Undecidable problems I

- There quite a few undecidable problems
- For example, program verification is in general not solvable
- We will discuss an undecidable example called the "halting problem"

A_{TM} I

$$A_{TM} = \{\langle M, w\rangle \mid M: \text{ a TM that accepts } w\}$$

- We will prove that A_{TM} is undecidable
- However, A_{TM} is Turing recognizable
- We can simply simulate $\langle M, w\rangle$
- To be decidable we hope to avoid an infinite loop
  if at one point, know it cannot halt
  $\Rightarrow$ reject
- Thus this problem is called the halting problem

Diagonalization method I

- We need a technique called "diagonalization method" for the proof
- It was developed by Cantor in 1873 to check if two infinite sets are equal
- Example: consider

  set of even integers

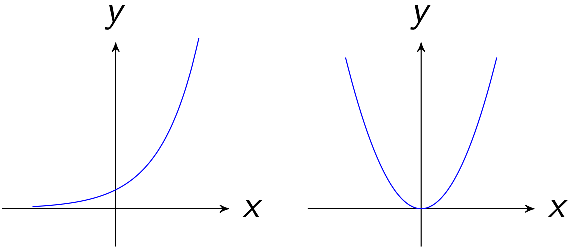
  versus

  set of $\{0, 1\}^*$
- Both are infinite sets. Which one is larger ?
- Definition: two sets are equal if elements can be paired

Definition 4.12 I

- f is a one-to-one function if:

$$f(a) \neq f(b) \text{ if } a \neq b$$



- Left: a one-to-one function; right: not

Definition 4.12 II

- $f : A \to B$ onto if

$$\forall b \in B, \exists a \text{ such that } f(a) = b$$

- Example:

$$f(a) = a^2, \text{ where } A = (-\infty, \infty) \text{ and } B = (-\infty, \infty)$$

This is not an onto function because for $b = -1$, there is no a such that $f(a) = b$

Definition 4.12 III

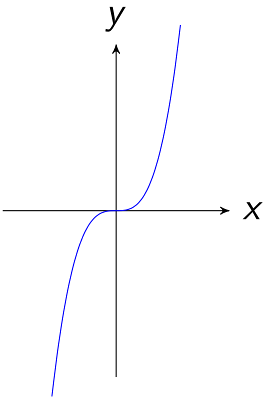
- However, if we change it to

$$f(a) = a^2, \text{ where } A = (-\infty, \infty) \text{ and } B = [0, \infty)$$

  it becomes an onto function
- Definition: a function is called a correspondence if it is one-to-one and onto
- Example:

$$f(a) = a^3, \text{ where } A = (-\infty, \infty) \text{ and } B = (-\infty, \infty)$$

Definition 4.12 IV



- Thus a correspondence is a way of pairing elements of a set with elements of another

Example 4.13 I

- $N = \{1, 2, \ldots\}$
- $E = \{2, 4, \ldots\}$
- The two sets can be paired

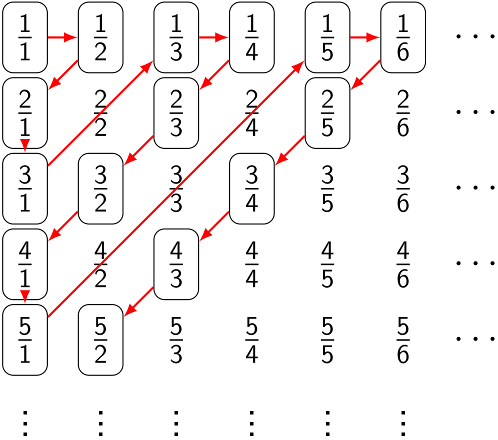
n	$f(n) = 2n$
1	2
2	4
$\vdots$	$\vdots$

- We consider N and E have the same size
- Definition: a set is countable if it is

  finite or same size as N

Rational Numbers Countable I

- $Q = \{m/n \mid m, n \in N\}$ countable



Rational Numbers Countable II

(Latex source from
`https://divisbyzero.com/2013/04/16/countability-of-the-rationals-drawn-using-tikz/`)

- Note that we skip counting elements with common factors (e.g., $2/2$)

Real Numbers not Countable I

- We will use the diagonalization method
- The proof is by contradiction
- Assume R is countable. Then there is a table as follows

n	$f(n)$
1	3.14159 ...
2	55.55555...
3	0.12345 ...
4	0.50000 ...
$\vdots$	

Real Numbers not Countable II

- Consider

$$x = 0.4641\ldots$$
$$4 \neq 1, 6 \neq 5$$

- We have

$$x \neq f(n), \forall n$$

- But $x \in R$, so a contradiction
- To avoid the problem

$$1 = 0.9999\cdots$$

for every digit of x we should not choose 0 or 9