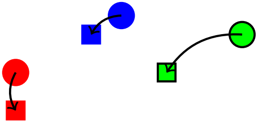
f(blue circle) $=$ blue square

f(circle with black border) $=$ square with black border

One to one. Each circle mapped to different square.

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

Same size?



Same number?

Make a function f : Circles $\rightarrow$ Squares.

f(red circle) $=$ red square

f(blue circle) $=$ blue square

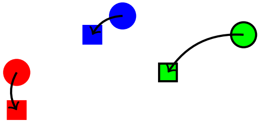
f(circle with black border) $=$ square with black border

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.

Same size?



Same number?

Make a function f : Circles $\rightarrow$ Squares.

f(red circle) $=$ red square

f(blue circle) $=$ blue square

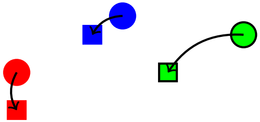
f(circle with black border) $=$ square with black border

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 .

Same size?



Same number?

Make a function f : Circles $\rightarrow$ Squares.

f(red circle) $=$ red square

f(blue circle) $=$ blue square

f(circle with black border) $=$ square with black border

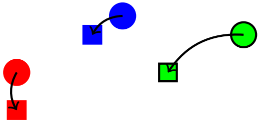
One to one. Each circle mapped to different square.

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 .

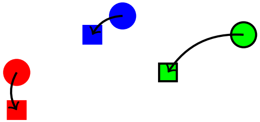
Onto: For all $s \in R$, $\exists c \in D, s = f(c)$.

Same size?



Same number?
Make a function f : Circles $\rightarrow$ Squares.
f(red circle) $=$ red square
f(blue circle) $=$ blue square
f(circle with black border) $=$ 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 $s \in R$, $\exists c \in D, s = f(c)$.

Same size?



Same number?
Make a function f : Circles $\rightarrow$ Squares.
f(red circle) $=$ red square
f(blue circle) $=$ blue square
f(circle with black border) $=$ 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, $|D| = |R|$.

Isomorphism principle.

Given a function, $f : D \rightarrow R$.

Isomorphism principle.

Given a function, $f : D \rightarrow R$.

One to One:

Isomorphism principle.

Given a function, $f : D \to R$.
One to One:
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

Isomorphism principle.

Given a function, $f : D \to R$.
One to One:
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.
or

Isomorphism principle.

Given a function, $f : D \to R$.

One to One:

For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

or

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

Isomorphism principle.

Given a function, $f : D \to R$.
One to One:
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.
or
$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

Isomorphism principle.

Given a function, $f : D \to R$.
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 $y \in R$, $\exists x \in D, y = f(x)$.

Isomorphism principle.

Given a function, $f : D \to R$.
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.

Given a function, $f : D \to R$.
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:

Isomorphism principle.

Given a function, $f : D \to R$.
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 $f : D \to R$ then $|D| = |R|$.

Countable.

How to count?

Countable.

How to count?

0,

Countable.

How to count?

0, 1,

Countable.

How to count?

0, 1, 2,

Countable.

How to count?

0, 1, 2, 3,

Countable.

How to count?

0, 1, 2, 3, ...

Countable.

How to count?

0, 1, 2, 3, $\ldots$

The Counting numbers.

Countable.

How to count?

0, 1, 2, 3, ...

The Counting numbers.
The natural numbers! N

Countable.

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.

Countable.

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**.

Countable.

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?

Where's 0?

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

Where's 0?

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

Natural numbers. 0,

Where's 0?

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

Natural numbers. $0, 1,$

Where's 0?

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

Natural numbers. $0, 1, 2,$

Where's 0?

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

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

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1,$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2,$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3,$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

Where’s 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where’s 0?

More natural numbers!

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

More natural numbers!

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

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

More natural numbers!

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

For any two $z_1 \neq z_2$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

More natural numbers!

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

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

More natural numbers!

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

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

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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!

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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,

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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 $z = n + 1$,

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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 $z = n + 1$, $f(z)$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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 $z = n + 1$, $f(z) = (n + 1) - 1$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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 $z = n + 1$, $f(z) = (n+1) - 1 = n$.

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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 $\mathbb{N}$

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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!

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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?

Where's 0?

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

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

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.

A bijection is a bijection.

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

A bijection is a bijection.

Notice that there is a bijection between N and Z^+ as well.
$f(n) = n + 1$.

A bijection is a bijection.

Notice that there is a bijection between N and Z^+ as well.
$f(n) = n + 1$. $0 \to 1,$

A bijection is a bijection.

Notice that there is a bijection between N and Z^+ as well.
$f(n) = n+1$. $0 \to 1, 1 \to 2,$

A bijection is a bijection.

Notice that there is a bijection between N and Z^+ as well.
$f(n) = n + 1$. $0 \rightarrow 1, 1 \rightarrow 2, \ldots$

A bijection is a bijection.

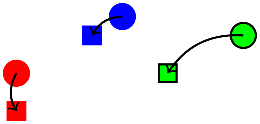
Notice that there is a bijection between N and Z^+ as well.
$f(n) = n+1$. $0 \to 1, 1 \to 2, \ldots$

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

A bijection is a bijection.

Notice that there is a bijection between N and Z^+ as well.
$f(n) = n+1$. $0 \to 1, 1 \to 2, \ldots$

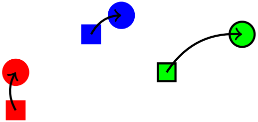
Bijection from A to $B \implies$ a bijection from B to A.



A bijection is a bijection.

Notice that there is a bijection between N and Z^{+} as well.
$f(n) = n+1$. $0 \to 1, 1 \to 2, \ldots$

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

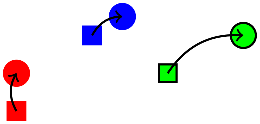


Inverse function!

A bijection is a bijection.

Notice that there is a bijection between N and Z^{+} as well.
$f(n) = n+1$. $0 \to 1, 1 \to 2, \ldots$

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



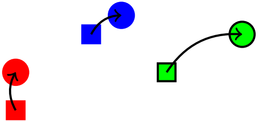
Inverse function!

Can prove equivalence either way.

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?

More large sets.

E - Even natural numbers?

$f : N \rightarrow E$.

More large sets.

E - Even natural numbers?

$f : N \rightarrow E$.

$f(n) \rightarrow 2n$.

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

Onto:

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

Onto: $\forall e \in E$, $f(e/2) = e$.

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

Onto: $\forall e \in E$, $f(e/2) = e$. $e/2$ is natural since e is even

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:

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

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

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

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

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

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.

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

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, Z?

All integers?

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

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

All integers?

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

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

One-to-one: For $x \neq y$

All integers?

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

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

One-to-one: For $x \neq y$
if x is even and y is odd,

All integers?

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

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

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

All integers?

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

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

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 $\implies f(x) \neq f(y)$

All integers?

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

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

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,

All integers?

What about Integers, Z?
Define $f : N \rightarrow Z$.

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

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 $x/2 \neq y/2$

All integers?

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

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

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 $x/2 \neq y/2 \implies f(x) \neq f(y)$

All integers?

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

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

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 $x/2 \neq y/2 \implies f(x) \neq f(y)$
$\ldots.$

All integers?

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

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

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 $x/2 \neq y/2 \implies f(x) \neq f(y)$
$\ldots$.

All integers?

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

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

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 $z \in Z$,

All integers?

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

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

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 $x/2 \neq y/2 \implies f(x) \neq f(y)$
$\dots$.

Onto: For any $z \in Z$,
if $z \geq 0$, $f(2z) = z$ and $2z \in N$.

All integers?

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

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

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 $z \in Z$,
if $z \geq 0$, $f(2z) = z$ and $2z \in N$.
if $z < 0$, $f(2|z|-1) = z$ and $2|z|+1 \in N$.

All integers?

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

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

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 $z \in Z$,
if $z \geq 0$, $f(2z) = z$ and $2z \in N$.
if $z < 0$, $f(2|z| - 1) = z$ and $2|z| + 1 \in N$.

Integers and naturals have same size!

Listings..

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

Listings..

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

Another View:

n	$f(n)$

Listings..

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

Another View:

n	$f(n)$
0	0

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
...	...

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
...	...

Notice that: A listing “is” a bijection with a subset of natural numbers.

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
...	...

Notice that: A listing “is” a bijection with a subset of natural numbers.
Function $\equiv$ “Position in list.”

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
...	...

Notice that: A listing “is” a bijection with a subset of natural numbers.
Function $\equiv$ “Position in list.”
If finite: bijection with $\{0, \ldots, |S| - 1\}$

Listings..

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

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
...	...

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 N.

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",
"Output next element of S"

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",
"Output next element of S"
...

Enumerability $\equiv$ countability.

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.

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",
"Output next element of S"
$\dots$
Any element x of S has *specific, finite* position in list.
$Z = \{0,$

Enumerability $\equiv$ countability.

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.
$Z = \{0, 1,$

Enumerability $\equiv$ countability.

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.
$Z = \{0, 1, -1,$

Enumerability $\equiv$ countability.

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.
$Z = \{0, 1, -1, 2,$

Enumerability $\equiv$ countability.

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.
$Z = \{0, 1, -1, 2, -2,$

Enumerability $\equiv$ countability.

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.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of *S*",
"Output next element of *S*"
$\ldots$
Any element x of S has *specific, finite* position in list.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$
$Z = \{\{0, 1, 2, \ldots, \}$

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",
"Output next element of S"
$\ldots$
Any element x of S has *specific, finite* position in list.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$
$Z = \{\{0, 1, 2, \ldots, \}$ and then $\{-1, -2, \ldots\}\}$

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of *S*",
"Output next element of *S*"
$\ldots$
Any element x of S has *specific, finite* position in list.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$
$Z = \{\{0, 1, 2, \ldots,\}$ and then $\{-1, -2, \ldots\}\}$

When do you get to -1?

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

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

$\ldots$

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

$Z = \{0, 1, -1, 2, -2, \ldots..\}$

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

When do you get to -1? at infinity?

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",
"Output next element of S"
$\ldots$
Any element x of S has *specific, finite* position in list.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$
$Z = \{\{0, 1, 2, \ldots,\}$ and then $\{-1, -2, \ldots\}\}$

When do you get to -1? at infinity?

Need to be careful.

Enumerability $\equiv$ countability.

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

When do you get to -1? at infinity?

Need to be careful.

61A

Enumerability $\equiv$ countability.

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.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$
$Z = \{\{0, 1, 2, \ldots,\}$ 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.

Countably infinite subsets.

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

Enumerate T as follows:

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,

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 $x \in T$.

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 $x \in T$.

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:

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:
Z^+ is countable.

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:
Z^+ is countable.
It is infinite since the list goes on.

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:
Z^+ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.

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:
Z^+ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.

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:
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.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi,$

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0,$

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1,$

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00,$

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11,$

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ is empty string.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ is empty string.

For any string, it appears at some position in the list.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ 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}.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ 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.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ 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.

$B = \{\phi;, 0, 00, 000, 0000, ...\}$

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ 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.

$B = \{\phi; , 0, 00, 000, 0000, ...\}$
Never get to 1.