CS201

Mathematics for Computer Science I

Lecture 3

Comparing Cardinalities

- In the last lecture, we showed that $|\mathbb{Q}| = |\mathbb{Z}| = |2\mathbb{Z}| = \aleph_0$.
- Is $|\mathbb{R}| = |\mathbb{Z}|$?
  - No.
  - Proof by diagonalization.
- It will be useful to first show that $|\mathbb{N}| = \aleph_0$.
  - Map

$$f(n) = \begin{cases} 2n+1 & \text{if } n \geq 0 \\ -2n & \text{if } n < 0 \end{cases}$$

    is a bijection between $\mathbb{Z}$ to $\mathbb{N}$.

Cardinality of $\mathbb{R}$

Theorem

$|\mathbb{R}| \neq \aleph_0$.

Proof.

- Consider a mapping $f : \mathbb{N} \mapsto \mathbb{R}$.
- Define a real number r as follows:
  - The number is between 0 and 1.
  - Check if the nth digit after decimal of $f(n)$ is 0. If yes, nth digit after decimal of r is set to 1.
  - If not, nth digit after decimal of r is set to 0.

Cardinality of $\mathbb{R}$

- Number r is well-defined and so $r \in \mathbb{R}$.
- Suppose $f(m) = r$.
- What is the value of mth digit of r?
  - If it is 0, then by definition of r, mth digit would be 1.
  - If it is non-zero, then by definition of r, mth digit would be 0.
- In either case, we have an impossibility and so our assumption that $f(m) = r$ is incorrect.
- Since f was arbitrary function, there exists no bijection between $\mathbb{N}$ and $\mathbb{R}$.
- Hence, $|\mathbb{R}| \neq \aleph_0$.

Cardinality of $\mathbb{R}$

- Previous theorem shows that $\mathbb{R}$ has a higher level of infinity than $\mathbb{Z}$ or $\mathbb{Q}$.
- Let $|\mathbb{R}| = \aleph_1$.
- Intuitively, we see that $\aleph_0 < \aleph_1$.
- We make it precise using, again, mappings between sets.

Comparing Cardinalities

Definition

We say that $|A| \leq |B|$ if there exists a one-to-one map from A to B.

- A one-to-one mapping from A to B embeds A into B without losing any information.
- Hence the definition is logical.
- It holds true for all sets, whether finite or infinite.
- The definition also fits with the Cantor-Bernstein-Schroeder Theorem which, in this notation, states that if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

More Infinities

- Are there infinities beyond $\aleph_1$?
- Yes, infinitely many!

Definition (Power Set)

For any set A, its power set, denoted by $\mathcal{P}(A)$ is defined as:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

More Infinities

Theorem

For any A, $|A| < |\mathcal{P}(A)|$.

Proof.

- If A is finite, then $|\mathcal{P}(A)| = 2^{|A|}$, hence $|A| < |\mathcal{P}(A)|$.
- Suppose A is infinite.
- Then mapping $f(a) = \{a\}$ is a one-to-one map from A to $\mathcal{P}(A)$ showing $|A| \leq |\mathcal{P}(A)|$.

$|A| < |B|$ means $|A| \leq |B|$ and $|A| \neq |B|$.

More Infinities

- Let h be a map from A to $\mathcal{P}(A)$.
- Define a subset B of A as:

$$B = \{x \mid x \in A \,\&\, x \notin h(x)\}.$$

- Suppose there exists $y \in A$ such that $h(y) = B$.
- Is $y \in B$?
  - If $y \in B = h(y)$ then by definition of B, $y \notin B$.
  - If $y \notin B = h(y)$, then by definition of B, $y \in B$.
- An impossibility either way. Hence there is no bijection between A and $\mathcal{P}(A)$.

More Infinities

- Therefore, we can construct infinitely many levels of infinities as:

$$\aleph_1 = |\mathbb{R}| < \mathcal{P}(\mathbb{R}) < \mathcal{P}(\mathcal{P}(\mathbb{R})) < \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R}))) < \cdots .$$

- Following shows that $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Z})|$:
  - Define map $f : \mathbb{R} \mapsto \mathcal{P}(\mathbb{Z})$ as:

$$f(n.d_1d_2d_3\cdots) = \{n, 10^{|n|+1}d_1, 10^{|n|+2}d_2, 10^{|n|+3}d_3, \cdots\}.$$

  - The key property of above set is that $n < 10^{|n|+1}d_1 < 10^{|n|+2}d_2 < 10^{|n|+3}d_3 < \cdots$.
  - f is one-to-one since two real numbers would differ in either their integral part or a digit after decimal.
  - In either case, the corresponding subsets of $\mathbb{Z}$ would be different.

More Infinities

- Following shows that $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$:
  - Define map $g : \mathcal{P}(\mathbb{N}) \mapsto \mathbb{R}$ as:

$$g(A) = 0.b_1 b_2 b_3 \cdots ,$$

    where $b_i = 1$ if $i \in A$ else $b_i = 0$.
  - g is one-to-one since for two distinct subsets of $\mathbb{N}$ there exists an i that belongs to one but not other. And so the output of g on the two subsets will differ on ith digit after decimal.
- It is easy to give a one-to-one map from $\mathcal{P}(\mathbb{Z})$ to $\mathcal{P}(\mathbb{N})$, showing that

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{Z})|.$$

Levels of Infinities

- Let
$$\aleph_i = |\mathcal{P}^i(\mathbb{Z})|,$$
where $\mathcal{P}^i(\mathbb{Z})$ stands for taking power-set i times and $\mathcal{P}^0(\mathbb{Z}) = \mathbb{Z}$.
- We get an infinite sequence of infinities of cardinalities
$$\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 < \cdots .$$

- Are there infinities even higher than all of these?
- Yes! One can show that construction of infinities can be continued indefinitely.

Continuum Hypothesis

- Are there infinities in between $\aleph_i$ and $\aleph_{i+1}$ for any i?
- Continuum Hypothesis states that there exist no infinities in between.
- It has been shown that Continuum Hypothesis can neither be proved not disproved in Zermalo-Fraenkel set theory.
- Hence, it is independent of the standard axioms of set theory.
- We can assume it to be true or false depending on our taste!