Countability and the Uncountable

Lecture 21

How do you count infinity?

- How do you make precise the intuition that there are more real numbers than integers? Both are infinite...
- When do we say two infinite sets A & B have the same size?
- **Definition:** $|A| = |B|$ if there is a bijection from A to B

  Definition good for finite sets too

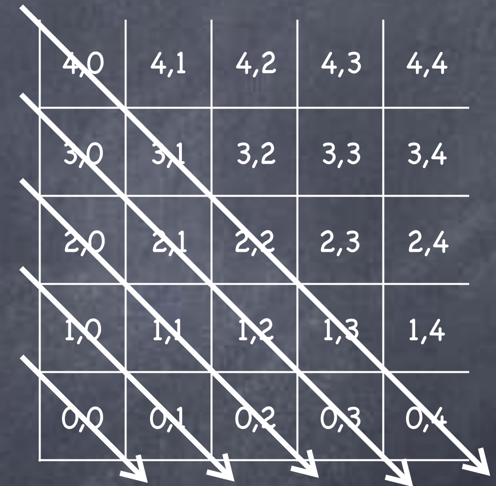
  - $|\mathbb{Z}| = |2\mathbb{Z}|$. ($2\mathbb{Z}$ = evens). $f:\mathbb{Z}\to 2\mathbb{Z}$ defined as $f(x)=2x$ is a bijection
  - $|\mathbb{Z}| = |\mathbb{N}|$. bijection $g:\mathbb{Z}\to\mathbb{N}$: $g(x) = 2x$ for $x\geq 0$, $g(x)=2|x|-1$ for $x<0$
  - $|\mathbb{N}| = |2\mathbb{Z}|$. $h: \mathbb{N}\to 2\mathbb{Z}$ defined as $h = f\circ g^{-1}$

Countable

- A set A is **countably infinite** if $|A|=|\mathbb{N}|$
  - i.e., there is a bijection $f: \mathbb{N} \rightarrow A$
  - Note: $|A|=|\mathbb{N}|$ iff $|A|=|\mathbb{Z}|$, $|A|=|2\mathbb{Z}|$ etc.
- A set is **countable** if it is finite or countably infinite
- Intuition: all "discrete" sets are countable

How do you count infinity?

- **We defined:** A is countably infinite if $|A| = |\mathbb{N}|$, i.e., if there is a bijection between A and $\mathbb{N}$.
  - $\mathbb{N}^2$ is countable. Bijection by ordering points in $\mathbb{N}^2$ on a "curve"

    (0,0), (1,0), (0,1), (2,0), (1,1), (0,2), …
    (i.e., f(0)=(0,0), f(1)=(1,0), f(2)=(0,1) …)
  - Note: (0,0), (1,0), (2,0), (3,0) … will not give a bijection
  - $\mathbb{Z}^2$ is countable. $f:\mathbb{Z}^2 \to \mathbb{N}$ defined as $f(a,b) = h(g(a),g(b))$, where $g:\mathbb{Z} \to \mathbb{N}$ and $h: \mathbb{N}^2 \to \mathbb{N}$ are bijections, is a bijection
  - More generally, if A and B are countable, the A×B is countable (extended to any finite number of sets by induction)

But Things Get Messy...

- Is $|\mathbb{Q}|$ countable?
  - We saw bijection between $\mathbb{Z}^2$ and $\mathbb{N}$. Enough to find a bijection between $\mathbb{Q}$ and $\mathbb{Z}^2$.
  - Not immediately clear: not all pairs (a,b) correspond to a distinct rational number a/b
    - a and b can have a common divisor; also, trouble with b=0
  - But easier to construct a <u>one-to-one</u> function $f:\mathbb{Q}\rightarrow\mathbb{Z}^2$ as $f(x) = (p,q)$ where $x=p/q$ is the "canonical representation" of x (i.e., $\gcd(p,q)=1$ and $q > 0$).
    - Hence one-to-one function $g\circ f:\mathbb{Q}\rightarrow\mathbb{N}$, where $g:\mathbb{Z}^2\rightarrow\mathbb{N}$ is a bijection
  - Also can construct a one-to-one function $h:\mathbb{N}\rightarrow\mathbb{Q}$ as $h(a)=a$

But Things Get Messy...

- Is $|\mathbb{Q}|$ countable?
  - One-to-one functions $f_1:\mathbb{Q}\rightarrow\mathbb{N}$ and $f_2:\mathbb{N}\rightarrow\mathbb{Q}$
  - Intuitively, if a one-to-one function from A to B, $|A|\leq|B|$
    - True for finite sets
- **Definition:** $|A| \leq |B|$ if there is a one-to-one function from A to B

Definition good for finite sets too

- So $|\mathbb{Q}|\leq|\mathbb{N}|$ and $|\mathbb{N}|\leq|\mathbb{Q}|$
- Want to show $|\mathbb{Q}|=|\mathbb{N}|$ (i.e., a bijection between $\mathbb{Q}$ and $\mathbb{N}$)

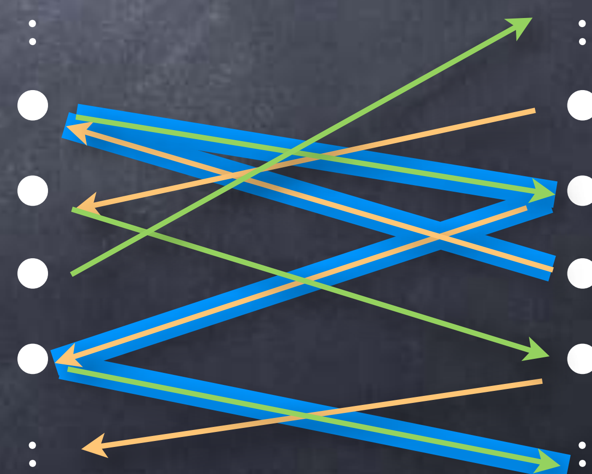
Bijection from Two Injections

Cantor-Schröder-Bernstein

- **Theorem [CSB]:** There is a bijection from A to B if and only if there is a one-to-one function from A to B, and a one-to-one function from B to A
- Restated: $|A|=|B| \Leftrightarrow |A| \leq |B|$ and $|B| \leq |A|$

Trivial for finite sets

- Proof idea: Let $f{:}A \rightarrow B$ and $g{:}B \rightarrow A$ (one-to-one).
- Consider infinite chains obtained by following the arrows
  - One-to-one $\Rightarrow$ no two chains collide. Each node in a unique chain
  - Chain could start from an A node, start from a B node or has no starting node (doubly infinite or cyclic). Say, types A,B and C
  - Let $h{:}A \rightarrow B$ s.t. $h(a)=f(a)$ if a's chain type A; else $h(a)=b$ s.t. $g(b)=a$.



Find a matching

Bijection from Two Injections

- Since $|\mathbb{Q}| \leq |\mathbb{N}|$ and $|\mathbb{N}| \leq |\mathbb{Q}|$, by CBS-theorem $|\mathbb{Q}| = |\mathbb{N}|$
  - $\mathbb{Q}$ is countable
- The set S of all finite-length strings made of [A-Z] is countably infinite
  - Interpret A to Z as the non-zero digits in base 27. Given $s \in S$, interpret it as a number. This mapping ($S \rightarrow \mathbb{N}$) is one-to-one
  - Map an integer n to A^n (string with n As). This is one-to-one.

Summary

Equivalently: there is an onto function from B to A (relying on the "Axiom of Choice")

- **Definition:** $|A| = |B|$ if there is a bijection from A to B
- **Definition:** $|A| \leq |B|$ if there is a one-to-one function from A to B
- **Theorem [CBS]:** $|A|=|B| \Leftrightarrow |A| \leq |B|$ and $|B| \leq |A|$
- A is **countably infinite** if $|A|=|\mathbb{N}|$
  - e.g., $|\mathbb{Z}|=|\mathbb{N}|$, $|2\mathbb{Z}|=|\mathbb{N}|$, $|\mathbb{N}^2|=|\mathbb{N}|$ etc. (saw explicit bijections)
  - e.g., $|\mathbb{Q}|=|\mathbb{N}|$ (saw one-to-one functions in both directions)
- A is **uncountable** if A is infinite but not countably infinite
  - Equivalently, if no function $f : A \rightarrow \mathbb{N}$ is one-to-one
  - Equivalently, if no function $f : \mathbb{N} \rightarrow A$ is onto

Uncountable Sets

- Claim: $\mathbb{R}$ is uncountable
- Related claims:
  - Set $\mathbb{T}$ of all infinitely long binary strings is uncountable
    - Contrast with set of all finitely long binary strings, which is a countably infinite set
  - The power-set of $\mathbb{N}$, $\mathbb{P}(\mathbb{N})$ is uncountable
    - There is a bijection $f: \mathbb{T} \rightarrow \mathbb{P}(\mathbb{N})$ defined as $f(s) = \{ i \mid s_i = 1 \}$

e.g., set of even numbers corresponds to the string 101010...

- How do we show something is not countable?!
- Cantor's "diagonal slash"

Cantor's Diagonal Slash

- To prove $\mathbb{P}(\mathbb{N})$ is uncountable
- Take any function $f: \mathbb{N} \rightarrow \mathbb{P}(\mathbb{N})$
- Make a binary table with $T_{ij} = 1$ iff $j \in f(i)$
- Consider the set $X \subseteq \mathbb{N}$ corresponding to the "flipped diagonal"
  - $X = \{ j \mid T_{jj} = 0 \}$
    $= \{ j \mid j \notin f(j) \}$
- X doesn't appear as a row in this table (why?)
  - So f not onto

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

DVEM

Question

- Which of the following are countably infinite?

  1. Set of all prime numbers
  2. Set of all bit strings of length 32
  3. Set of all bit strings of finite length
  4. Set of all infinitely long bit strings

  A. 1, 2, 3 and 4
  B. 1, 2 and 3 only
  C. 1, 3 and 4 only
  D. 1 and 3 only
  E. None of the above choices

Cantor's Diagonal Slash

- Take any function $f: \mathbb{N} \to \mathbb{P}(\mathbb{N})$
- Make a binary table with $T_{ij} = 1$ iff $j \in f(i)$
- Consider the set $X \subseteq \mathbb{N}$ corresponding to the "flipped diagonal"
  - $X = \{ j \mid T_{jj} = 0 \}$
    $= \{ j \mid j \notin f(j) \}$
- X doesn't appear as a row in this table (why?)
  - So f not onto

Generalizes:

No onto function $f: A \to \mathbb{P}(A)$

for any set A

May not have a table enumerating f (if A is uncountable)

Let $X = \{ j \in A \mid j \notin f(j) \}$

Claim: $\nexists\, i \in A$ s.t. $X = f(i)$

Suppose not: i.e., $\exists i$, $X = f(i)$.

$i \in X \leftrightarrow i \in f(i) \leftrightarrow i \notin X$

Contradiction!

PFYC

Question

- Pick the correct statement. A is a non-empty set.

A. There is no one-to-one function from A to $\mathbb{P}(A)$

B. There is no onto function from $\mathbb{P}(A)$ to A

C. There is no one-to-one function from $\mathbb{P}(A)$ to A

D. There is a bijection between A and $\mathbb{P}(A)$ iff A is finite

E. None of the above

There is an onto function from A to B iff there is a one-to-one function from B to A

Paradoxes and Relatives

- Russell's Paradox: In the universe of all sets, let $S = \{ s \mid s \notin s \}$. Then $S \in S \leftrightarrow S \notin S$!
  - "Naïve Set Theory" is inconsistent. Consistent theories developed which do not let one define such sets.
- In a library of catalogs, can you have a catalog of all catalogs in the library that don't list themselves? (answer: No!)
- Liar's paradox: "This statement is false." (The statement is true iff it is false! Requires a logic with "undefined" as truth value.)
- Gödel numbered statements in a theory and showed that in any "rich" theory there must be a statement with number g which says "statement with Gödel number g is <u>not provable</u>"
  - This statement must be true if theory <u>consistent</u> (else a false statement is provable). Then the theory would be <u>incomplete</u>.

Reals are Uncountable

- We saw that $\mathbb{T}$, the set of infinite binary strings is uncountable
- Enough to show a one-to-one mapping from $\mathbb{T}$ to $\mathbb{R}$ (why?)
- Idea: treat a binary string $s_1s_2s_3...$ as the real number $0.s_1s_2s_3...$ in decimal
    - This is a one-to-one mapping: a finite difference between the real numbers that two different strings map to
    - Note: if used binary representation instead of decimal representation, we'll have strings 011111.. and 10000... map to the same real number (though that can be handled)
- On the other hand $|\mathbb{R}^2| = |\mathbb{R}|$.
    - Because $|\mathbb{T}^2|=|\mathbb{T}|$ (bijection by interleaving), and we saw $|\mathbb{R}|=|\mathbb{T}|$ (and hence $|\mathbb{R}^2|=|\mathbb{T}^2|$ too)