CS70: Countability and Uncountability

Alex Psomas

June 30, 2016

Warning!

Warning: I’m really loud!

Today.

One idea, from around 130 years ago.

At the heart of set theory.

Started a crisis in mathematics in the middle of the previous century!!!!!

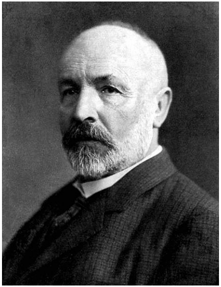
The man who worked on this was described as:

- Genious?
- Renegade?
- Corrupter of youth?
- The King in the North?

The idea.

The idea: **More than one infinities!!!!!!**

The man:



Georg Cantor

Life before Cantor

How many elements in $\{1, 2, 4\}$? 3

How many elements in $\{1, 2, 4, 10, 13, 18\}$? 6

How many primes? Infinite!

How many elements in $\mathbb{N}$? Infinite!

How many elements in $\mathbb{N} \setminus \{0\}$? Infinite!

How many elements in $\mathbb{Z}$? Infinite!

How many elements in $\mathbb{R}$? Infinite!

What is this infinity though?

The symbol you write after taking a limit....

Don't think about it....

Even Gauss: " ... first of all I must protest against the use of an infinite magnitude as a completed quantity, which is never allowed in mathematics. The Infinite is just a mannner of speaking, in which one is really talking in terms of limits, which certain ratios may approach as close as one wishes, while others may be allowed to increase without restriction. "

Cantor's questions

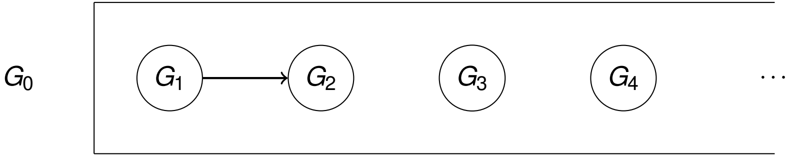
Is $\mathbb{N} \setminus \{0\}$ smaller than $\mathbb{N}$?

Is $\mathbb{N}$ smaller than $\mathbb{Z}$? What about $\mathbb{Z}^2$?

Is $\mathbb{N}$ smaller than $\mathbb{R}$?

Hilbert's hotel

A hotel with infinite rooms. Rooms are numbered from 1 to infinity. Every room is occupied. Room i has guest G_i.

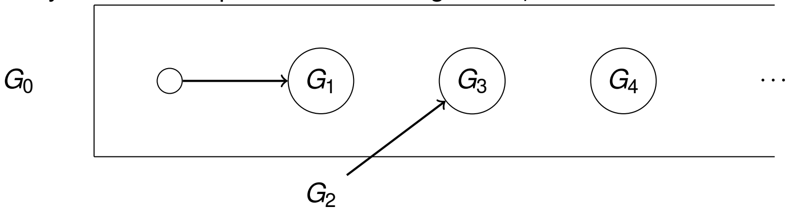


G_0 shows up. What do we do?

Move G_1 to room number 2.

Hilbert's hotel

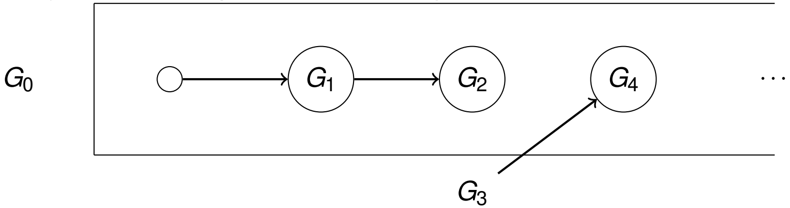
A hotel with infinite rooms. Rooms are numbered from 1 to infinity.
Every room is occupied. Room i has guest G_i.



Move G_2 to room number 3.

Hilbert's hotel

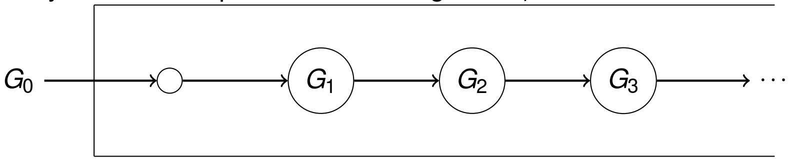
A hotel with infinite rooms. Rooms are numbered from 1 to infinity.
Every room is occupied. Room i has guest G_i.



Move G_3 to room number 4.

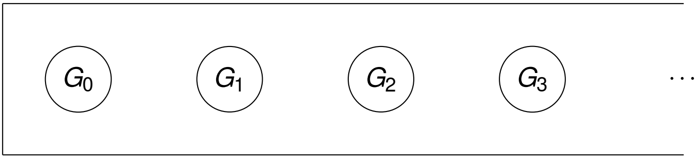
Hilbert's hotel

A hotel with infinite rooms. Rooms are numbered from 1 to infinity.
Every room is occupied. Room i has guest G_i.



And so on.

Now G_0 can go to room number 1!!



Moral of the story

$\mathbb{N} \setminus \{0\}$ is **not** smaller than $\mathbb{N}$.

$\mathbb{N} \setminus \{0\}$ is not bigger than $\mathbb{N}$. Why? Because it's a subset.

Therefore, $\mathbb{N} \setminus \{0\}$ must have the same number of elements as $\mathbb{N}$.

Is this a proof? How would we show this formally???

Countable.

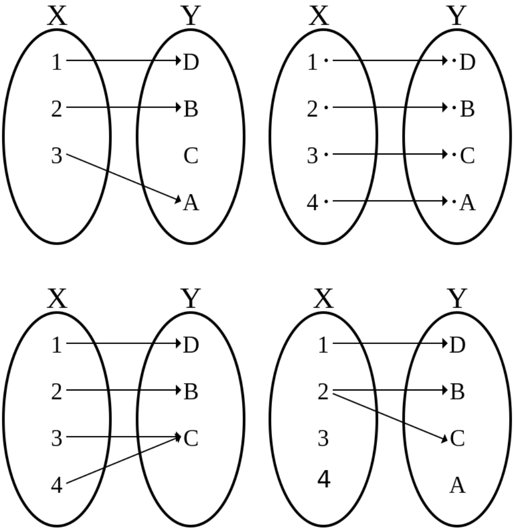
Definition: S is **countable** if there is a bijection between S and some subset of $\mathbb{N}$.

If the subset of $\mathbb{N}$ is finite, S has finite **cardinality**.

If the subset of $\mathbb{N}$ is infinite, S is **countably infinite**.

Bijection to or from natural numbers implies countably infinite.

Bijections

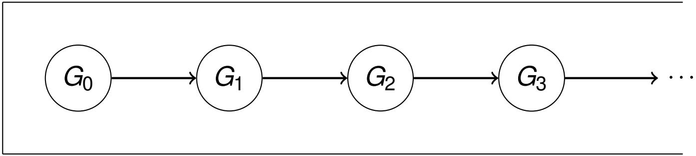


One to one. Bijection: one to one and onto. Onto. Not a function.

Countable.

- Enumerable means countable.
- Subsets of countable set are countable.
  For example the set $\{14, 54, 5332, 10^{12} + 4\}$ is countable. (It has 4 elements) Even numbers are countable. Prime numbers are countable. Multiples of 3 are countable.
- All countably infinite sets are the same cardinality as each other.

Back to Hilbert's hotel



Where's the function?

We want a bijection from: $\mathbb{N}$ to $\mathbb{N} \setminus \{0\}$.

$f(x) = x + 1$. Maps every number from $\mathbb{N}$ to a number in $\mathbb{N} \setminus \{0\}$, and every number in $x \in \mathbb{N} \setminus \{0\}$ has exactly one number $y \in \mathbb{N}$ such that $f(y) = x$.

What if we had a bijection from $\mathbb{N} \setminus \{0\}$ to $\mathbb{N}$?

Same thing! Bijection means that the sets have the same size. Invert it and you'll get a bijection from $\mathbb{N}$ to $\mathbb{N} \setminus \{0\}$.

Examples

Countably infinite (same cardinality as naturals)

- E even numbers.
  Where are the odds? Half as big?
  Enumerate: 0, 2, 4, ...
  Bijection: $f(e) = e/2$.
- Z- all integers.
  Twice as big?
  Enumerate: $0, 1, 2, 3, ...$
  When will we get to -1???
  New Enumeration: $0, -1, 1, -2, 2...$
  Bijection: $f(z) = 2|z| - sign(z)$.
  Where $sign(z) = 1$ if $z > 0$ and $sign(z) = 0$ otherwise.

Examples: Countable by enumeration

- $\mathbb{N} \times \mathbb{N}$ - Pairs of integers.
  Square of countably infinite?
  Enumerate: $(0,0),(0,1),(0,2),\ldots$???
  Never get to $(1,1)$!
  Enumerate: $(0,0),(1,0),(0,1),(2,0),(1,1),(0,2)\ldots$

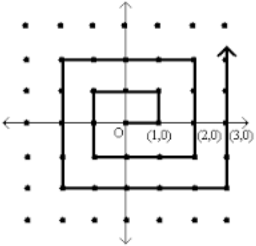
$$
\begin{array}{ccccccc}
(0,0) & \rightarrow & (0,1) & & (0,2) & \rightarrow & (0,3) \\
& \swarrow & & \nearrow & & \swarrow & \\
(1,0) & & (1,1) & & (1,2) & & \ddots \\
\downarrow & \nearrow & & \swarrow & & & \\
(2,0) & & (2,1) & & \ddots & & \\
& \swarrow & & & & & \\
(3,0) & & \ddots & & & & \\
\downarrow & & & & & & \\
\vdots & & & & & &
\end{array}
$$

  (a,b) at position $(a+b+1)(a+b)/2+b$ in this order.

- Positive Rational numbers. Infinite subset of pairs of natural numbers. Same as above!

Rationals

All rational numbers $\mathbb{Q}$: $\frac{a}{b}$, such that $a, b \in \mathbb{Z}$, and $b \neq 0$.
Enumerate: list 0, positive and negative. How?
Same as $\mathbb{Z}^2$!!!! In fact, $\mathbb{Z}^2$ is "bigger" than $\mathbb{Q}$



Enumerate: 0, first positive, first negative, second positive..
Will eventually get to any rational. Where's my bijection???
Too complicated! Enumeration is good enough. Just make sure you don't miss any elements. And that you don't map different elements to the same natural number.

Reals

Is the set of Reals countable?

Lets consider the reals $[0, 1]$.

Each real has a decimal representation.
.500000000... $(1/2)$
.785398162... $\pi/4$
.367879441... $1/e$
.632120558... $1 - 1/e$
.345212312... Some real number

Diagonalization.

If countable, there exists a listing (enumeration), L contains all reals in $[0,1]$. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
⋮

Construct "diagonal" number: $.77677\ldots$

Diagonal Number: Digit i is 7 if number i's ith digit is not 7
and 6 otherwise.

Diagonal number for a list differs from every number in list!
Diagonal number not in list.

Diagonal number is real.

Contradiction!

Subset $[0,1]$ is not countable!!

All reals?

Subset $[0, 1]$ is not countable!!

What about all reals?
Uncountable.

Any subset of a countable set is countable.

If reals are countable then so is $[0, 1]$.

Diagonalization.

1. Assume that a set S can be enumerated.
2. Consider an arbitrary list of all the elements of S.
3. Use the diagonal from the list to construct a new element t.
4. Show that t is different from all elements in the list
   $\implies$ t is not in the list.
5. Show that t is in S.
6. Contradiction.

Another diagonalization.

The set of all subsets of N.

Example subsets of N: $\{0\}$, $\{0,\ldots,7\}$,
evens, odds, primes, multiples of 10

- Assume is countable.
- There is a listing, L, that contains all subsets of N.
- Define a diagonal set, D:
  If ith set in L does not contain i, $i \in D$.
  otherwise $i \notin D$.
- D is different from ith set in L for every i.
  $\implies$ D is not in the listing.
- D is a subset of N.
- L does not contain all subsets of N.

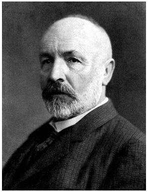
  Contradiction.

Theorem: The set of all subsets of N is not countable.
(The set of all subsets of S, is the **powerset** of N.)

Countable or uncountable??

- Binary strings?
- Trees?
- Weighted trees?
- Inputs to the stable marriage algorithm?
- Mathematical proofs?
- Programs in Java?
- All possible endings to Game of Thrones?
- All subsets of Reals?
- Functions from $\mathbb{N}$ to $\mathbb{N}$?

What happened with Cantor?



Cantor's work between 1874 and 1884 is the origin of set theory.
No one had realized that set theory had any nontrivial content.
Before Cantor: Finite , Infinite
After Cantor:

- Countable
  - Finite and countable. For example $\{1, 2, 3\}$
  - Infinite and countable. For example $\mathbb{N}$, $\mathbb{Z}$, ...
- Uncountable. For example $[0, 1]$, $\mathbb{R}$...
- Bigger than uncountable! (Math 135, Math 136, Math 227A ...)

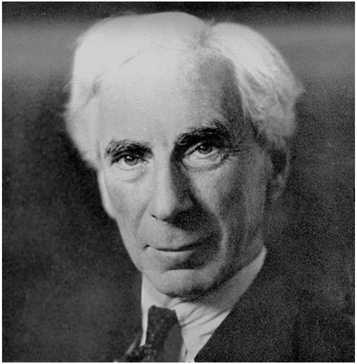
Everyone was upset! Many puzzled... Many openly hostile to Cantor... Cantor was clinically depressed. In and out of hospitals until the end of his life. Died in poverty...

Cantor’s legacy

Gottlob Frege: Let’s look at the foundations!
Clear ambition: Become the new Euclid.
Make up a bunch of axioms for number theory. (In the case of geometry ”A straight line segment can be drawn joining any two points” etc)
Everything that is true in number theory can be inferred from the axioms.
Writes Basic Laws of Arithmetic vol. 1. 680 pages in Amazon.
About to publish vol. 2. And then......
Disaster!!

A bug

Bertrand Russell finds a bug!



Frege's reaction: "Hardly anything more unfortunate can befall a scientific writer than to have one of the foundations of his edifice shaken after the work is finished. This was the position I was placed in by a letter of Mr. Bertrand Russell, just when the printing of this volume was nearing its completion."

A poem

Zisimos Lorentzatos.
”Beware of systems grandiose, of mathematically strict causalities as you’re trying, stone by stone, to found the goldenwoven tower of the logical, castle and fort immune to contradiction. Designed in two volumes, the foundational laws of arithmetic, or Grundgesetze of der arithmetic in 1893, the first, 1903 the second. A life’s work. Hammer on chisel blows for years and years. So far, so good. But as Frege Gottlob was correcting, content, the printer’s proofs already of the second volume, one cursed logic paradox, one not admitting refutation, question by Russell Bertrand, forced, without delay, the great thinker of Mecklemburg to add a last paragraph to his system, show me a great thinker who would resist the truth, accepting the reversible disaster. His foundations in ruin, his logic flawed, his work wasted, and his two volumes imagine the colossal set back, odd load and ballast for the refuge cart.”

Russell's Paradox.

- "This statement is false"
  Is the statement above true?
- A barber says "I shave all and only those men who do not shave themselves."
  Who shaves the barber??
- Self reference.........

Russell's Paradox.

Naive Set Theory: Any definable collection is a set.

$$\exists y \forall x (x \in y \iff P(x)) \tag{1}$$

y is the set of elements that satifies the proposition $P(x)$.

$P(x) = x \notin x$.

There exists a y that satisfies statement 1 for $P(\cdot)$.

Take $x = y$.

$$y \in y \iff y \notin y.$$

Oops!

What type of object is a set that contain sets?

Change Axioms!

Changing Axioms?

But, they kept trying to put all of mathematics on a firm basis.
Trying to find a set of axioms such that is

- Consistent: You can't prove false statements
- Complete: Everything true can be proven.

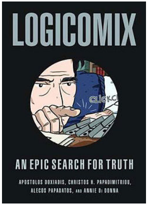
Other people in this story: Russell , Whitehead , Wittgenstein , Hilbert (We must know. We will know.) ...
Until 1931.

Changing Axioms?

Kurt Gödel:
Any set of axioms is either
inconsistent (can prove false statements) or
incomplete (true statements cannot be proven.)

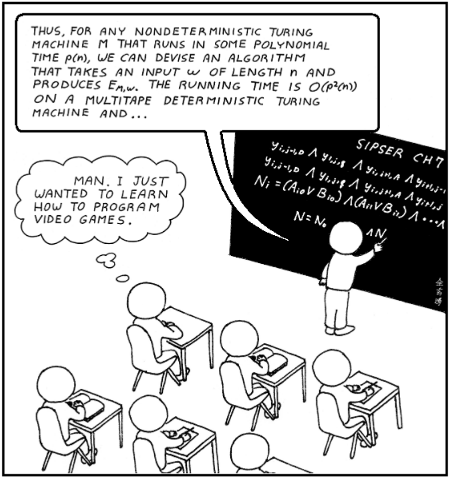
Concrete example:
Continuum hypothesis (see official notes if interested)

- Gödel ..starved himself out of fear of being poisoned..
- Russell .. was fine.....but for two schizophrenic children..
- Wittgenstein ... multiple tragedies in his family.
- Dangerous work?
- See Logicomix by Doxiadis, Papadimitriou (my advisor!), Papadatos, Di Donna.



Next Topic: Undecidability.

- Undecidability. A happy ending?



Turing

Is it actually useful?

Turing: Write me a program checker!

A program that checks that the compiler works!

How about.. Check that the compiler terminates on a certain input.

$HALT(P, I)$
  P - program
  I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Notice:
Need a computer
...with the notion of a stored program!!!!
Program is a text string.
Text string can be an input to a program.
Program can be an input to a program.

Implementing HALT.

$HALT(P, I)$
  P - program
  I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Run P on I and check!

How long do you wait?

Something about infinity here, maybe?

Halt does not exist.

$HALT(P, I)$

P - program

I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Theorem: There is no program HALT.

Halt and Turing.

Proof: Assume there is a program $HALT(\cdot,\cdot)$.

Turing(P)
1. If HALT(P,P) ="halts", then go into an infinite loop.
2. Otherwise, halt immediately.

Assumption: there is a program HALT.
There is text that "is" the program HALT.
There is text that is the program Turing.
Can run Turing on Turing!

Does Turing(Turing) halt?

Turing(Turing) halts
$\implies$ then HALTS(Turing, Turing) $=$ halts
$\implies$ Turing(Turing) loops forever.

Turing(Turing) loops forever
$\implies$ then HALTS(Turing, Turing) $\neq$ halts
$\implies$ Turing(Turing) halts.

Contradiction. Program HALT does not exist! $\square$

Another view of proof: diagonalization.

Any program is a fixed length string.
Fixed length strings are enumerable.
Program halts or not any input, which is a string.

	"P_1"	"P_2"	"P_3"	$\cdots$
P_1	H	H	L	$\cdots$
P_2	L	L	H	$\cdots$
P_3	L	H	H	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Program P_1 halts on input "P_1" and "P_2", doesn't halt on input "P_3", and so on...
Halt - diagonal.
Turing - is not Halt.
and is different from every P_i on the diagonal.
Turing is not on list. Turing is not a program.
Turing can be constructed from Halt.
Halt does not exist! $\square$

Wow, that was easy!

We should be famous!

No computers for Turing!

In Turing's time.

No computers.

Concept of program as data wasn't really there.

Undecidable problems.

Does a program ever print “Hello World”?
Find exit points and add statement: **Print** “Hello World.”

Is there program that makes other programs faster?

Is there program that decides if two other programs are equivalent?

Does this computer program have any security vulnerabilities?

More about Alan Turing.

- Brilliant codebreaker during WWII, helped break German Enigma Code (which probably shortened war by 1 year).
- Seminal paper in numerical analysis: Condition number.
- Seminal paper in mathematical biology.

Turing: personal.

Tragic ending...

- Arrested as a homosexual, (not particularly closeted)
- given choice of prison or (quackish) injections to eliminate sex drive;
- took injections.
- lost security clearance...
- suffered from depression;
- suicided with cyanide at age 42.
  (A bite from the apple....) accident?

British Apology.

Gordon Brown. 2009. “Thousands of people have come together to demand justice for Alan Turing and recognition of the appalling way he was treated. While Turing was dealt with under the law of the time and we can’t put the clock back, his treatment was of course utterly unfair and I am pleased to have the chance to say how deeply sorry I and we all are for what happened to him. Alan and the many thousands of other gay men who were convicted as he was convicted under homophobic laws were treated terribly. Over the years millions more lived in fear of conviction. ....
So on behalf of the British government, and all those who live freely thanks to Alan’s work I am very proud to say: we’re sorry, you deserved so much better.”
2013. Granted Royal pardon.

Summary

Infinity is interesting!

And mind boggling

Computer Programs are an interesting thing.

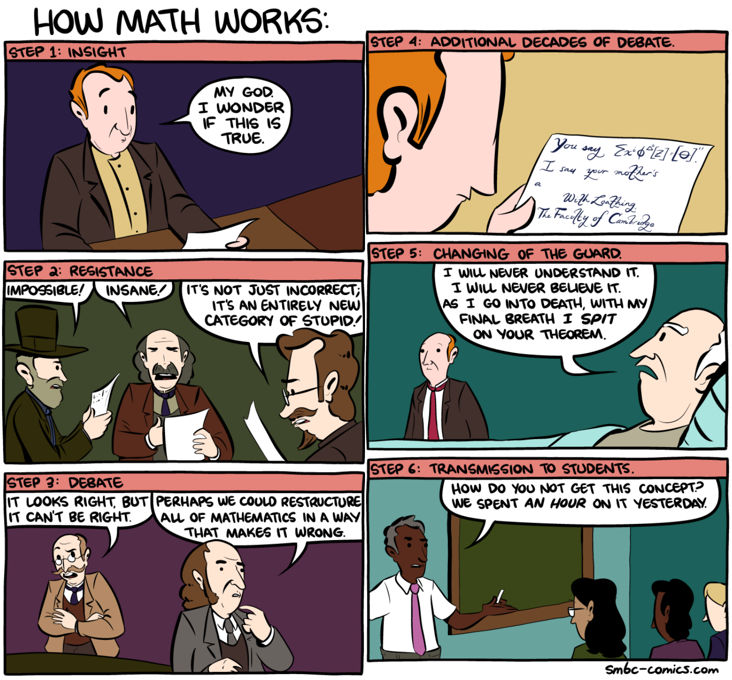
Like Math.

Formal Systems.

Computer Programs cannot completely “understand” computer programs.

Example: no computer program can tell if any other computer program HALTS.

Programming is a super power.


HOW MATH WORKS:
STEP 1: INSIGHT
MY GOD. I WONDER IF THIS IS TRUE.
STEP 2: RESISTANCE
IMPOSSIBLE!
INSANE!
IT'S NOT JUST INCORRECT; IT'S AN ENTIRELY NEW CATEGORY OF STUPID!
STEP 3: DEBATE
IT LOOKS RIGHT, BUT IT CAN'T BE RIGHT.
PERHAPS WE COULD RESTRUCTURE ALL OF MATHEMATICS IN A WAY THAT MAKES IT WRONG.
STEP 4: ADDITIONAL DECADES OF DEBATE.
You say "$\Sigma x^i \phi^\Delta[z]=[\theta]$."
I say your mother's a
With Loathing,
The Faculty of Cambridge
STEP 5: CHANGING OF THE GUARD.
I WILL NEVER UNDERSTAND IT. I WILL NEVER BELIEVE IT. AS I GO INTO DEATH, WITH MY FINAL BREATH I *SPIT* ON YOUR THEOREM.
STEP 6: TRANSMISSION TO STUDENTS.
HOW DO YOU NOT GET THIS CONCEPT? WE SPENT AN *HOUR* ON IT YESTERDAY.
smbc-comics.com