Administrivia

Mid-Term Exam: Thursday, March 9

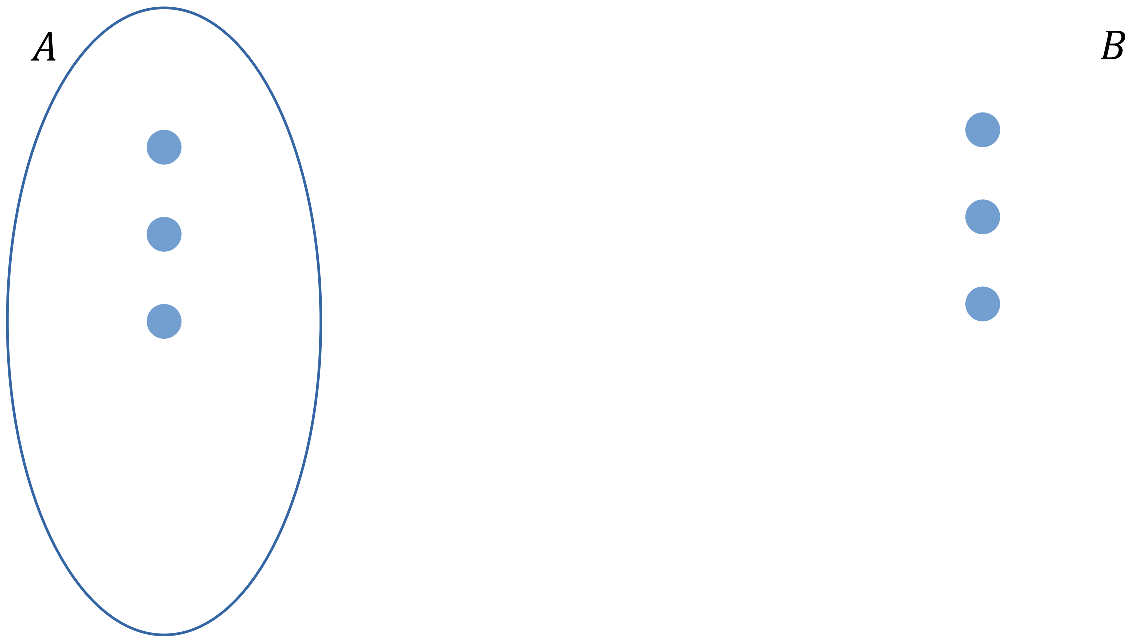
- In class
- One 8-1/2 x 11” cheat sheet allowed
    - write/type/draw on both sides
- No electronic devices
- Topics: Logic, Sets, Relations, Functions, Proof Techniques, Induction

Which is bigger?

1. {1, 2, 3} or {Alice, Bob, Charlie}
2. {10, 20, 25} or {234, 567}
3. {10, 20, 25} or {10, 20, 250}
4. {0, 1, 2, …} or {1, 2, 3, …}
5. {0, 2, 3, …} or {1, 2, 3, …}

What does it even mean for two sets to be equal in size?

Sets of equal cardinality



Associate ***every*** member of A with a ***unique*** member of B.
If every member of B is associated with a unique member of A then $|A| = |B|$.

Definition: $|A| = |B|$ if and only if there is a bijection from A to B.

This is the definition of equality of set sizes, even for infinite sets!

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

Sets A and B have the same cardinality (denoted |A|=|B|) if

$\exists f: A \to B$ and f is bijective (one-to-one correspondence).

$f(x)$	$\mathbb{Z}$	-4	-3	-2	-1	0	1	2	3	4
x	$\mathbb{N}$	7	5	3	1	0	2	4	6	8

Example: $f: \mathbb{N} \to \mathbb{Z}$ where $f(x) = \begin{cases} \frac{x}{2}, & if\ x\ is\ even \\ -\frac{x+1}{2}, & if\ x\ is\ odd \end{cases}$

f is bijective. Therefore, $|\mathbb{N}| = |\mathbb{Z}|$

Countable Sets

Definition: A set S is *countable* if there is an injective function $f: S \to \mathbb{N}$.

Easy facts:

- Every finite set is countable.
- Every subset of $\mathbb{N}$ is countable.

A set S is *countably infinite* if there is a bijective function $f: \mathbb{N} \to S$.

The intuition: we can enumerate the elements of S one-by-one

$$f(0), f(1), f(2), f(3), \cdots$$

Countably Infinite Sets

If we can list all the elements of an infinite set without repetition, then the set is countably infinite.

Examples of countable sets:

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

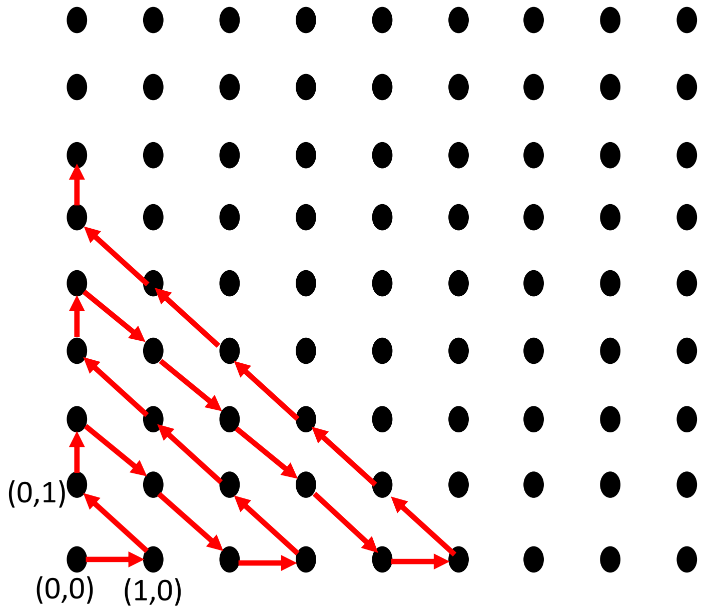
$$|\{0,2,4,6,\ldots\}| = |\{1,3,5,7,\ldots\}| = |\mathbb{N}|$$

$$|PRIMES| = |\mathbb{N}|$$

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

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

$\mathbb{N}\times\mathbb{N}$ is Countable



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

What is $f(n)$?

Find k: $\frac{k(k+1)}{2} \leq n \leq \frac{k(k+3)}{2}$

Let $d = n - k(k+1)/2$

Then $f(n) = \begin{cases} (k-d, d), & if\ k\ is\ odd \\ (d, k-d), & if\ k\ is\ even \end{cases}$

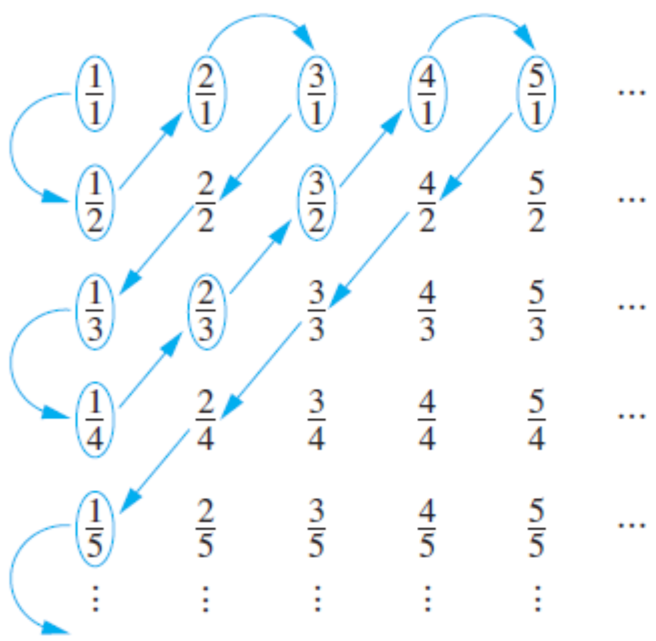
Theorem: If A, B are countable sets then $A\times B$ is countable

The Set $\mathbb{Q}$ of Rationals is Countable

Every rational number $\frac{a}{b}$ has multiple representations.

To establish a bijection $f: \mathbb{N} \rightarrow \mathbb{Q}$ we must count every rational number exactly once.

So, count the first representation, and skip the rest.



Is every set countable?

Can we list all the elements without repetition and not miss any element?

Power Sets

The power set $P(S)$ of a set S is defined as:

$$P(S) = \{X : X \subseteq S\}$$

"The set of all subsets of S"

$$P(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$$

$$P(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

If a finite set S has m elements, then $P(S)$ has $2^m > m$ elements.

What if S is infinite?

For example, is $P(\mathbb{N})$ countable?

Mapping Subsets of $\mathbb{N}$ to Binary Strings

We will associate a subset of the natural numbers $S \subseteq \mathbb{N}$ with an infinite length binary string.

$\{0\}$	$1000000000 \cdots\cdots\cdots$
$\{1\}$	$0100000000 \cdots\cdots\cdots$
$\{0,2\}$	$1010000000 \cdots\cdots\cdots$
$\{0,2,4,5\}$	$1010110000 \cdots\cdots\cdots$
Odd	$01010101010 \cdots\cdots\cdots$
Primes	$0011010100010 1\cdots\cdots\cdots$

Every infinite string of 0s and 1s corresponds to a unique subset of $\mathbb{N}$.

000110100111000000$\cdots\cdots\cdots$ {3,4,6,9,10,11, …}

In other words, there is a 1-1 correspondence (bijection)

$$\chi\colon \mathcal{P}(\mathbb{N}) \to \{\text{Infinite length 0-1 strings}\}$$

If $\mathcal{P}(\mathbb{N})$ is countable then so is the set {Infinite length 0-1 strings}

Cantor's Theorem

Theorem: $\mathcal{P}(\mathbb{N})$ is not countable.

Proof (by Contradiction): Suppose that $\mathcal{P}(\mathbb{N})$ is countable.

Then so is the set {Infinite length 0-1 strings}

Therefore, there is a bijection from the natural numbers to the set of infinite binary strings

Let $\mathcal{E}: \mathbb{N} \rightarrow$ {Infinite length 0-1 strings} be such a bijection.

We'll show that no listing of infinite length strings can include all of them!

This will imply that $\mathcal{E}$ is NOT bijective.
This contradicts our assumption; therefore, $\mathcal{P}(\mathbb{N})$ is not countable.

Cantor's Diagonalization Method

Consider any list of infinite length binary strings.

$\mathcal{E}(0)$	0	1	1	0	0	1	0	0	1	0	1	1	.	.	.
$\mathcal{E}(1)$	1	1	0	0	0	0	1	1	0	1	1	0	.	.	.
$\mathcal{E}(2)$	0	0	1	0	1	1	0	0	1	0	1	1	.	.	.
$\mathcal{E}(3)$	1	1	0	0	0	0	1	1	1	0	0	0	.	.	.
$\mathcal{E}(4)$	0	0	0	0	0	0	1	1	0	0	1	1	.	.	.
$\mathcal{E}(5)$	0	1	1	1	1	0	0	1	1	0	0	1	.	.	.
$\mathcal{E}(6)$	0	0	1	0	1	1	0	1	1	1	0	1	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.			
.	.	.	.	.	.	.	.	.							

Define $C = C_0 C_1 C_2 \ldots$
where $\forall i \geq 0$: $C_i = 1 - \mathcal{E}_i(i)$

Then $\forall i \geq 0$: $C \neq \mathcal{E}(i)$
C does not appear on the list!

Consider the string C that starts out 1001111
C is different from $\mathcal{E}(0), \mathcal{E}(1), \mathcal{E}(2), \ldots, \mathcal{E}(6)$

The Power Set Hierarchy

Theorem. For every set S, $|S| < |\mathrm{P}(S)|$ where $\mathrm{P}(S)$ is the power set of S.

Proof Outline:

Case 1. If S is finite and has m elements, then $\mathrm{P}(S)$ has $2^m > m$ elements.

Therefore, the proposition $|S| < |\mathrm{P}(S)|$ is true.

Case 2. If S is infinite then we will show that no function from S to $\mathrm{P}(S)$ is surjective (i.e., no bijection exists), and therefore the proposition is true.

Since there are no other cases to consider, the proposition is always true and therefore the theorem is valid.

(But we need to prove Case 2!)

Proof of Case 2.

Case 2. If S is infinite then we will show that no function from S to $P(S)$ is surjective (i.e., no bijection exists).

Proof: Let $f: S \to P(S)$ be surjective.

Define $C = \{x \in S: x \notin f(x)\}$

C is a well-defined subset of S, and therefore is an element of $P(S)$.

Let $a \in S$ be any element in S.

$a \in C \;\Rightarrow\; a \notin f(a)$ Therefore, $f(a) \neq C$

$a \notin C \;\Rightarrow\; a \in f(a)$ Therefore, $f(a) \neq C$

Since $\forall a \in S: f(a) \neq C$, it follows that f is not surjective!

Some uncountable sets

Consider the set $P(\mathbb{N})$, the power set of $\mathbb{N}$.

1. $P(\mathbb{N})$ is infinite.

2. By the theorem, there is no bijection from $\mathbb{N}$ to $P(\mathbb{N})$.

Therefore, $P(\mathbb{N})$ is not countable.

In other words, $|\mathbb{N}| < |P(\mathbb{N})|$

Also, by the theorem, there is no bijection from $P(\mathbb{N})$ to $P(P(\mathbb{N}))$

So $|P(\mathbb{N})| < |P\big(P(\mathbb{N})\big)|$

We can keep going!

The Infinite Hierarchy of Infinite Sets

$\boldsymbol{N}$	$\boldsymbol{P}(\boldsymbol{N})$	$\boldsymbol{P}(\boldsymbol{P}(\boldsymbol{N}))$	$\boldsymbol{P}(\boldsymbol{P}(\boldsymbol{P}(\boldsymbol{N})))$	…
$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_3$	…

$$|\boldsymbol{P}(\boldsymbol{N})| = |\mathrm{R}|$$

Cantor's Continuum Hypothesis

https://www.ias.edu/ideas/2011/kennedy-continuum-hypothesis