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

Domain ↙ $f : A \to B$ ↖ Co-domain

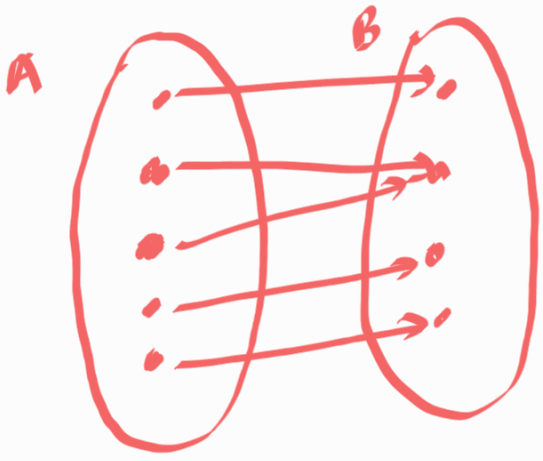
(i) $\forall a \in A$: $f(a)$ is defined

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

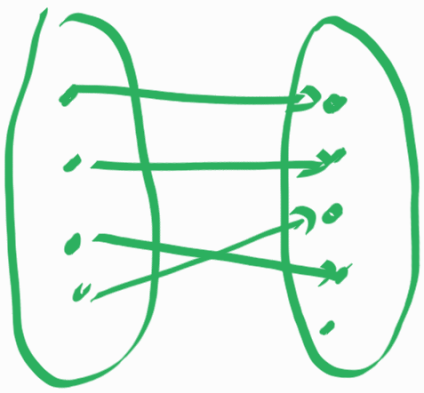
(iii) $\forall a \in A$: $f(a) \in B$

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

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



not one-to-one

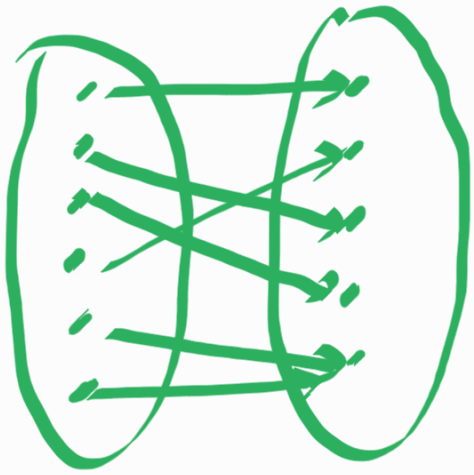


Def

Given function $f: A \to B$,

we say that f is onto (surjective) if,

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

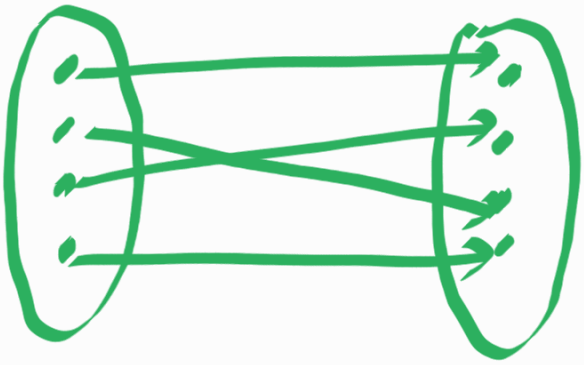


Def

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

Let's look at an example.

Ex 1

$E = \{$ set of all even (natural) numbers $\}$

$f(n) = 2n$

$f : \mathbb{N} \longrightarrow E$

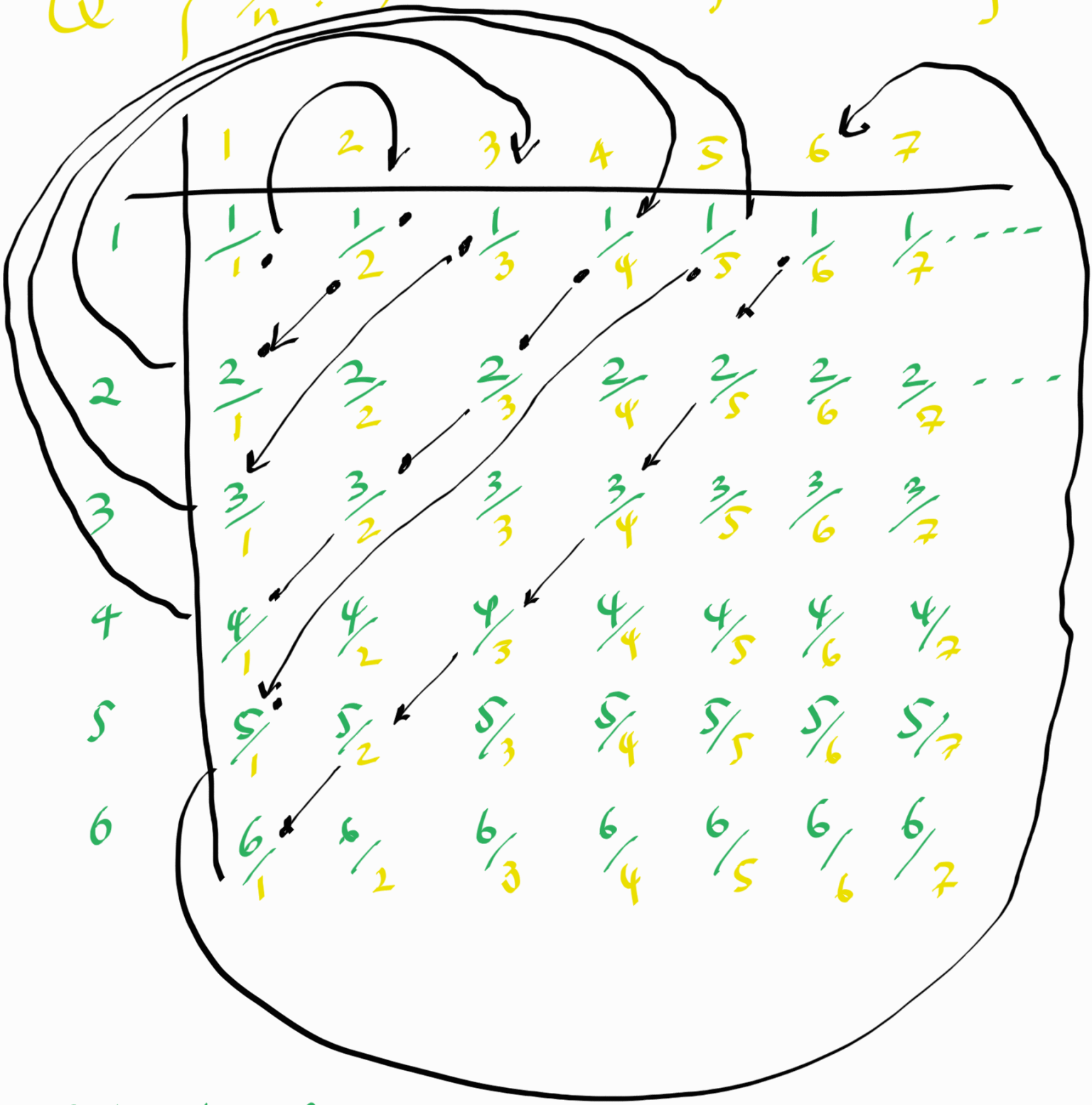
$E = \{ 2, 4, 6, 8, 10, \ldots \}$

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

Ex 2: $\mathbb{Q}^+ = \{ m/n : m, n \in \mathbb{N} \}$

I want to prove set of positive rational numbers are countable.

$\mathbb{Q}^+ = \{ m/n : m, n \in \mathbb{N} \text{ and } \gcd(m,n) = 1 \}$



$\{ 1/1, 1/2, 2/1, 1/3, 3/1, 1/4, 2/3, 3/2, 4/1, \ldots \}$

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