Theory of computation

① Automata theory

// what DFAs / NFAs / PDAs or other special computers can or cannot do.

② computability theory

// What a general computer can or cannot do.

③ Computational complexity

// what a computer can or cannot do efficiently.

The diagonalization method

(G. Cantor 1873)

— How do we measure size of a set?

i) Finite set : Just count

ii) Infinite set — not trivial

We will first go through some definitions.

Def

$$f : \underset{\text{Domain}}{A} \to \underset{\text{Co-domain}}{B}$$

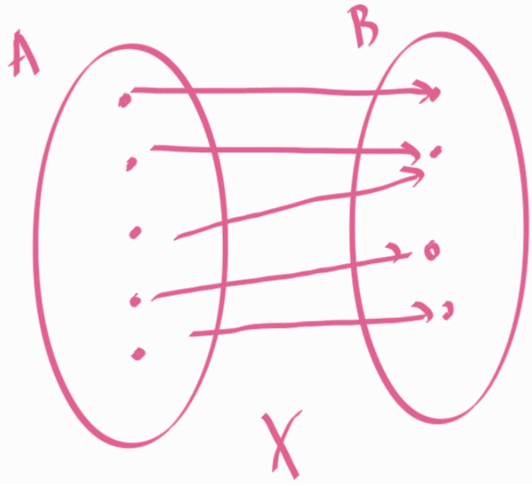
(i) $\forall a \in A$: $f(a)$ is defined

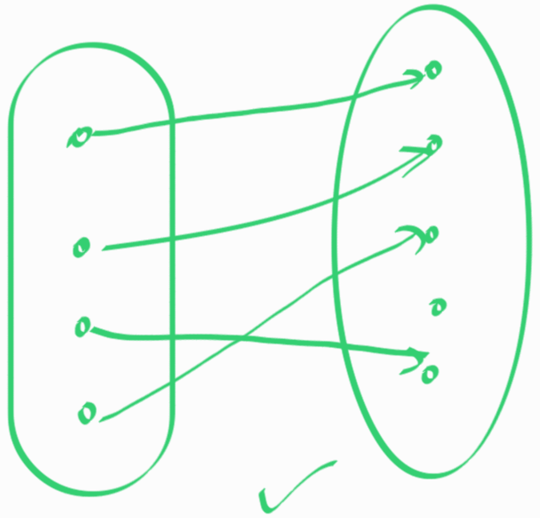
(ii) $\forall a \in A$: $f(a)$ produces an unique value.

(iii) $\forall a \in A$: $f(a) \in B$

Def Given function $f : A \to B$, we say that f is one-to-one (1:1, injective) if,

(i) $\forall a, b \in A$: $f(a) = f(b) \Rightarrow a = b$

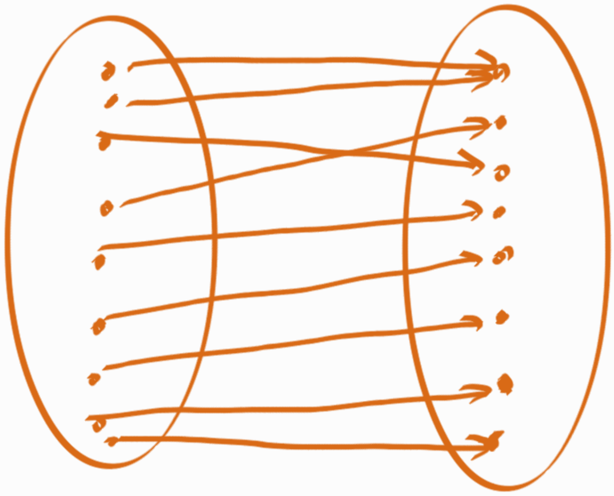




Def

Given function $f: A \to B$, we say that f is onto (surjective), if,

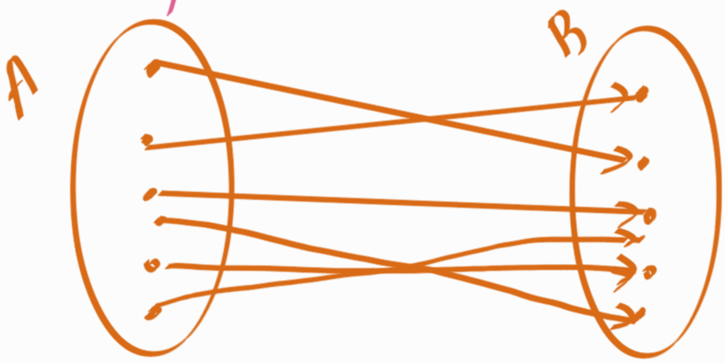
(ii) $\forall b \in B : \exists a : A : f(a) = b$



Def

Given function $f: A \to B$, we say that f is a correspondence (bijective), if f is onto and one-to-one.

Note that if $f: A \to B$ is a correspondence, then $|A| = |B|$



Def

A set A is countable if it is finite or it has the same size as $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.

Theorem

Every subset of a countable set is countable.

Let's look at an example.

$$E = \{e \in \mathbb{N} : e \,\%\, 2 = 0\}$$

I want to define bijection $f : \mathbb{N} \longrightarrow E$

$$f(n) = 2n$$

$$E = \{2, 4, 6, 8, 10, 12, \ldots\}$$

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$$

Ex2: $\mathbb{Q}^+ = \{ m/n : m, n \in \mathbb{N} \}$

- we can show a correspondence between $\mathbb{Q}^+$ and $\mathbb{N}$.

- One way to do this is to list all elements of $\mathbb{Q}^+$.
- we should list all elements of $\mathbb{Q}^+$ exactly once
- Then we can pair up 1^{st} element with 1, 2^{nd} element with 2, and so on.

$p+q=K$

	1	2	3	4	5	6	7 ...
1	$1/1$	$1/2$	$1/3$	$1/4$	$1/5$	$1/6$	$1/7$
2	$2/1$	$2/2$	$2/3$	$2/4$	$2/5$	$2/6$	$2/7$
3	$3/1$	$3/2$	$3/3$	$3/4$	$3/5$	$3/6$	$3/7$ ...
4	$4/1$	$4/2$	$4/3$	$4/4$	$4/5$	$4/6$	$4/7$
5	$5/1$	$5/2$	$5/3$	$5/4$	$5/5$	$5/6$	$5/7$
6	$6/1$	$6/2$	$6/3$	$6/4$	$6/5$	$6/6$	$6/7$
⋮				⋮			

$$\left\{ \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \ldots \right.$$

$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$

$$\left\{ 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots \right.$$

Ex: $\mathbb{R}$ is uncountable.

- In order to show that $\mathbb{R}$ is uncountable, we need to show that there exist no bijection between $\mathbb{R}$ and $\mathbb{N}$.

- proof is by contradiction.

Assume there exist a bijection
$f : \mathbb{N} \longrightarrow \mathbb{R}$.

Then, we must be able to map each element in $\mathbb{N}$ to an unique element in $\mathbb{R}$, and every element in $\mathbb{R}$ must be mapped by this function f.

As an example f could be something like following

n	$f(n)$
1	2.314689.......
2	8.1123478 89.---
3	0.0199999 9.-----
4	0.99111.......
5	
⋮	⋮

$x = 2.1502\ldots\ldots$

we construct $x \in \mathbb{R}$ such that each i^{th} decimal point in x differs from the real number mapped by bijection f.

Since, I can construct this $x \in \mathbb{R}$, and we see that this value is not mapped by the bijection f.

$\therefore$ f cannot be a bijection

$\therefore$ $\mathbb{R}$ is uncountable.