Lecture 11: Countability

Infinity is weeeeeeird

What Is "Same Size"?

Consider two sets:

$\{1, 2, 3, 4\}$

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

What Is "Same Size"?

Consider two sets:

$\{1, 2, 3, 4\}$

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

Are these the same size?

What Is “Same Size”?

Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What Is "Same Size"?

Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What about:
$\mathbb{Z}^+ = \{1, 2, 3, 4, ...\}$
$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

What Is "Same Size"?

Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What about:
$\mathbb{Z}^+ = \{1, 2, 3, 4, ...\}$
$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

$\mathbb{N}$ has an extra element...

What Is "Same Size"?

Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What about:
$\mathbb{Z}^+ = \{1, 2, 3, 4, ...\}$
$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

$\mathbb{N}$ has an extra element...but both are infinite?

What Is "Same Size"?

Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What about:
$\mathbb{Z}^+ = \{1, 2, 3, 4, ...\}$
$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

$\mathbb{N}$ has an extra element...but both are infinite?
Is $\infty + 1 = \infty$?

What Is “Same Size”?

Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What about:
$\mathbb{Z}^+ = \{1, 2, 3, 4, ...\}$
$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

$\mathbb{N}$ has an extra element...but both are infinite?
Is $\infty + 1 = \infty$?
????

What Is “Same Size”?

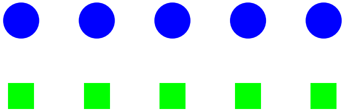
Consider two sets:
$\{1, 2, 3, 4\}$
$\{0, 1, 2, 3, 4\}$

Are these the same size?
No! Second set has an extra element!

What about:
$\mathbb{Z}^+ = \{1, 2, 3, 4, ...\}$
$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

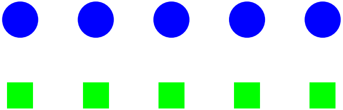
$\mathbb{N}$ has an extra element...but both are infinite?
Is $\infty + 1 = \infty$?
????
Need different way to think about “size”

Finite Example



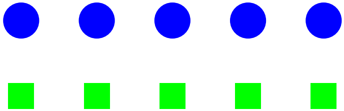
Are there same number of circles and squares?

Finite Example



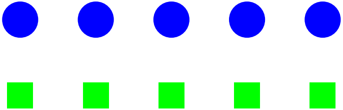
Are there same number of circles and squares?
How do we know?

Finite Example



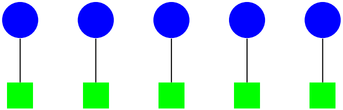
Are there same number of circles and squares?
How do we know? I can't count to 5...

Finite Example

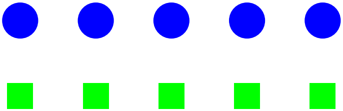


Are there same number of circles and squares?
How do we know? I can't count to 5...

Idea: Draw lines between squares and circles

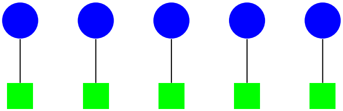


Finite Example



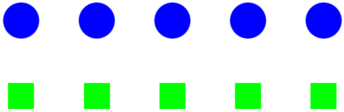
Are there same number of circles and squares?
How do we know? I can't count to 5...

Idea: Draw lines between squares and circles



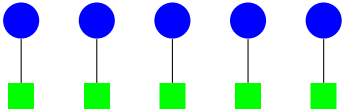
Only possible if same number of squares and circles!

Finite Example



Are there same number of circles and squares?
How do we know? I can't count to 5...

Idea: Draw lines between squares and circles



Only possible if same number of squares and circles!

How to generalize to infinite sets?

Bijections and Size

Idea: sets "same size" if $\exists$ bijection between them

Bijections and Size

Idea: sets "same size" if $\exists$ bijection between them

Does this make sense for finite sets?

Bijections and Size

Idea: sets "same size" if $\exists$ bijection between them

Does this make sense for finite sets?

Suppose have bijection $b : \{1, 2, 3\} \to S$
How many elements in S?

Bijections and Size

Idea: sets "same size" if $\exists$ bijection between them

Does this make sense for finite sets?

Suppose have bijection $b : \{1, 2, 3\} \to S$
How many elements in S?
$S = \{b(1), b(2), b(3)\}$, so 3 elements as well!

Bijections and Size

Idea: sets "same size" if $\exists$ bijection between them

Does this make sense for finite sets?

Suppose have bijection $b : \{1, 2, 3\} \to S$
How many elements in S?
$S = \{b(1), b(2), b(3)\}$, so 3 elements as well!

Bijections capture the "same num of elts" idea
But also makes sense for infinite sets!

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$
Why?

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$
Why? Has inverse $f^{-1}(y) = y - 1$

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$
Why? Has inverse $f^{-1}(y) = y - 1$

But what about $f(x) = x$? Not onto!

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$
Why? Has inverse $f^{-1}(y) = y - 1$

But what about $f(x) = x$? Not onto!
Don't need all functions bijective! Only need one.

---

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$
Why? Has inverse $f^{-1}(y) = y - 1$

But what about $f(x) = x$? Not onto!
Don't need all functions bijective! Only need one.

Adding one elt to infinite set doesn't seem to change size...

[1] Here $|S|$ means the cardinality or "size" of S

Same Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}^+|$[1]

How can we prove this?
Need a bijection!

Claim: $f(x) = x + 1$ is bijection $\mathbb{N} \to \mathbb{Z}^+$
Why? Has inverse $f^{-1}(y) = y - 1$

But what about $f(x) = x$? Not onto!
Don't need all functions bijective! Only need one.

Adding one elt to infinite set doesn't seem to change size...what if we added more?

[1]Here $|S|$ means the cardinality or "size" of S

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \rightarrow 0$

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \rightarrow 0$

$1 \rightarrow 1$

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \to 0$

$1 \to 1$

$2 \to -1$

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \rightarrow 0$

$1 \rightarrow 1$

$2 \rightarrow -1$

$3 \rightarrow 2$

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \rightarrow 0$

$1 \rightarrow 1$

$2 \rightarrow -1$

$3 \rightarrow 2$

$4 \rightarrow -2$

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \to 0$

$1 \to 1$

$2 \to -1$

$3 \to 2$

$4 \to -2$

...

More Infinities

Claim: $|\mathbb{N}| = |\mathbb{Z}|$

How can we map from $\mathbb{N}$ to $\mathbb{Z}$?

$0 \to 0$

$1 \to 1$

$2 \to -1$

$3 \to 2$

$4 \to -2$

...

Take $f(x) = \begin{cases} \frac{x+1}{2} & x \text{ is odd} \\ -\frac{x}{2} & x \text{ is even} \end{cases}$

Inverse is $f^{-1}(y) = \begin{cases} 2y - 1 & y > 0 \\ -2y & y \leq 0 \end{cases}$

Bijection Alternatives

Explicitly stating a bijection can be a pain...

Bijection Alternatives

Explicitly stating a bijection can be a pain...
What alternatives do we have?

Bijection Alternatives

Explicitly stating a bijection can be a pain...
What alternatives do we have?

To prove $|S| = |\mathbb{N}|$, can give *enumeration* of S:
List "1st" elt of S, then "2nd", then "3rd", etc.
Need to eventually hit every element

Bijection Alternatives

Explicitly stating a bijection can be a pain...
What alternatives do we have?

To prove $|S| = |\mathbb{N}|$, can give *enumeration* of S:
List "1st" elt of S, then "2nd", then "3rd", etc.
Need to eventually hit every element

Ex: For $\mathbb{Z}$, can enumerate as
$0, 1, -1, 2, -2, 3, -3, \ldots$

Bijection Alternatives

Explicitly stating a bijection can be a pain...
What alternatives do we have?

To prove $|S| = |\mathbb{N}|$, can give *enumeration* of S:
List "1st" elt of S, then "2nd", then "3rd", etc.
Need to eventually hit every element

Ex: For $\mathbb{Z}$, can enumerate as
$0, 1, -1, 2, -2, 3, -3, \ldots$

Careful — need finite position for any element!
Ex: $0, 1, 2, \ldots, -1, -2, -3, \ldots$ *not* valid for $\mathbb{Z}$

Enumeration Example

Definition: $\{0,1\}^*$ is set of finite bit strings

Enumeration Example

Definition: $\{0,1\}^*$ is set of finite bit strings

Theorem: $|\{0,1\}^*| = |\mathbb{N}|$

Enumeration Example

Definition: $\{0,1\}^*$ is set of finite bit strings

Theorem: $|\{0,1\}^*| = |\mathbb{N}|$

Could give bijection, but lots of words

Enumeration Example

Definition: $\{0,1\}^*$ is set of finite bit strings

Theorem: $|\{0,1\}^*| = |\mathbb{N}|$

Could give bijection, but lots of words

Instead, enumerate:
$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, \ldots$

Enumeration Example

Definition: $\{0,1\}^*$ is set of finite bit strings

Theorem: $|\{0,1\}^*| = |\mathbb{N}|$

Could give bijection, but lots of words

Instead, enumerate:
$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, \ldots$

Any string *with finite length* hit eventually!

Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

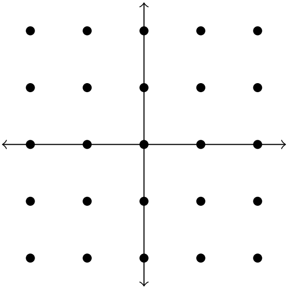
Should be surprising — seems like many more pairs!

Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

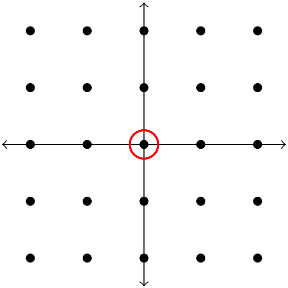


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

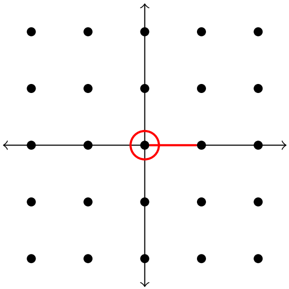


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

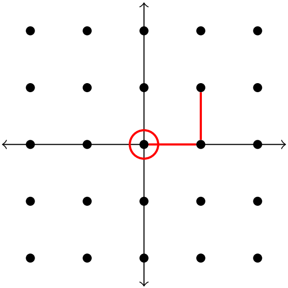


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

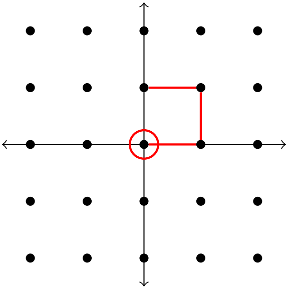


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

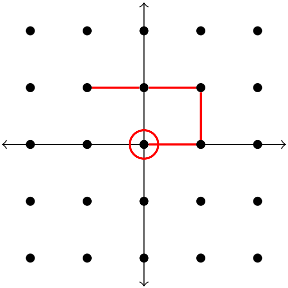


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

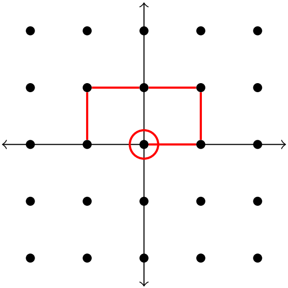


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

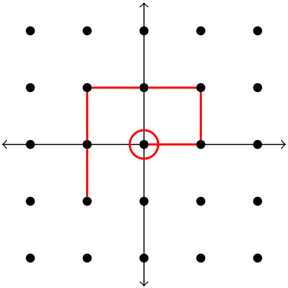


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

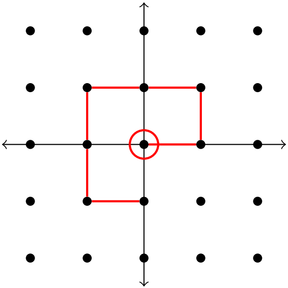


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

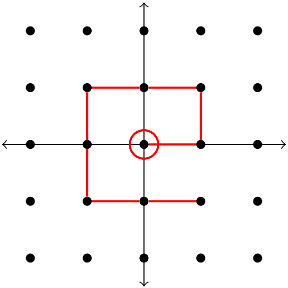


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

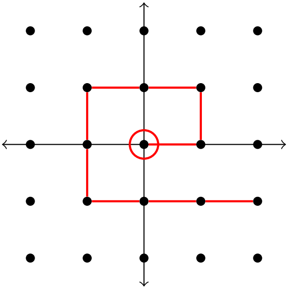


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

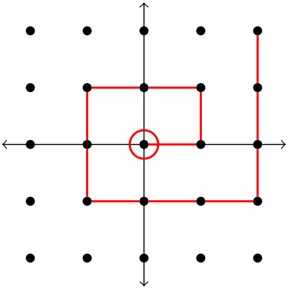


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

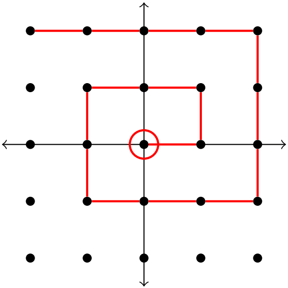


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

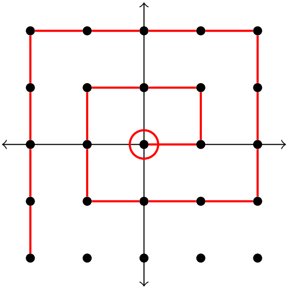


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

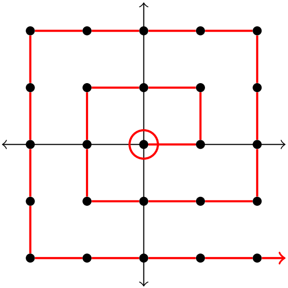


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:

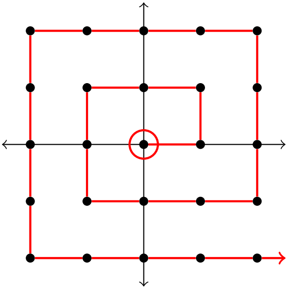


Have Some More Enumeration

Theorem: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Should be surprising — seems like many more pairs!

Proof by picture:



Gives an enumeration of $\mathbb{Z} \times \mathbb{Z}$!

Be Rational!

How does $|\mathbb{Q}|$ compare to $|\mathbb{Z} \times \mathbb{Z}|$?

Be Rational!

How does $|\mathbb{Q}|$ compare to $|\mathbb{Z} \times \mathbb{Z}|$?

Can create function $f\colon \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ as follows:
If $q = \frac{a}{b}$ in lowest terms, $f(q) = (a, b)$

Be Rational!

How does $|\mathbb{Q}|$ compare to $|\mathbb{Z} \times \mathbb{Z}|$?

Can create function $f \colon \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ as follows:
If $q = \frac{a}{b}$ in lowest terms, $f(q) = (a, b)$
$f(2) = (2, 1)$, $f(0.25) = (1, 4)$, $f(0.\overline{66}) = (2, 3)$, etc.

Be Rational!

How does $|\mathbb{Q}|$ compare to $|\mathbb{Z} \times \mathbb{Z}|$?

Can create function $f\colon \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ as follows:
If $q = \frac{a}{b}$ in lowest terms, $f(q) = (a, b)$
$f(2) = (2, 1)$, $f(0.25) = (1, 4)$, $f(0.\overline{66}) = (2, 3)$, etc.

Is f a bijection?

Be Rational!

How does $|\mathbb{Q}|$ compare to $|\mathbb{Z} \times \mathbb{Z}|$?

Can create function $f\colon \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ as follows:
If $q = \frac{a}{b}$ in lowest terms, $f(q) = (a, b)$
$f(2) = (2, 1)$, $f(0.25) = (1, 4)$, $f(0.\overline{66}) = (2, 3)$, etc.

Is f a bijection?
No! Not onto (eg $(1, 0)$, $(-1, -1)$, $(2, 4)$, ...)

Be Rational!

How does $|\mathbb{Q}|$ compare to $|\mathbb{Z} \times \mathbb{Z}|$?

Can create function $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ as follows:
If $q = \frac{a}{b}$ in lowest terms, $f(q) = (a, b)$
$f(2) = (2, 1)$, $f(0.25) = (1, 4)$, $f(0.\overline{66}) = (2, 3)$, etc.

Is f a bijection?
No! Not onto (eg $(1, 0)$, $(-1, -1)$, $(2, 4)$, ...)

But notice: is one-to-one
Can we conclude anything from this?

What Is An Outjection?

Cantor-Schröder-Bernstein Theorem

If $\exists$ injections $f\colon A \to B$ and $g : B \to A$, $\exists$ bijection

What Is An Outjection?

Cantor-Schröder-Bernstein Theorem

If $\exists$ injections $f : A \to B$ and $g : B \to A$, $\exists$ bijection

Proof in Bonus Lecture tomorrow!

What Is An Outjection?

Cantor-Schröder-Bernstein Theorem

If $\exists$ injections $f : A \rightarrow B$ and $g : B \rightarrow A$, $\exists$ bijection

Proof in Bonus Lecture tomorrow!

What does this mean to us?

What Is An Outjection?

Cantor-Schröder-Bernstein Theorem
If $\exists$ injections $f\colon A \to B$ and $g: B \to A$, $\exists$ bijection

Proof in Bonus Lecture tomorrow!

What does this mean to us?
Can say $|A| \leq |B|$ if $\exists$ injection $f\colon A \to B$
If $|A| \leq |B|$ and $|B| \leq |A|$, CSB says $|A| = |B|$!

What Is An Outjection?

Cantor-Schröder-Bernstein Theorem

If $\exists$ injections $f \colon A \to B$ and $g : B \to A$, $\exists$ bijection

Proof in Bonus Lecture tomorrow!

What does this mean to us?
Can say $|A| \leq |B|$ if $\exists$ injection $f \colon A \to B$
If $|A| \leq |B|$ and $|B| \leq |A|$, CSB says $|A| = |B|$!

Note: Have inject $A \to B$ iff have surject $B \to A$

What Is An Outjection?

Cantor-Schröder-Bernstein Theorem
If $\exists$ injections $f: A \to B$ and $g: B \to A$, $\exists$ bijection

Proof in Bonus Lecture tomorrow!

What does this mean to us?
Can say $|A| \leq |B|$ if $\exists$ injection $f: A \to B$
If $|A| \leq |B|$ and $|B| \leq |A|$, CSB says $|A| = |B|$!

Note: Have inject $A \to B$ iff have surject $B \to A$
So surjection $B \to A$ means $|B| \geq |A|$!

Back To $\mathbb{Q}$

Previously: found injection $\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$

Back To $\mathbb{Q}$

Previously: found injection $\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$
Hence, $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Back To $\mathbb{Q}$

Previously: found injection $\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$
Hence, $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Notice, have injection $\mathbb{N} \to \mathbb{Q}$ by "inclusion"
So $|\mathbb{N}| \leq |\mathbb{Q}|$

Back To $\mathbb{Q}$

Previously: found injection $\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$
Hence, $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$

Notice, have injection $\mathbb{N} \to \mathbb{Q}$ by “inclusion”
So $|\mathbb{N}| \leq |\mathbb{Q}|$

Thus $|\mathbb{Q}| = |\mathbb{N}|$!

Brake

Time for a 4-minute break!

Brake

Time for a 4-minute break!

Today's Discussion Question:
https://tinyurl.com/70-discussion-q

Countability

Say a set S is *countable* if $|S| \leq |\mathbb{N}|$

Countability

Say a set S is *countable* if $|S| \leq |\mathbb{N}|$

So far, all sets we've seen are countable!

Countability

Say a set S is *countable* if $|S| \leq |\mathbb{N}|$
So far, all sets we've seen are countable!

Natural question: are all sets countable?

Countability

Say a set S is *countable* if $|S| \leq |\mathbb{N}|$
So far, all sets we've seen are countable!

Natural question: are all sets countable?
Turns out, no!

Not With That Attitude You Cant-or

Def: Let $\{0, 1\}^\infty$ be set of *infinite length* bit strings

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
⋮	⋮

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
⋮	⋮

Consider $s = 1$

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
⋮	⋮

Consider $s = 11$

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
⋮	⋮

Consider $s = 110$

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
⋮	⋮

Consider $s = 1101$

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 …
1	1 0 1 0 1 …
2	1 1 1 0 1 …
3	0 1 0 0 0 …
$\vdots$	$\vdots$

Consider $s = 1101\ldots$

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 …
1	1 0 1 0 1 …
2	1 1 1 0 1 …
3	0 1 0 0 0 …
⋮	⋮

Consider $s = 1101\ldots$

$s \neq o(n)$ for all n!

Not With That Attitude You Cant-or

Def: Let $\{0,1\}^\infty$ be set of *infinite length* bit strings
Theorem: $|\{0,1\}^\infty| > |\mathbb{N}|$

Proof:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \{0,1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
⋮	⋮

Consider $s = 1101\ldots$

$s \neq o(n)$ for all n!

Method known as *Cantor Diagonalization*

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
⋮	⋮

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
$\vdots$	$\vdots$

Consider $r = .1$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
$\vdots$	$\vdots$

Consider $r = .10$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

“Proof”:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
$\vdots$	$\vdots$

Consider $r = .100$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

“Proof”:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
⋮	⋮

Consider $r = .1000$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
⋮	⋮

Consider $r = .1000\ldots$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

“Proof”:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
$\vdots$	$\vdots$

Consider $r = .1000...$

$r \neq o(n)$ for all n!

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

“Proof”:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 …
1	.1 9 2 9 3 …
2	.0 0 9 0 0 …
3	.2 3 5 9 6 …
⋮	⋮

Consider $r = .1000\ldots$

$r \neq o(n)$ for all n!

So we've proved $|[0,1]| > |\mathbb{N}|$

I Cant-or Think Of A Better Pun

Theorem: $|\mathbb{R}| > |\mathbb{N}|$
Will in fact prove $|[0,1]| > |\mathbb{N}|$

“Proof”:
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to [0,1]$

n	$o(n)$
0	.0 9 9 9 9 ...
1	.1 9 2 9 3 ...
2	.0 0 9 0 0 ...
3	.2 3 5 9 6 ...
$\vdots$	$\vdots$

Consider $r = .1000\ldots$

$r \neq o(n)$ for all n!

So we’ve proved $|[0,1]| > |\mathbb{N}|$ ...or have we?

Oops

Slight subtlety with $\mathbb{R}$:
Decimal expansion not always unique!

Oops

Slight subtlety with $\mathbb{R}$:
Decimal expansion not always unique!

Eg, $.09999... = .10000...$

Oops

Slight subtlety with $\mathbb{R}$:
Decimal expansion not always unique!

Eg, $.09999... = .10000...$

$+1$ to daig ensures different decimal expansion
Not necessarily different number!

Oops

Slight subtlety with $\mathbb{R}$:
Decimal expansion not always unique!

Eg, $.09999... = .10000...$

$+1$ to daig ensures different decimal expansion
Not necessarily different number!

In our picture, $o(0) = 0.999... = .1000... = r$

Oops

Slight subtlety with $\mathbb{R}$:
Decimal expansion not always unique!

Eg, $.09999... = .10000...$

$+1$ to daig ensures different decimal expansion
Not necessarily different number!

In our picture, $o(0) = 0.999... = .1000... = r$

Easily recoverable: just do $+2$ instead of $+1$

Oops

Slight subtlety with $\mathbb{R}$:
Decimal expansion not always unique!

Eg, $.09999... = .10000...$

$+1$ to daig ensures different decimal expansion
Not necessarily different number!

In our picture, $o(0) = 0.999... = .1000... = r$

Easily recoverable: just do $+2$ instead of $+1$

Moral: be careful when claiming $r \neq o(n)$!

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
⋮	⋮

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
⋮	⋮

Consider $q = .3$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":

Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
$\vdots$	$\vdots$

Consider $q = .31$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0,1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
⋮	⋮

Consider $q = .314$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
⋮	⋮

Consider $q = .3141$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
$\vdots$	$\vdots$

Consider $q = .3141...$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0,1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
$\vdots$	$\vdots$

Consider $q = .3141...$

$q \neq o(n)$ for all n!

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
⋮	⋮

Consider $q = .3141...$

$q \neq o(n)$ for all n!

So we've proved $|\mathbb{Q} \cap [0, 1]| > |\mathbb{N}|$

Not Recoverable

"Theorem": $|\mathbb{Q}| > |\mathbb{N}|$

"Proof":
Suppose for contra $\exists$ onto fn $o : \mathbb{N} \to \mathbb{Q} \cap [0, 1]$

n	$o(n)$
0	.1 9 1 9 1 ...
1	.5 9 2 2 2 ...
2	.0 0 2 0 0 ...
3	.6 9 5 9 5 ...
$\vdots$	$\vdots$

Consider $q = .3141...$

$q \neq o(n)$ for all n!

So we've proved $|\mathbb{Q} \cap [0, 1]| > |\mathbb{N}|$ ...or have we?

Double Oops

How do we know that q is rational?

Double Oops

How do we know that q is rational? We don't!

Double Oops

How do we know that q is rational? We don't!
In picture, $q = \frac{\pi}{10} \notin \mathbb{Q}$

Double Oops

How do we know that q is rational? We don't!
In picture, $q = \frac{\pi}{10} \notin \mathbb{Q}$

Doesn't matter that $q \neq o(n)$
Not trying to cover q!

Double Oops

How do we know that q is rational? We don't!
In picture, $q = \frac{\pi}{10} \notin \mathbb{Q}$

Doesn't matter that $q \neq o(n)$
Not trying to cover q!

This proof not recoverable — $|\mathbb{Q}| = |\mathbb{N}|$

Double Oops

How do we know that q is rational? We don't!
In picture, $q = \frac{\pi}{10} \notin \mathbb{Q}$

Doesn't matter that $q \neq o(n)$
Not trying to cover q!

This proof not recoverable — $|\mathbb{Q}| = |\mathbb{N}|$

Moral: make sure construct in required set!

Fin

Next time: computability!