

~~The word~~ infinity used to just be a figure of speech or a useful abstraction, not a real thing.

late 19<sup>th</sup>, early 20<sup>th</sup> century, Georg Cantor ~~was~~ undertook a serious attempt to formalize and understand the infinite extending our idea of finite sets to infinite ones.

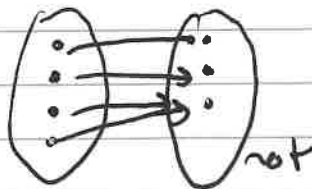
For ~~the~~ any set, we denote  $|S|$  as its cardinality. If  $S$  is finite then  $|S|$  is just the size. If  $A$  has less ~~than~~ elements than  $B$  we may write  $|A| < |B|$ .

What should  $|\mathbb{N}|$  be?  $\mathbb{N} = \{0, 1, 2, \dots\}$   
certainly  $\forall$  finite sets  $F, |F| < |\mathbb{N}|$  right?

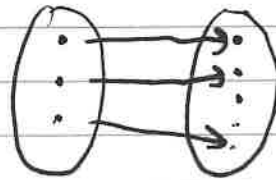
Defn: we say a set is "countable" if  $|S| \leq |\mathbb{N}|$ .  
we say a set is "countably infinite" if  $|S| = |\mathbb{N}|$ .

How can we show a set is the "same size" as  $\mathbb{N}$ .  $\rightarrow$

Recall  $f: A \rightarrow B$  is one-to-one (injective) if  $f(a) = f(b) \Rightarrow a = b$ .

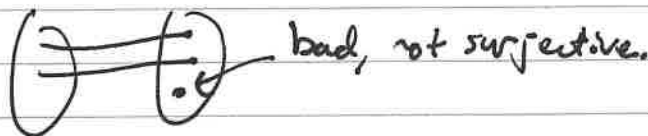


not



yes

$f: A \rightarrow B$  is onto (surjective) if  $\forall y, \exists x$  st  $f(x) = y$ .  
no unmapped elements in the co-domain goes unmapped



bad, not surjective.

We say a function is bijective if it's injective and surjective

bijections give us a natural "same-size-ness" because if there is a bijection between two sets, the elements seem to line up nicely.

Defn: we say a set  $S$  is countably infinite if  $\exists$  a bijection  $f: \mathbb{N} \rightarrow S$ . Recall bijections are in the inverse of a bijection is also a bijection so equivalently if  $\exists$  a bijection  $g: S \rightarrow \mathbb{N}$ .

Example:  $|\mathbb{N}| = |\mathbb{N}^{\geq 1}|$  these "other naturals" are countably infinite.

$$\mathbb{N} = \{0, 1, 2, \dots\} \quad \mathbb{N}^{\geq 1} = \{1, 2, 3, \dots\}$$

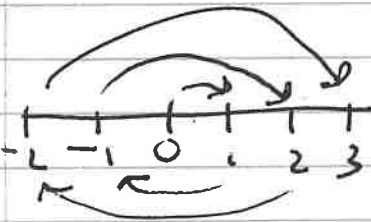
$f: \mathbb{N} \rightarrow \mathbb{N}^{\geq 1}$  by  $f(n) = n+1$ .  $0 \rightarrow 1, 1 \rightarrow 2$  etc.



Example:  $|\mathbb{N}| = |2\mathbb{N}|$ .  $2\mathbb{N} = \{0, 2, 4, \dots\}$   $f(n) = 2n$

Example:  $|\mathbb{N}| = |\mathbb{Z}|$   $\mathbb{Z} = \{-2, -1, 0, 1, 2, \dots\}$  intuitively we

can also find a bijection if we can list the elements in some order, (i.e. count them)



$$f(0) = 0, f(1) = 1$$

$$f(n) = -n/2 \text{ if } n \text{ is even}$$

$$f(n) = n+1/2 \text{ if } n \text{ is odd}$$

$$\mathbb{Z} \quad 0, 1, -1, 2, -2, 3, -3, 4, \dots$$

$$\mathbb{N} \quad 0, 1, 2, 3, 4, 5, 6, 7, \dots$$

What about the (positive) rationals?  $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{N}, b \neq 0 \}$ .

It would seem like there are infinitely more rationals than naturals.

$\exists$  infinite sequences of rationals with limits  $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots \rightarrow \frac{1}{\infty}$

which the integers doesn't have. Also between any two

rationals is only a finite amount of naturals.  $a, a+1, \dots, a+b$ .  
but between ~~any~~ any two rationals,  $\exists$  an infinite amount of naturals.

$$\frac{a}{b} \quad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \frac{c}{d}$$

The rationals are "dense" in this sense, between any two exist infinitely more.

The rationals are countably infinite. Put them into a table

$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$
$\frac{2}{1}$	$\frac{3}{2}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{2}{5}$
$\frac{3}{1}$	$\frac{4}{2}$	$\frac{3}{3}$	$\frac{4}{4}$	$\frac{3}{5}$
$\frac{4}{1}$	$\frac{5}{2}$	$\frac{4}{3}$	$\frac{5}{4}$	$\frac{4}{5}$
$\frac{5}{1}$	$\frac{6}{2}$	$\frac{5}{3}$	$\frac{6}{4}$	$\frac{5}{5}$

going line by line is a bad idea, each row is infinite, would never reach the second row

$\frac{1}{1} \rightarrow \frac{1}{2} \rightarrow \frac{1}{3} \rightarrow \dots$  bad.

The solution is then to compose anti-diagonals, ignoring repetition each number is guaranteed to be hit this way.

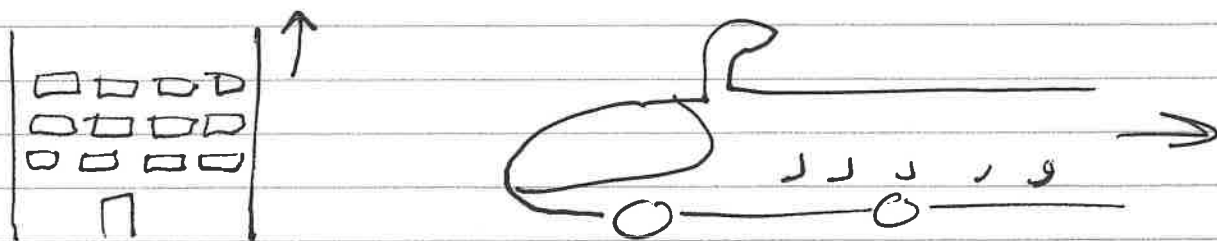
Another solution  $f(a/b) = 2^a 3^b$ . Then this is bijective to some set  $S = \{ 2^i 3^j \mid i, j \in \mathbb{N} \}$

notice that  $|\mathbb{Q}| = |S|$  and since  $S \subseteq \mathbb{N}$ , then  $|S| \leq |\mathbb{N}|$ . So by transitivity  $|\mathbb{Q}| = |S| \leq |\mathbb{N}| \Rightarrow$   
since  $|\mathbb{Q}|$  is infinite that

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

Similarly  $\mathbb{N} \times \mathbb{N}$  is countably infinite. Inductively,  
 so is  $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N} = \mathbb{N}^3$  and so on.  $\mathbb{N}^k$  is

Hilbert's Hotel:



Suppose we have an infinitely tall hotel of countably infinite rooms. A guest arrives, but instead of ~~any~~ ~~any~~ ~~any~~ them saying they make room for them tell everyone in the hotel to switch from room  $i$  to  $i+1$ . Now room zero is empty for our guest.

Suppose an infinitely long bus arrives with countably infinite # ~~guests~~ travelers. The full hotel can still accommodate them. Tell each guest to move from room  $i$  to  $2i$ , then the new guests all move into the odd numbered rooms.

But there exist even higher infinities: Cantor's Theorem:

$$|A| < |\mathcal{P}(A)|$$

obv true for infinite sets.

$$\mathcal{P}(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\} \text{ For finite sets } |A|=n, \mathcal{P}(A)=2^n$$

$\mathcal{P}A$  is countably infinite.

Proof by a new technique: Diagonalization

Suppose  $A = \mathcal{P}(N)$  & for each  $S \subseteq N$  associate ~~the~~ with it the infinite binary sequence "characteristic sequence"  $\chi_S$   
~~is the  $i$ th element  $\rightarrow$  as~~

$$\chi_S[i] = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{otherwise} \end{cases}$$

for example, if  $S \subseteq N$  &  $S = \{0, 3, 4\}$ ,  $\chi_S = 10011000000\dots$   
 if  $S \subseteq N$   $S = 2N = \{0, 2, 4, 6, \dots\}$  then  $\chi_S = 10101010\dots$

Assume to the contrary  $\mathcal{P}(A)$  is countable. Then there exists an ordering of its elements like  $S_0, S_1, S_2, \dots$  where every element is in this ordering. let  $\chi_0, \chi_1, \chi_2, \dots$  be defined according to this ordering. Define "the diagonal" line  ~~$D[i]$~~

$$D[i] = 1 - \chi_i[i]. \quad \text{The } i\text{th element of}$$

$D$  is the opposite of the  $i$ th element of  $\chi_i$

$D$  is an infinite binary sequence, so must be the characteristic

sequence of some set  $S_j$  in our ordering  $S_0, S_1, \dots$  so

$D$  is the  $j$ th sequence, so  $D = \chi_j$ . What is  $D[j]$ ?

well it must be  $D[j] = \chi_j[j]$ . But by the

way  $D$  was defined,  $D[j] = 1 - \chi_j[j] = \overline{\chi_j[j]}$

so  $\chi_j[j] = \overline{\chi_j[j]}$  a contradiction.

$x_0$	1	0	1	1	0	1	0	1
$x_1$	1	0	0	1	1	0	1	
$x_2$	1	1	1	1	1	0	1	1
$x_3$	0	0	0	1	0	1	1	1
$\vdots$								

$D =$  complement of diagonal

$D$  as defined is an infinite binary sequence. So it must exist in our ordering somewhere. But as defined, is different from every row in at least one place, so it can never be in our ordering.

$D = 0100$

$\mathcal{P}(\mathbb{N})$  is what we call uncountable. By a similar argument the real interval  $[0,1]$  is also uncountable, all real intervals, and  $\mathbb{R}$  itself are uncountable. ~~Since~~ you can make many "stretch" bijections.  $(0,1] \rightarrow [1,\infty)$  by  $f(x) = 1/x$ . and  $(0,1] \rightarrow [0,\infty)$  by  $1/x + 1$ .

$\mathcal{P}(\mathbb{N}), \mathbb{R}$  are uncountable, and so is  $\sum_{n=0}^{\infty}$  (not  $\sum_{n=1}^{\infty}$ !) = strings of infinite length. By diagonalization.

The "whole equals sum of its parts" is total of maintained.

$|\mathbb{N}| < |\mathbb{R}|$ . if  $|S| \leq |\mathbb{N}|$ , its finite or countably infinite. If  $S$  contains an uncountable subset  $A$ , since  $|A| \leq |S|$ , then  $S$  must also be uncountable. The union of two countable sets is countable.

Let  $A, B$  be countable. we show  $A \cup B$  is.  $\exists f, g$   $f: A \rightarrow \mathbb{N}, g: B \rightarrow \mathbb{N}$ .

$$h(x) = \begin{cases} 2f(x) & \text{if } x \in A \\ 2g(x)+1 & \text{if } x \in B \end{cases}$$

$h(x)$  is bijective, left as an exercise.

7.7 A countable union of countable sets is countable.

Most unions you have ever seen are countable. They index over  $\mathbb{N}$  with  $i=1, 2, \dots$ . But the index set of a union need not be countable in general. Consider

$\bigcup_{x \in \mathbb{R}} \{x\}$  here we index over  $\mathbb{R}$ , an uncountable set. Each element is a singleton containing just  $x$ ; it is finite, therefore countable. But our (uncountable) union over  ~~$\mathbb{R}$~~  (countable (finite) sets is  $\mathbb{R}$ , uncountable.

~~Let~~ Rough proof. Let  $A_i$  be countable and each  $S_i$  be countable.

$\left| \bigcup_{i \in A} S_i \right| \leq |A \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ . So a countable union of countable sets is countable.

lets do a problem. Let  $\mathbb{N}^* =$  finite, terminating sequences of integers. we show  $\mathbb{N}^*$  is countable using three proofs.

1) Students way

let  $A_i =$  sequences whose elements sum to  $i$ .  $A_3 = \{[1, 0, 1, 1], [3], [2, 1], \dots\}$   
Then since each <sup>sequence</sup> element of  $\mathbb{N}^*$  sums to something,

$\mathbb{N}^* = \bigcup_{i=0}^{\infty} A_i$  where each  $A_i$  is finite and disjoint. Therefore,  $\mathbb{N}^*$  is a countable union of countable sets, so must be countable.

2) Gödelian way. let  $f([x_1, x_2, \dots, x_k]) = 2^{x_1} 3^{x_2} 5^{x_3} \dots = \prod_{i=1}^k p_i^{x_i}$   
by the fundamental theorem of arithmetic, every number has a unique prime factorization. And since no two sequences can get the same number! so  $f$  is injective to  $\mathbb{N}$ . and  $|\mathbb{N}^*| \leq |\mathbb{N}|$  so its countable.

3) Diogenes way. somehow your brain can tell two sequences apart.  $[0, 1]$  and  $[1, 1, 3]$  so different.  $\rightarrow$

$f(a) = "a"$  str(a)

$f(S) = \{f(a) \mid a \in S\}$

$f(\mathbb{N}^*) \subseteq \sum^*$

~~countable~~ subsets of countable sets are countable

Why is  $\sum^*$  countable? countable union of countable sets.  $\sum^* = \bigcup_{i=0}^{\infty} \sum^i = \sum^0 \cup \sum^1 \cup \dots$

8.

How many Turing-recognizable languages are there? What is the cardinality of  $\mathcal{L}(TM)$ ? Each  $L \in \mathcal{L}(TM)$  is recognized by some TM uniquely. Each TM is finite in description and can be encoded (like finite) as a string. The set of Turing machines is countable, so not  $\mathcal{L}(TM)$ .

How many languages are there in total? Each language  $L \subseteq \Sigma^*$  so  $L \in \mathcal{P}(\Sigma^*)$ . By Cantor's theorem  $|\mathcal{P}(\Sigma^*)|$ , so there are uncountably many languages.

Since there are only countably many languages in  $\mathcal{L}(TM)$ , but an uncountably many in  $\mathcal{P}(\Sigma^*)$ . So  $\exists$  languages (many actually) which are not Turing-recognizable.

We have just ~~un~~constructively proved the existence of languages which ~~are~~ not Turing recognizable!

Typewriter principle: If the elements of a set  $S$  can be described uniquely with finite description, then  $S$  is countable.

Alternatively, if the elements of a set require infinite length description ( $\Sigma^\infty$  infinite strings,  $\mathbb{N}^\infty$  infinite sequences,  $\mathbb{R}$   $[0, 1]$  decimal expansions) then the set can be diagonalized out of and is uncountable.

Finitism, rejection of the infinite. Given  $0, S(x) = x+1$ , can generate  $0, 1, 2, 3, \dots$  w/ an infinite process. Very different than calling it  $\mathbb{N} = \{0, 1, 2, \dots\}$ .

Ultrafinitism. Rejection of even big numbers.  $2^{100}$  is not a number. All of this is just coping with death.