CS70

Counting.

Undecidability.

Countability

Cantor Size: A and B have the same size if there is a bijection between A and B.

A set is **countable** if there is a bijection from A to a subset of the natural numbers.

A set is countably infinite if it is countable and not finite.

A set is countable if one can enumerate it; output elements in a list where every element appears in the list in a specific finite position.

$0, 1, -1, 2, -2, \ldots$ Z is countable.
$\phi, 0, 00, 01, 10, 11, \ldots$ Binary strings are countable.

Be careful: $0, 00, 000, 0000, \ldots$ never gets to 1!

Computer Science: Stream interleaving.
The union of two countable sets is countable!

More fractions?

Are rationals countable.

Enumerate the rational numbers in order...

$0, \ldots, 1/2, ..$

Where is $1/2$ in list?

After $1/3$, which is after $1/4$, which is after $1/5$...

A thing about fractions:
any two fractions has another fraction between it.

Can't even get to "next" fraction!

Can't list in "order".

Pairs of natural numbers.

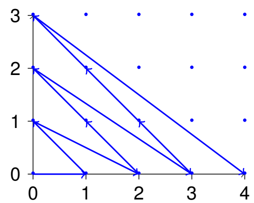
Consider pairs of natural numbers: $N \times N$
E.g.: $(1,2)$, $(100,30)$, etc.

For finite sets S_1 and S_2,
then $S_1 \times S_2$
has size $|S_1| \times |S_2|$.

So, $N \times N$ is countably infinite squared ???

Pairs of natural numbers.

Enumerate in list:
$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), \ldots\ldots$



The pair (a, b), is within the first $(a+b)(a+b)$ elements of list! (i.e., "square containing triangle ").

Countably infinite.

Same size as the natural numbers!!

Rationals?

Positive rational number.
Lowest terms: a/b
$a, b \in N$
with $gcd(a, b) = 1$.

Infinite subset of $N \times N$.

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.

First negative, then nonegative ??? No!

Repeatedly and alternatively take one from each list.
Interleave Streams in 61A

The rationals are countably infinite.

Real numbers..

Real numbers are same size as integers?

The reals.

Are 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 a listing, L contains all reals. For example

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

Construct "diagonal" number: .77677...

Diagonal Number: Digit i is 7 if number i's ith digit is not 7
and 6 otherwise. 6 is apparently isn't afraid!

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?
No.

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, ...

Assume that it 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.)

Diagonalize Natural Number.

Natural numbers have a listing, L.

Make a diagonal number, D:
differ from ith element of L in ith digit.

Differs from all elements of listing.

D is a natural number... Not.

Any natural number has a finite number of digits.

"Construction" requires an infinite number of digits.

The Continuum hypothesis.

There is no set with cardinality between the naturals and the reals.

First of Hilbert's problems!

Cardinalities of uncountable sets?

Cardinality of $(0,1]$ smaller than all the reals?

$f : R^+ \to (0,1]$.

$$f(x) = \begin{cases} x + \frac{1}{2} & 0 \leq x \leq 1/2 \\ \frac{1}{4x} & x > 1/2 \end{cases}$$

One to one. $x \neq y$
If both in $[0,1/2]$, a shift $\implies f(x) \neq f(y)$.
If neither in $[0,1/2]$ a division $\implies f(x) \neq f(y)$.
If one is in $[0,1/2]$ and one isn't, different ranges $\implies f(x) \neq f(y)$.
Onto. Every element in $(0,1]$ has pre-image.
Bijection!

$[0,1]$ is same cardinality as nonegative reals.

Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.

Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.

Can a program refer to a program?

Can a program refer to itself?

Uh oh....

Next Topic: Undecidability.

- Undecidability.

Barber paradox.

Barber announces:
"The barber shaves every person who does not shave themselves."

Who shaves the barber?

Get around paradox?
The barber lies.

Russell's Paradox.

Naive Set Theory: Any definable collection is a set.

$$\exists y \forall x (x \in y \iff P(x)) \qquad (1)$$

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?

Axioms changed.

Changing Axioms?

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

Concrete example:
Continuum hypothesis: "no cardinatity between reals and naturals."
Continuum hypothesis not disprovable in ZFC(Goedel 1940.)

Continuum hypothesis not provable. (Cohen 1963: only Fields medal in logic)

BTW:
Cantor ..bipolar disorder..
Goedel ..starved himself out of fear of being poisoned..
Russell .. was fine.....but for ...two schizophrenic children..
Dangerous work?

See Logicomix by Doxiaidis, Papadimitriou (professor here?), Papadatos, Di Donna.

Is it actually useful?

Write me a program checker!

Check 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!!!!
(not an adding machine! not a person and an adding machine.)

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.

Proof: Yes! No! Yes! No! No! Yes! No! Yes! .. □

What is Rao talking about?
(A) Rao is confused.
(B) Fermat's Theorem.
(C) Diagonalization.

(C). maybe (A) too.

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. See above!
Can run Turing on Turing!

Does Turing(Turing) halt?

Case 1: Turing(Turing) halts
$\Longrightarrow$ then HALTS(Turing, Turing) $=$ halts
$\Longrightarrow$ Turing(Turing) loops forever.

Case 2: Turing(Turing) loops forever
$\Longrightarrow$ then HALTS(Turing, Turing) $\neq$ halts
$\Longrightarrow$ Turing(Turing) halts.

Contradiction. Program HALT does not exist! □

Questions?

Wow.

A lot of mind bending stuff.

See you on Friday to regroup!