Lecture 35: Diagonalization

Date: December 6, 2019.

Cantor's Definition. For infinite sets A and B, we will say $|A| \leq |B|$ if there is a injective function $f : A \to B$.

- If there is a surjective function $f : A \to B$ then $|A| \geq |B|$.
- We will say $|A| = |B|$ if there is a bijective function $f : A \to B$.

Countable Sets. A (finite or infinite) set A is said to be **countable** if there is an injective function $f : A \to \mathbb{N}$. In other words, if $|A| \leq |\mathbb{N}|$.

Proposition 1. *The sets $\mathbb{Z}$ and $\mathbb{N} \times \mathbb{N}$ are countable.* $\mathbb{Q}$ is countable.

Theorem 2 (Cantor). *For any set A,* $|\mathsf{pow}(A)| \not\leq |A|$

Corollary 3. $\mathsf{pow}(\mathbb{N})$ *is not countable.* Need to show $|\mathsf{pow}(\mathbb{N})| \not\leq |\mathbb{N}|$

We will show any function $f : \mathbb{N} \to \mathsf{pow}(\mathbb{N})$ is not surjective.
Let f be an arbitrary fn. from $\mathbb{N} \to \mathsf{pow}(\mathbb{N})$
Any subset of $\mathbb{N}$ as infinite seq of 0's and 1's

$\mathbb{N}$	0	1	2	3	. . . .	
0	$\boxed{1}$	0	0	1	. . .	$f(0)$
1	0	$\boxed{1}$	0	0	. . . .	$f(1)$
→ 2	1	1	$\boxed{\cancel{1}}$ 0	0	. . .	$f(2)$
⋮						

When row 2 is changed as above
A_f is 001 . . . .

$$A_f = \{ i \in \mathbb{N} \mid i \notin f(i) \}$$

[A_f as a bit sequence <u>0 0 0 . . .</u>

<u>Claim</u>: $A_f \notin \mathrm{img}(f)$.

<u>Proof</u>: Suppose (for contradiction) $A_f = f(i)$

$\underbrace{i \in A_f}_{i\text{th entry} = 1}$ iff $\underbrace{i \notin f(i)}_{i\text{th diag entry} = 0}$ Thus $A_f \neq f(i)$ contradiction.

Computational Problems and Programs

Proposition 4. *The number of programs is countable.*

~~Finite~~ Any program in any language is a finite sequence of ASCII characters.

Consider $num : Progs \rightarrow \mathbb{N}$.

$num(p)$ = number whose representation base $|ASCII|$ is the string p.

num is injective.

Computational Problem. Each problem is a function that demands a certain answer be computed in response to an input.

Decision Problems. Problems that demand a Boolean answer in response to an input. Since every input is a binary string, decision problems are functions of type $\{0,1\}^* \to \{0,1\}$. $f : \mathbb{N} \to \{0,1\}$.

Proposition 5. *The number of decision problems is uncountable.*

The set of decision problems is set fn from $\mathbb{N} \to \{0,1\}$.

$|$Decision prob$| = |$pow$(\mathbb{N})|$

There are computational problems that cannot be solved on computers.