

Monday November 15

We have the following subset relationships between sets of numbers:

$$\mathbb{Z}^+ \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

Which of the proper subset inclusions above can you prove? **All**

Witnesses :
for proper
subset inclusion

$$0 \in \mathbb{N} - \mathbb{Z}^+$$

$$-1 \in \mathbb{Z} - \mathbb{N}$$

$$0.5 \in \mathbb{Q} - \mathbb{Z}$$

$$\sqrt{2} \in \mathbb{R} - \mathbb{Q}$$

Definition: A finite set is one whose distinct elements can be counted by a natural number.

Notice : $\mathbb{Z}^+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ each not finite i.e. infinite.

Motivating question: when can we say one set is *bigger than* another?

Which is bigger?

- The set $\{1, 2, 3\}$ or the set $\{0, 1, 2, 3\}$?
- The set $\{0, \pi, \sqrt{2}\}$ or the set $\{\mathbb{N}, \mathbb{R}, \emptyset\}$?
- The set \mathbb{N} or the set \mathbb{R}^+ ?

$$|\{1, 2, 3\}| = 3 \quad |\{0, 1, 2, 3\}| = 4$$

correspondence between elements



Which of the sets above are finite? infinite? **\mathbb{N}, \mathbb{R}^+ both infinite sets.**
size of sets

Key idea for cardinality: Counting distinct elements is a way of labelling elements with natural numbers. This is a function! In general, functions let us associate elements of one set with those of another. If the association is "good", we get a correspondence between the elements of the ~~subsets~~ which can relate the sizes of the sets.

Analogy: Musical chairs



People try to sit down when the music stops

Person ☺ sits in Chair 1, Person ☻ sits in Chair 2,

Person ☹ is left standing!

What does this say about the number of chairs and the number of people?

Recall that a function is defined by its (1) domain, (2) codomain, and (3) rule assigning each element in the domain exactly one element in the codomain. The domain and codomain are nonempty sets. The rule can be depicted as a table, formula, English description, etc.

A function can *fail to be well-defined* if there is some domain element where the function rule doesn't give a unique codomain element. For example, the function rule might lead to more than one potential image, or to an image outside of the codomain.

Example: $f_A : \mathbb{R}^+ \rightarrow \mathbb{Q}$ with $f_A(x) = x$ is **not** a well-defined function because

$\sqrt{2} \in \mathbb{R}^+$ so applying rule $f_A(\sqrt{2}) = \sqrt{2}$
gives an element outside codomain.

Example: $f_B : \mathbb{Q} \rightarrow \mathbb{Z}$ with $f_B\left(\frac{p}{q}\right) = p + q$ is **not** a well-defined function because

$$x = 0.5 = \frac{1}{2} = \frac{2}{4}$$

$$f_B(x) = f_B\left(\frac{1}{2}\right) = 1+2=3 \quad \text{not unique image.}$$

$$f_B(x) = f_B\left(\frac{2}{4}\right) = 2+4=6$$

Example: $f_C : \mathbb{Z} \rightarrow \mathbb{R}$ with $f_C(x) = \frac{x}{|x|}$ is **not** a well-defined function because

Notice $x = -1$ gives $f_C(x) = \frac{-1}{|-1|} = -1$
 $y = -2$ gives $f_C(y) = \frac{-2}{|-2|} = -1$ ok.

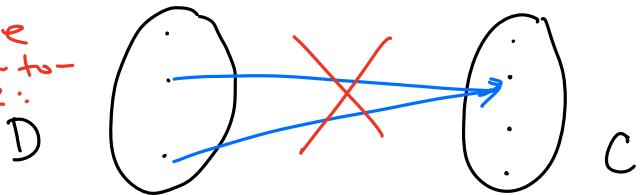
But when $z = 0$ gives $f_C(z) = \frac{0}{|0|} = \frac{0}{0}$ uhh.

Definition : A function $f : D \rightarrow C$ is **one-to-one** (or injective) means for every a, b in the domain D , if $f(a) = f(b)$ then $a = b$.

Formally, $f : D \rightarrow C$ is one-to-one means $\forall a \in D \forall b \in D (f(a) = f(b) \rightarrow a = b)$ i.e.

Informally, a function being one-to-one means "no duplicate images".

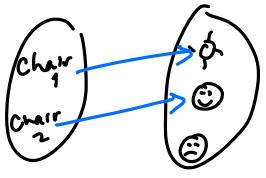
Failure
of one-to-one:



$$\forall a \in D \forall b \in D (a \neq b \rightarrow f(a) \neq f(b))$$

Definition: For nonempty sets A, B , we say that the **cardinality of A is no bigger than the cardinality of B** , and write $|A| \leq |B|$, to mean there is a one-to-one function with domain A and codomain B . Also, we define $|\emptyset| \leq |B|$ for all sets B .

In the analogy: The function $sitter : \{Chair1, Chair2\} \rightarrow \{Person\diamond, Person\odot, Person\circledcirc\}$ given by $sitter(Chair1) = Person\diamond$, $sitter(Chair2) = Person\odot$, is one-to-one and witnesses that



$$|\{Chair1, Chair2\}| \leq |\{Person\diamond, Person\odot, Person\circledcirc\}|$$

Let S_2 be the set of RNA strands of length 2, formally $S_2 = \{s \in S \mid rnalen(s) = 2\}$.

True or False: $|\{A, U, G, C\}| \leq |S_2|$

Why?

with rule

Define function

Input	Output
A	CG
U	AA
G	UG
C	CU

$$f: \{A, U, G, C\} \rightarrow S_2$$

This function is one-to-one, thus it witnesses size relationship.

Details: prove 1-1

Notice $16 \leq 16$

True or False: $|\{A, U, G, C\} \times \{A, U, G, C\}| \leq |S_2|$

Why?

Define function $f: B \times B \rightarrow S_2$

where $f(b_1, b_2) = b_1 b_2$ for $b_1, b_2 \in B$
This function is one-to-one and therefore, it witnesses size relationship

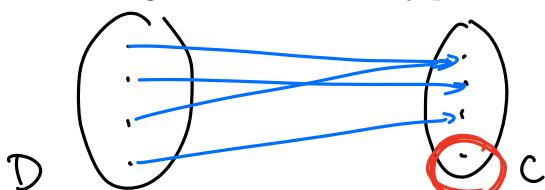
Details: prove 1-1.

Definition: A function $f : D \rightarrow C$ is **onto** (or surjective) means for every b in the codomain, there is an element a in the domain with $f(a) = b$.

Formally, $f : D \rightarrow C$ is onto means $\forall b \in C \exists a \in D (f(a) = b)$

Informally, a function being onto means "every potential image is an actual image".

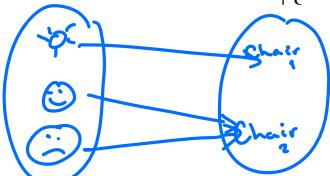
Failure of onto:



Definition: For nonempty sets A, B , we say that the cardinality of A is no smaller than the cardinality of B , and write $|A| \geq |B|$, to mean there is an onto function with domain A and codomain B . Also, we define $|A| \geq |\emptyset|$ for all sets A .

In the analogy: The function $triedToSit : \{Person\diamond, Person\odot, Person\circledcirc\} \rightarrow \{Chair1, Chair2\}$ given by $triedToSit(Person\diamond) = Chair1$, $triedToSit(Person\odot) = Chair2$, $triedToSit(Person\circledcirc) = Chair2$, is onto and witnesses that

$$|\{Person\diamond, Person\odot, Person\circledcirc\}| \geq |\{Chair1, Chair2\}|$$



Let S_2 be the set of RNA strands of length 2.

True or False: $|S_2| \geq |\{A, U, G, C\}|$

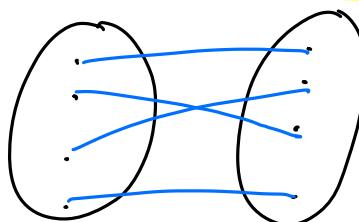
Why? Define the function $g: S_2 \rightarrow \{A, U, G, C\}$ by
 $g(s) = \text{(leftmost base in } s\text{)} \text{, for } s \in S_2.$

To prove g is onto we need to show
 $\forall b \in \{A, U, G, C\} \exists s \in S_2 (g(s) = b)$. Let b be arbitrary, pick witness
 $s = bU$. Then $g(s) = \text{leftmost base in } bU = b$, as required.

True or False: $|S_2| \geq |\{A, U, G, C\} \times \{A, U, G, C\}|$

Why? Define the function $\tilde{g}: S_2 \rightarrow B \times B$ by
 $\tilde{g}(s) = (\text{(leftmost base in } s\text{), rightmost base in } s\text{)}$
To prove \tilde{g} is onto, consider arbitrary $(b_1, b_2) \in B \times B$
let $x = b_1b_2$. WTS $\tilde{g}(x) = (b_1, b_2)$. By definition
 $\tilde{g}(x) = \tilde{g}(b_1b_2) = (b_1, b_2)$ as required.

Definition: A function $f: D \rightarrow C$ is a **bijection** means that it is both one-to-one and onto. The **inverse** of a bijection $f: D \rightarrow C$ is the function $g: C \rightarrow D$ such that $g(b) = a$ iff $f(a) = b$.



Cardinality of sets

For nonempty sets A, B we say

$|A| \leq |B|$ means there is a one-to-one function with domain A , codomain B

$|A| \geq |B|$ means there is an onto function with domain A , codomain B

$|A| = |B|$ means there is a bijection with domain A , codomain B

For all sets A , we say $|A| = |\emptyset|$, $|\emptyset| = |A|$ if and only if $A = \emptyset$.

Caution: we use familiar symbols to define cardinality, like $|\quad| \leq |\quad|$ and $|\quad| \geq |\quad|$ and $|\quad| = |\quad|$, but the meaning of these symbols depends on context. We've seen that vertical lines can mean absolute value (for real numbers), divisibility (for integers), and now sizes (for sets).

Now we see that \leq and \geq can mean comparing numbers or comparing sizes of sets. When the sets being compared are finite, the definitions of $|A| \leq |B|$ agree.

But, properties of numbers cannot be assumed when comparing cardinalities of infinite sets.

In a nutshell: cardinality of sets is defined via functions. This definition agrees with the usual notion of "size" for finite sets.

Review

1.

Select all and only the **finite** sets below.

- (a) $X = \{a, b, c\}$
- (b) $Y = \{1, 2, 3, 4, 5\}$
- (c) $Z = \{10, 20, 30\}$
- (d) \emptyset
- (e) \mathbb{Z}
- (f) $\{\emptyset\}$
- (g) $\{\mathbb{Z}\}$

2.

Consider the following input-output definition tables with $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4, 5\}$ and $Z = \{10, 20, 30\}$

Table 1	
Input	Output
1	10
2	20
3	30

Table 2	
Input	Output
a	1
b	4
c	5

Table 3	
Input	Output
10	a
20	b
30	a

- (a) Select all and only the tables that each define a well-defined function whose domain and codomain is each X , Y , or Z .
- (b) Select all and only the tables that each define a well-defined function (with domain X or Y or Z and with codomain X or Y or Z) and that is one-to-one.
- (c) Select all and only the tables that each define a well-defined function (with domain X or Y or Z and with codomain X or Y or Z) and that is onto.

3.

Consider the following functions:

$f : \mathbb{Z} \rightarrow \mathbb{N}$ $f(n) = \begin{cases} 0 & \text{when } n = 0 \\ (-2 \cdot n) - 1 & \text{when } n < 0 \\ 2 \cdot n & \text{when } n > 0 \end{cases}$	$g : \mathbb{Z} \rightarrow \mathbb{N}$ $g(n) = \begin{cases} -1 \cdot n & \text{when } n < 0 \\ n & \text{when } n \geq 0 \end{cases}$
$h : \mathbb{N} \rightarrow \mathbb{Z}$ $h(n) = \begin{cases} (-2 \cdot n) + 1 & \text{when } n \text{ is even} \\ 2 \cdot n & \text{when } n \text{ is odd} \end{cases}$	$q : \mathbb{N} \rightarrow \mathbb{Z}$ $q(n) = \begin{cases} -1 \cdot ((n+1) \text{ div } 2) & \text{when } n \text{ is odd} \\ n \text{ div } 2 & \text{when } n \text{ is even} \end{cases}$

(a) What is the result of $f(-3)$?

(b) What is the result of $q(f(-4))$?

Notice we are looking at function composition here: first apply f and then apply q to the result.

(c) What is the result of $f(h(4))$?

Notice we are looking at function composition here: first apply h and then apply f to the result.

(d) What is the result of $g(-4)$?

(e) What is the result of $g(4)$?

(f) Consider the following statements, and indicate if they are true for each of f , g , h , and q .

- i. This function is one-to-one.
- ii. This function is onto.
- iii. This function is a bijection.
- iv. This function could serve as a witness for $|\mathbb{Z}| \leq |\mathbb{N}|$.
- v. This function could serve as a witness for $|\mathbb{Z}| \geq |\mathbb{N}|$.
- vi. This function could serve as a witness for $|\mathbb{N}| \leq |\mathbb{Z}|$.
- vii. This function could serve as a witness for $|\mathbb{N}| \geq |\mathbb{Z}|$.

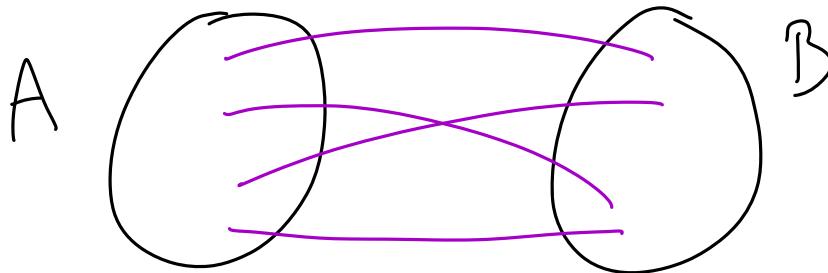
Wednesday November 17

Properties of cardinality

nice behavior

$$\left\{ \begin{array}{l} \forall A (|A| = |A|) \text{ every set has same size as itself} \\ \forall A \forall B (|A| = |B| \rightarrow |B| = |A|) \\ \forall A \forall B \forall C ((|A| = |B| \wedge |B| = |C|) \rightarrow |A| = |C|) \end{array} \right.$$

Extra practice with proofs: Use the definitions of bijections to prove these properties.



Cantor-Schroder-Bernstein Theorem: For all nonempty sets,

$$|A| = |B| \quad \text{if and only if} \quad (|A| \leq |B| \text{ and } |B| \leq |A|) \quad \text{if and only if} \quad (|A| \geq |B| \text{ and } |B| \geq |A|)$$

get 1-1
function
 $A \rightarrow B$ get 1-1
function
 $B \rightarrow A$
 To prove $|A| = |B|$, we can do any one of the following

get onto
function
 $A \rightarrow B$ get onto
function
 $B \rightarrow A$

- Prove there exists a bijection $f : A \rightarrow B$; *(definition)*
- Prove there exists a bijection $f : B \rightarrow A$; *(symmetry)*
- Prove there exist two functions $f_1 : A \rightarrow B$, $f_2 : B \rightarrow A$ where each of f_1, f_2 is one-to-one.
- Prove there exist two functions $f_1 : A \rightarrow B$, $f_2 : B \rightarrow A$ where each of f_1, f_2 is onto.

Last time: saw examples of finite sets of same size and of different sizes.

To day: infinite sets

$$\mathbb{Z} \quad \mathbb{N} \quad \mathbb{Z}^+ \quad \mathbb{Q}$$

Definition: A set A is **countably infinite** means it is the same size as \mathbb{N} .

Natural numbers \mathbb{N}

List: 0 1 2 3 4 5 6 7 8 9 10...

identity : $\mathbb{N} \rightarrow \mathbb{N}$ with $identity(n) = n$

Claim: *identity* is a bijection. *Proof:* Ex.

Corollary: $|\mathbb{N}| = |\mathbb{N}|$

Positive integers \mathbb{Z}^+

List: 1 2 3 4 5 6 7 8 9 10 11...

positives : $\mathbb{N} \rightarrow \mathbb{Z}^+$ with $positives(n) = n + 1$

Claim: *positives* is a bijection. *Proof:* Ex.

Corollary: $|\mathbb{N}| = |\mathbb{Z}^+|$

Negative integers \mathbb{Z}^-

List: -1 -2 -3 -4 -5 -6 -7 -8 -9 -10 -11...

negatives : $\mathbb{N} \rightarrow \mathbb{Z}^-$ with $negatives(n) = \begin{cases} n & \text{if } n \leq 0 \\ -n-1 & \text{if } n > 0 \end{cases}$

Claim: *negatives* is a bijection.

Corollary: $|\mathbb{N}| = |\mathbb{Z}^-|$

Proof: We need to show it is a well-defined function that is one-to-one and onto.

- Well-defined?

Consider an arbitrary element of the domain, $n \in \mathbb{N}$. We need to show it maps to exactly one element of \mathbb{Z}^- . $negatives(n) = -n-1$ is an integer

moreover $negatives(n) = -n-1$ because $n > 0$

i.e. $negatives(n)$ is an integer less than or equal to -1, so in \mathbb{Z}^- .

- One-to-one? distinct inputs give distinct outputs.

Consider arbitrary elements of the domain $a, b \in \mathbb{N}$. We need to show that

$$(negatives(a) = negatives(b)) \rightarrow (a = b)$$

Assume $negatives(a) = negatives(b)$. WTS $a = b$.

Use definition: $negatives(a) = -a-1$ $negatives(b) = -b-1$.

We have $-a-1 = -b-1$. Add 1: $-a = -b$. Multiply by -1: $a = b$ \blacksquare

- Onto? all codomain elements are "hit" by function

Consider arbitrary element of the codomain $b \in \mathbb{Z}^-$. We need witness in \mathbb{N} that maps to b .

Define $a = -b-1$ • in \mathbb{N} ? Yes b/c $b \leq -1 \Rightarrow -b \geq 1 \Rightarrow -b-1 \geq 0$

$$\begin{aligned} \bullet \quad & negatives(a) = negatives(-b-1) \\ & -(-b-1)-1 = b+1-1 = b \quad \square \end{aligned}$$

Integers \mathbb{Z}

List: 0 -1 1 -2 2 -3 3 -4 4 -5 5...

$f : \mathbb{Z} \rightarrow \mathbb{N}$ with $f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x-1 & \text{if } x < 0 \end{cases}$

given integer function f computes its index in the list

$$\begin{aligned} \text{Notice } f(-1) &= -2(-1)-1 \\ &= 2-1=1 \end{aligned}$$

Claim: f is a bijection. *Proof:* Ex.

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

More examples of countably infinite sets

Claim: S is countably infinite

RNA strands

Basis Step

AES CES

GES UES

Rec Step: If $s \in S$ be B then $s \in S$.

Similarly: The set of all strings over a specific alphabet is countably infinite.

Bijection using alphabetical-ish ordering (first order by length, then alphabetically among strings of same length) of strands

Define function $\text{index}: S \rightarrow \mathbb{N}$

given by $\text{index}(s) = \text{Index of } s \text{ in this alphabetical-ish list of strands.}$

Claim: L is countably infinite

$[] (0, C) (1, []) (2, []) (3, [])$

$(0, (0, C)) (0, (1, []))$

$\text{toNum}: L \rightarrow \mathbb{N}$

$\text{toNum}([]) = 0$

$\text{toNum}((n, l)) = 2^n 3^{\text{toNum}(l)}$ for $n \in \mathbb{N}, l \in L$

Witnesses: $|L| \leq |\mathbb{N}|$

witnesses $|L| \leq |\mathbb{N}|$

Claim: $|\mathbb{Z}^+| = |\mathbb{Q}|$

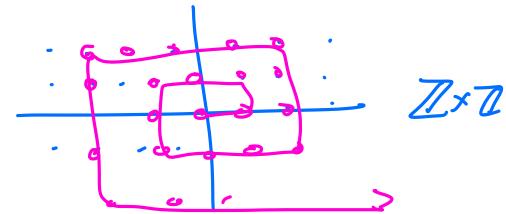
$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$$

One-to-one function from \mathbb{Z}^+ to \mathbb{Q} is $f_1: \mathbb{Z} \rightarrow \mathbb{Q}$ with $f_1(n) = n$ for all $n \in \mathbb{N}$.

\mathbb{R}

$f_2: \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}$

$$f_2(x) = \begin{cases} (0, 1) & \text{if } x = 0 \\ (p, q) & \text{if } x = \frac{p}{q}, \\ & \gcd(p, q) = 1, q > 0 \end{cases}$$



$f_3: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+$

$$f_3((x, y)) = \begin{cases} (2x + 2, 2y + 2) & \text{if } x \geq 0, y \geq 0 \\ (-2x - 1, 2y + 2) & \text{if } x < 0, y \geq 0 \\ (2x + 2, -2y + 1) & \text{if } x \geq 0, y < 0 \\ (-2x - 1, -2y - 1) & \text{if } x < 0, y < 0 \end{cases}$$

$f_4: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$

$$f_4((x, y)) = 2^x 3^y \quad \text{for } x, y \in \mathbb{Z}^+$$

\mathbb{N}	0	1	2	3	4	5	6	--
\mathbb{Z}^+	1	2	3	4	5	6	7	--
\mathbb{Z}^-	-1	-2	-3	-4	-5	-6	-7	--
\mathbb{Z}	0	-1	1	-2	2	-3	3	--
S	A	C	G	U	AA	AC	AG	--
L	$[]$	$(0, [])$	$(1, [])$	$(0, (0, []))$	$(2, [])$	$(0, (0, (0, [])))$	$(NOT$ $USED$)	$(1, (0, (0, [])))$

Note: $toNum: L \rightarrow \mathbb{N}$ being one-to-one means we have a list where all linked lists show up exactly once, but some slots (indices) are not used.

$$toNum([]) = 0$$

$$toNum((0, [])) = 2^0 3^{toNum([])}$$

$$toNum((1, [])) = 2^1 3^{toNum([])}$$

$$toNum((2, [])) = 2^2 3^{toNum([])}$$

$$toNum((0, (0, []))) = 2^0 3^{toNum((0, []))}$$

$$toNum((1, (0, []))) = 2^1 3^{toNum((0, []))}$$

Review

1. Consider the function $f : \mathbb{N} \rightarrow \mathbb{Z}$ given by $f(n) = \begin{cases} n \text{ div } 4 & \text{if } n \text{ is even} \\ -((n+1) \text{ div } 4) & \text{if } n \text{ is odd} \end{cases}$

Select all and only the true statements below.

- (a) f is one-to-one
- (b) f is onto
- (c) f is a bijection
- (d) f witnesses that $|\mathbb{N}| \leq |\mathbb{Z}|$
- (e) f witnesses that $|\mathbb{N}| \geq |\mathbb{Z}|$
- (f) f witnesses that $|\mathbb{N}| = |\mathbb{Z}|$
- (g) There is a one-to-one function with domain \mathbb{N} and codomain \mathbb{Z}
- (h) There is an onto function with domain \mathbb{N} and codomain \mathbb{Z}
- (i) There is a bijection with domain \mathbb{N} and codomain \mathbb{Z}
- (j) $|\mathbb{N}| \leq |\mathbb{Z}|$
- (k) $|\mathbb{N}| \geq |\mathbb{Z}|$
- (l) $|\mathbb{N}| = |\mathbb{Z}|$

2.

Goals for this question: Reason through multiple nested quantifiers. Fluently use the definition and properties of the set of rationals.

Recall the definition of the set of rational numbers, $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$. We define the set of **irrational** numbers $\overline{\mathbb{Q}} = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.

- (i) $\forall x \in \mathbb{Q} \forall y \in \mathbb{Q} \exists z \in \mathbb{Q} (x + y = z)$
 - (ii) $\forall x \in \mathbb{Q} \forall y \in \mathbb{Q} \exists z \in \mathbb{Q} (x + z = y)$
 - (iii) $\forall x \in \mathbb{Q} \forall y \in \mathbb{Q} \exists z \in \mathbb{Q} (x \cdot y = z)$
 - (iv) $\forall x \in \mathbb{Q} \forall y \in \mathbb{Q} \exists z \in \mathbb{Q} (x \cdot z = y)$
 - (v) $\forall x \in \overline{\mathbb{Q}} \forall y \in \overline{\mathbb{Q}} \exists z \in \overline{\mathbb{Q}} (x + y = z)$
 - (vi) $\forall x \in \overline{\mathbb{Q}} \forall y \in \overline{\mathbb{Q}} \exists z \in \overline{\mathbb{Q}} (x + z = y)$
 - (vii) $\forall x \in \overline{\mathbb{Q}} \forall y \in \overline{\mathbb{Q}} \exists z \in \overline{\mathbb{Q}} (x \cdot y = z)$
 - (viii) $\forall x \in \overline{\mathbb{Q}} \forall y \in \overline{\mathbb{Q}} \exists z \in \overline{\mathbb{Q}} (x \cdot z = y)$
- (a) Which of the statements above (if any) could be **disproved** using the counterexample $x = \frac{1}{2}$, $y = \frac{3}{4}$?
- (b) Which of the statements above (if any) could be **disproved** using the counterexample $x = \sqrt{4}$, $y = \sqrt{3}$?
- (c) Which of the statements above (if any) could be **disproved** using the counterexample $x = 0$, $y = 3$?
- (d) Which of the statements above (if any) could be **disproved** using the counterexample $x = \sqrt{2}$, $y = 0$?
- (e) Which of the statements above (if any) could be **disproved** using the counterexample $x = \sqrt{2}$, $y = -\sqrt{2}$?

Hint: we proved in class that $\sqrt{2} \notin \mathbb{Q}$. You may also use the facts that $\sqrt{3} \notin \mathbb{Q}$ and $-\sqrt{2} \notin \mathbb{Q}$.

Bonus - not to hand in: prove these facts; that is, prove that $\sqrt{3} \notin \mathbb{Q}$ and $-\sqrt{2} \notin \mathbb{Q}$.

Friday November 19

Cardinality categories

A set A is **finite** means it is empty or it is the same size as $\{1, \dots, n\}$ for some $n \in \mathbb{N}$.

A set A is **countably infinite** means it is the same size as \mathbb{N} . Notice: all countably infinite sets are the same size as each other.

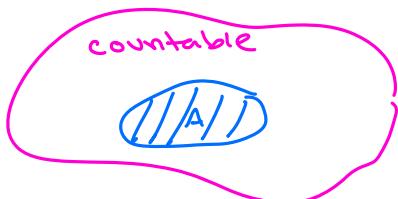
$$\mathbb{Z}^+ \quad \mathbb{Z}^- \quad \mathbb{Z} \quad L \quad S \quad \mathbb{Q}$$

A set A is **countable** means it is either finite or countably infinite.

A set A is **uncountable** means it is not countable. *not finite and not same size as \mathbb{N}*

Lemmas about countable and uncountable sets
"smallish" "large"

Lemma: If A is a subset of a countable set, then it's countable.

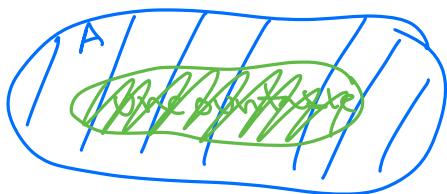


Idea: subset's size is upper bounded by size of superset

Idea: countably infinite sets are "smallest" among infinite sets.

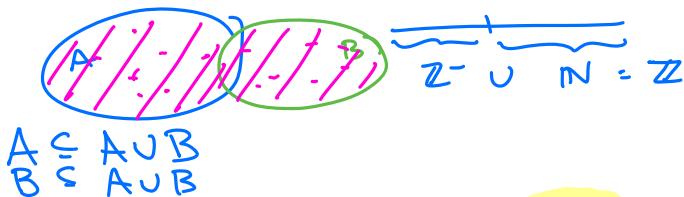
Lemma: If A is a superset of an uncountable set, then it's uncountable.

similar ideas to prove.



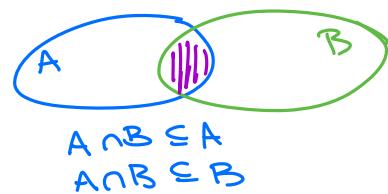
Lemma: If A and B are countable sets, then $A \cup B$ is countable and $A \cap B$ is countable.

Use same ideas $|\mathbb{Z}| = |\mathbb{N}|$



$$A \subseteq A \cup B$$

$$B \subseteq A \cup B$$



$$A \cap B \subseteq A$$

$$A \cap B \subseteq B$$

Lemma: If A and B are countable sets, then $A \times B$ is countable.

Generalize pairing ideas from $\mathbb{Z}^+ \times \mathbb{Z}^+$ to \mathbb{Z}^+

Lemma: If A is a subset of B , to show that $|A| = |B|$, it's enough to give one-to-one function from B to A or an onto function from A to B . *(assume A, B nonempty)*

PF Let A, B be arbitrary nonempty sets. Assume $A \subseteq B$. Consider the function $\text{id}: A \rightarrow B$ given by $\text{id}(x) = x$ for all $x \in A$. This is a well-defined (b/c $A \subseteq B$) one-to-one function so witnesses $|A| \leq |B|$. By Cantor-Schroeder-Bernstein, it'll be enough to prove $|B| \leq |A|$ or $|A| \geq |B|$ to conclude $|A| = |B|$

Are there always *bigger* sets?

Recall: When U is a set, $\mathcal{P}(U) = \{X \mid X \subseteq U\}$

Key idea: For finite sets, the power set of a set has strictly greater size than the set itself. Does this extend to infinite sets?

Definition: For two sets A, B , we use the notation $|A| < |B|$ to denote $(|A| \leq |B|) \wedge \neg(|A| = |B|)$.

0	$\emptyset = \{\}$	$\mathcal{P}(\emptyset) = \{\emptyset\}$	1	$ \emptyset < \mathcal{P}(\emptyset) $
1	$\{1\}$	$\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$	2	$ \{1\} < \mathcal{P}(\{1\}) $
2	$\{1, 2\}$	$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$	4	$ \{1, 2\} < \mathcal{P}(\{1, 2\}) $

n element set gives 2^n element power set.

\mathbb{N} and its power set

Example elements of \mathbb{N}

0 1 7

Example elements of $\mathcal{P}(\mathbb{N})$

$\emptyset \quad \{0\} \quad \{3, 100, 20\} \quad \{2^n \mid n \in \mathbb{N}\}$

Claim: $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$

How to prove? Use definition of size comparison in terms of functions with special properties.

Need witness function $f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$

that is one-to-one.

There are lots of functions that could be used, for definiteness let's consider

$f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ where

~~$f(n) = \{2x \mid x \in \mathbb{N}\}$~~

~~constant function~~
~~not one-to-one~~

$f(n) = \{2^n\}$

e.g. $f(0) = \{0\}$, $f(1) = \{2\}$, $f(2) = \{4\}$, . . .

Show: f is one-to-one

ED

To prove f is one-to-one we need

$$\forall a \in \mathbb{N} \forall b \in \mathbb{N} (f(a) = f(b) \rightarrow a = b)$$

Towards universal generalization, let a, b be arbitrary natural numbers. Assume, towards direct proof, that $f(a) = f(b)$. WTS $a = b$.

By definition of f $f(a) = \{2a\}$, $f(b) = \{2b\}$

Thus, our assumption is that

$$\{2a\} = \{2b\}$$

By definition of set equality, this means $2a = 2b$.

Dividing both sides by 2 maintains the equality (properties of real numbers) so

$a = b$ as required \square

We want $|N| < |\mathcal{P}(N)|$ we have $|N| \leq |\mathcal{P}(N)|$
and we need $|N| \neq |\mathcal{P}(N)|$.

Claim: There is an uncountable set. Example: $\mathcal{P}(N)$

Proof: By definition of countable, since $\mathcal{P}(N)$ is not finite, to show is $|N| \neq |\mathcal{P}(N)|$.

Rewriting using the definition of cardinality, to show is no witness function for this same size, i.e. $\nexists f: N \rightarrow \mathcal{P}(N)$ (f is bijection)

DeMorgan's: $\neg \exists f: N \rightarrow \mathcal{P}(N)$ (f is not bijection)

Towards a proof by universal generalization, consider an arbitrary function $f: N \rightarrow \mathcal{P}(N)$.

To show: f is not a bijection. It's enough to show that f is not onto. i.e. to show there are some sets of natural numbers that are not $f(n)$ for any n .
Rewriting using the definition of onto, to show:

$$\neg \forall B \in \mathcal{P}(N) \exists a \in N (f(a) = B)$$

every set of nums

image under f of a

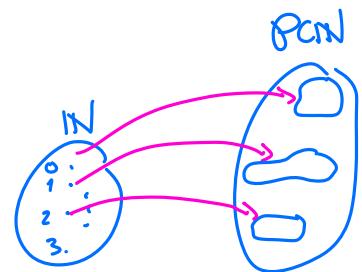
. By logical equivalence, we can write this as an existential statement:

$$\exists B \in \mathcal{P}(N) \forall a \in N (f(a) \neq B)$$

In search of a witness, define the following collection of nonnegative integers:

$D_f = \{n \in N \mid n \notin f(n)\}$

depends on f



. By definition of power set, since all elements of D_f are in N , $D_f \in \mathcal{P}(N)$. It's enough to prove the following Lemma:

Lemma: $\forall a \in N (f(a) \neq D_f)$. in other word D_f is our witness that f is not onto.

Proof of lemma: Consider arbitrary $a \in N$. Have two cases:
notice $a \in f(a) \vee a \notin f(a)$.

Case ① assume $a \in f(a)$. So by def of D_f , $a \notin D_f$ So a witness $f(a) \neq D_f$.

Case ② assume $a \notin f(a)$. So by def of D_f , $a \in D_f$ So a witness $f(a) \neq D_f$.

By the Lemma, we have proved that f is not onto, and since f was arbitrary, there are no onto functions from N to $\mathcal{P}(N)$. QED

Where does D_f come from? The idea is to build a set that would disagree with each of the images of f about some element.

Diagonal.

D

$n \in N$	$f(n) = X_n$	Is $0 \in X_n$?	Is $1 \in X_n$?	Is $2 \in X_n$?	Is $3 \in X_n$?	Is $4 \in X_n$?	...	Is $n \in D_f$?
0	$f(0) = X_0$	Y / N	Y / N	Y / N	Y / N	Y / N	...	N / Y
1	$f(1) = X_1$	Y / N	Y / N	Y / N	Y / N	Y / N	...	N / Y
2	$f(2) = X_2$	Y / N	Y / N	Y / N	Y / N	Y / N	...	N / Y
3	$f(3) = X_3$	Y / N	Y / N	Y / N	Y / N	Y / N	...	N / Y
4	$f(4) = X_4$	Y / N	Y / N	Y / N	Y / N	Y / N	...	N / Y
:								

Notice: depending on f , D_f could be the empty set or could be N or could be something in between.

Countable vs. uncountable: sets of numbers

Comparing \mathbb{Q} and \mathbb{R}

Both \mathbb{Q} and \mathbb{R} have no greatest element.

Both \mathbb{Q} and \mathbb{R} have no least element.

The quantified statement

$$\forall x \forall y (x < y \rightarrow \exists z (x < z < y))$$

is true about both \mathbb{Q} and \mathbb{R} .

Both \mathbb{Q} and \mathbb{R} are infinite. But, \mathbb{Q} is countably infinite whereas \mathbb{R} is uncountable.

The set of real numbers

$$\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

Order axioms (Rosen Appendix 1):

Reflexivity	$\forall a \in \mathbb{R} (a \leq a)$
Antisymmetry	$\forall a \in \mathbb{R} \forall b \in \mathbb{R} ((a \leq b \wedge b \leq a) \rightarrow (a = b))$
Transitivity	$\forall a \in \mathbb{R} \forall b \in \mathbb{R} \forall c \in \mathbb{R} ((a \leq b \wedge b \leq c) \rightarrow (a \leq c))$
Trichotomy	$\forall a \in \mathbb{R} \forall b \in \mathbb{R} ((a = b) \vee b > a \vee a < b)$

Completeness axioms (Rosen Appendix 1):

Least upper bound	Every nonempty set of real numbers that is bounded above has a least upper bound
Nested intervals	For each sequence of intervals $[a_n, b_n]$ where, for each n , $a_n < a_{n+1} < b_{n+1} < b_n$, there is at least one real number x such that, for all n , $a_n \leq x \leq b_n$.

Each real number $r \in \mathbb{R}$ is described by a function to give better and better approximations

$$x_r : \mathbb{Z}^+ \rightarrow \{0, 1\} \quad \text{where } x_r(n) = n^{\text{th}} \text{ bit in binary expansion of } r$$

r	Binary expansion	x_r
0.1	0.00011001...	$x_{0.1}(n) = \begin{cases} 0 & \text{if } n > 1 \text{ and } (n \bmod 4) = 2 \\ 0 & \text{if } n = 1 \text{ or if } n > 1 \text{ and } (n \bmod 4) = 3 \\ 1 & \text{if } n > 1 \text{ and } (n \bmod 4) = 0 \\ 1 & \text{if } n > 1 \text{ and } (n \bmod 4) = 1 \end{cases}$
$\sqrt{2} - 1 = 0.4142135\dots$	0.01101010...	Use linear approximations (tangent lines from calculus) to get algorithm for bounding error of successive operations. Define $x_{\sqrt{2}-1}(n)$ to be n^{th} bit in approximation that has error less than $2^{-(n+1)}$.

Claim: $\{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}$ is uncountable.

Approach 1: Mimic proof that $\mathcal{P}(\mathbb{Z}^+)$ is uncountable.

Proof: By definition of countable, since $\{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}$ is not finite, **to show** is $|\mathbb{N}| \neq |\{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}|$.

To show is $\forall f : \mathbb{Z}^+ \rightarrow \{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}$ (f is not a bijection). Towards a proof by universal generalization, consider an arbitrary function $f : \mathbb{Z}^+ \rightarrow \{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}$. **To show:** f is not a bijection. It's enough to show that f is not onto. Rewriting using the definition of onto, **to show**:

$$\exists x \in \{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\} \forall a \in \mathbb{N} (f(a) \neq x)$$

In search of a witness, define the following real number by defining its binary expansion

$$d_f = 0.b_1 b_2 b_3 \dots$$

where $b_i = 1 - b_{ii}$ where b_{jk} is the coefficient of 2^{-k} in the binary expansion of $f(j)$. Since¹ $d_f \neq f(a)$ for any positive integer a , f is not onto.

Approach 2: Nested closed interval property

To show $f : \mathbb{N} \rightarrow \{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}$ is not onto. **Strategy:** Build a sequence of nested closed intervals that each avoid some $f(n)$. Then the real number that is in all of the intervals can't be $f(n)$ for any n . Hence, f is not onto.

Consider the function $f : \mathbb{N} \rightarrow \{r \in \mathbb{R} \mid 0 \leq r \wedge r \leq 1\}$ with $f(n) = \frac{1+\sin(n)}{2}$

n	$f(n)$	Interval that avoids $f(n)$
0	0.5	
1	0.920735...	
2	0.954649...	
3	0.570560...	
4	0.121599...	
\vdots		

Other examples of uncountable sets

- The power set of any countably infinite set is uncountable. For example:

$$\mathcal{P}(\mathbb{N}), \mathcal{P}(\mathbb{Z}^+), \mathcal{P}(\mathbb{Z})$$

are each uncountable.

- The closed interval $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$, any other nonempty closed interval of real numbers whose endpoints are unequal, as well as the related intervals that exclude one or both of the endpoints.
- The set of all real numbers \mathbb{R} is uncountable and the set of irrational real numbers $\overline{\mathbb{Q}}$ is uncountable.

¹There's a subtle imprecision in this part of the proof as presented, but it can be fixed.

Review

1.

The diagonalization argument constructs, for each function $f : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$, a set D_f defined as

$$D_f = \{x \in \mathbb{N} \mid x \notin f(x)\}$$

which has the property that, for all $n \in \mathbb{N}$, $f(n) \neq D_f$. Consider the following two functions with domain \mathbb{N} and codomain $\mathcal{P}(\mathbb{N})$

$$f_1(x) = \{y \in \mathbb{N} \mid y \bmod 3 = x \bmod 3\}$$

$$f_2(x) = \{y \in \mathbb{N} \mid (y > 0) \wedge (x \bmod y \neq 0)\}$$

Select all and only the true statements below.

- (a) $0 \in D_{f_1}$
- (b) D_{f_1} is infinite
- (c) D_{f_1} is uncountable
- (d) $1 \in D_{f_2}$
- (e) D_{f_2} is empty
- (f) D_{f_2} is countably infinite

2.

Recall the definitions from previous assignments and class: The bases of RNA are elements of the set $B = \{A, C, G, U\}$. The set of RNA strands S is defined (recursively) by:

Basis Step: $A \in S, C \in S, U \in S, G \in S$
Recursive Step: If $s \in S$ and $b \in B$, then $sb \in S$

For b an integer greater than 1 and n a positive integer, the **base b expansion of n** is

$$(a_{k-1} \cdots a_1 a_0)_b$$

where k is a positive integer, a_0, a_1, \dots, a_{k-1} are nonnegative integers less than b , $a_{k-1} \neq 0$, and

$$n = a_{k-1}b^{k-1} + \cdots + a_1b + a_0$$

For b an integer greater than 1, w a positive integer, and n a nonnegative integer with $n < b^w$, the **base b fixed-width w expansion of n** is

$$(a_{w-1} \cdots a_1 a_0)_{b,w}$$

where a_0, a_1, \dots, a_{w-1} are nonnegative integers less than b and

$$n = a_{w-1}b^{w-1} + \cdots + a_1b + a_0$$

For b an integer greater than 1, w a positive integer, w' a positive integer, and x a real number the **base b fixed-width expansion of x with integer part width w and fractional part width w'** is

$$(a_{w-1} \cdots a_1 a_0 . c_1 \cdots c_{w'})_{b,w,w'}$$

where $a_0, a_1, \dots, a_{w-1}, c_1, \dots, c_{w'}$ are nonnegative integers less than b and

$$x \geq a_{w-1}b^{w-1} + \cdots + a_1b + a_0 + c_1b^{-1} + \cdots + c_{w'}b^{-w'}$$

and

$$x < a_{w-1}b^{w-1} + \cdots + a_1b + a_0 + c_1b^{-1} + \cdots + (c_{w'} + 1)b^{-w'}$$

For each set below, determine if it is empty, nonempty and finite, countably infinite, or uncountable.

Challenge - not to hand in: how would you prove this?

- (a) B
- (b) S
- (c) $\{x \in \mathbb{N} \mid x = (4102)_3\}$
- (d) $\{x \in \mathbb{R} \mid x \text{ has a binary fixed-width 5 expansion}\}$
- (e) $\{x \in \mathbb{R} \mid x = (0.10)_{(2,1,2)}\}$