

**Theorem:**

Let  $S$  be a set, then there is no onto mapping  $g: S \rightarrow P(S)$  (from  $S$  to its power set).

Remarks:

- A mapping  $f: S \rightarrow T$  is onto if  $\forall t \in T \exists s \in S: f(s) = t$ .  $f$  is also called “surjective”.
- A mapping  $f: S \rightarrow T$  is one-to-one if  $\forall x, y \in S: x \neq y \Rightarrow f(x) \neq f(y)$ .  $f$  is also called “injective”.
- A mapping  $f: S \rightarrow T$  is a correspondence if  $f$  is one-to-one and onto.  $f$  is also called “bijjective”.

Proof:

Assume that  $g: S \rightarrow P(S)$  is onto. Define a set  $G = \{s \in S \mid s \notin g(s)\} \subset S$ . In particular,  $G \in P(S)$ . Since  $g$  is onto, there exists  $t \in S$  such that  $g(t) = G$ . Then, if  $t \in G$ , then  $t \in g(t)$  then  $t \notin G$  by the definition of  $G$ , a contradiction. If  $t \notin G$  then  $t \notin g(t)$  then by the definition of  $G: t \in G$ , again a contradiction.

Therefore there cannot exist an onto-mapping  $g$  from a set to its power set.  $\square$

**When do 2 sets have the same cardinality:**

For finite sets it is immediate. For infinite sets, there are infinitely sizes of infinity. The intuition to distinguish between different infinities, is to look at how we count: when we count, we construct a correspondence between a finite set of consecutive integers and those objects that we count.

It comes in handy for infinite sets:

**Theorem:**

There are as many even natural numbers as there are natural numbers:  $|\mathbb{N}| = |\mathbb{N}_{\text{even}}|$ .

Proof:

We will construct a correspondence:  $f: \mathbb{N} \rightarrow \mathbb{N}_{\text{even}}$ , that is  $\forall n \in \mathbb{N}: f(n) = 2n$ .

$f$  is one-to-one: let  $m, n \in \mathbb{N}$  then if  $n \neq m$  then  $f(n) = 2n \neq 2m = f(m)$ , as required.

$f$  is onto: let  $m$  be an even integer, then  $m = 2n$  and for  $n \in \mathbb{N}: f(n) = m$ .

Visualization:

$\mathbb{N}$	$\mathbb{N}_{\text{even}}$
1	2
2	4
3	6
...	...
$n$	$2n$

**Theorem:**

There is a correspondence between  $\mathbb{N}$  and  $\mathbb{Z}$ :

Proof:

$g: \mathbb{Z} \rightarrow \mathbb{N}$  is defined as:  $z \rightarrow \begin{cases} 2z, & z \geq 0 \\ -2z - 1, & z < 0 \end{cases}$  – map the positive to even naturals, and negative to odd naturals.

For instance:  $1 \rightarrow 2, 2 \rightarrow 4, -1 \rightarrow 1, -2 \rightarrow 3$  and so on.

To continue the prof we need to formally show that  $g$  is one-to-one and onto.

Some cardinality arithmetic:

$|S| \leq |T|$  if there is an injection (one-to-one mapping) from  $S$  to  $T$ .

**Theorem:**

There is a correspondence between  $\mathbb{N}$  and  $\mathbb{Q}$ .

Proof:

First, we need to show that there are as many positive rational numbers as there are naturals, as we've seen a correspondence  $\mathbb{Z} \rightarrow \mathbb{N}$  and we can apply that logic here. So we'll look for a correspondence in  $\mathbb{N} \rightarrow \mathbb{Q}^+$ . The book writes in a table all rational numbers in their numerator/denominator representation, and maps them to  $\mathbb{N}$  diagonally, skipping over numbers already seen:

	Denominator				
N	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$
U	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$
M	$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$
E	$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$
R	$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$

The diagram shows a grid of rational numbers. Blue arrows indicate a path starting from the top-left cell (1/1) and moving diagonally down and to the right. Red arrows indicate that certain cells are skipped because they have already been visited. For example, after visiting 1/1, the path skips 2/1 and 3/1, moving to 2/2. From 2/2, it skips 3/2 and 4/2, moving to 3/3. From 3/3, it skips 4/3 and 5/3, moving to 4/4. From 4/4, it skips 5/4, moving to 5/5. The path continues in this manner, zig-zagging across the grid.

The blue arrows show the direction of the mapping, the red ones jump over those already mapped (e.g.  $\frac{1}{1}$  is mapped, then we skip over  $\frac{2}{1}, \frac{3}{1}$  and so on).

**Recounting the Rationals (Calkin and Wilf, 2000):**

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{2}{3}, \frac{3}{2}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{2}{5}, \frac{5}{3}, \dots$$

If we look at  $(b_n) = 1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, \dots$

$b_n$  is the number of hyperbinary representations on  $n$  (representations as a sum of powers of 2, where each power repeats 0, 1, or 2 times in the representation). For instance,  $b_5 = 2$  means that 5 has 2 binary representations (sums of powers of 2):  $4 + 1$  or  $2 + 2 + 1$ .

The paper actually shows that the sequence of numerators is  $b_n$ . The paper shows that the sequence holds:  $f(2n + 2) = f(n) + f(n + 1)$ . For instance,  $f(10) = f(5) + f(4) = 2 + 3 = 5$ :

$4 = 1 \cdot 2^2 = 2 \cdot 2^1 = 2 \cdot 2^0 + 1 \cdot 2^1 - 3$  representations; and we have already seen 5 has 2.

In addition:  $f(2n + 1) = f(n)$ . These 2 formulas give us a recursion that allows us computing all hyperbinary representations.

We can consider these numbers as a tree: If the parent is of the form  $\frac{i}{j}$  then the left child is  $\frac{i}{j+i}$  and the right child is  $\frac{i+j}{j}$ .

The paper states that the numerator and denominator of the parent, left and right child are relatively prime. If there's a rational in the tree  $\frac{r}{s}$  such that  $r, s$  are NOT relatively prime ( $\gcd(r, s) > 1$ ), then let  $\frac{r}{s}$  be on the minimal level. If  $\frac{r}{s}$  is a left child, then its parent is  $\frac{r}{s-r}$ . But since  $r, s$  are not relatively prime, also  $r, s-r$  are not, so  $r, s-r$  would have a common divisor – a contradiction to the minimality of the level of  $\frac{r}{s}$ . If  $\frac{r}{s}$  is a right child, its parent is  $\frac{r-s}{s}$ , and again a contradiction. The rest is in the paper.

### Theorem:

There is no correspondence between  $\mathbb{N}$  and  $\mathbb{R}$ .

### Proof:

By contradiction, assume there is such correspondence  $g: \mathbb{N} \rightarrow \mathbb{R}$ . Look at the decimal expansions of  $g(1), g(2), g(3), \dots$ :

	$10^{-1}$	$10^{-2}$	$10^{-3}$	$10^{-4}$
$g(1)$	<b>0</b>	1	5	5
$g(2)$	4	<b>7</b>	8	4
$g(3)$	7	9	<b>9</b>	0
	...			
$g(k)$				

$g(k)$  is defined to have at each  $i$ th position a number that is different than the  $i$ th position of  $g(i)$ . So we define that number  $a = 0.a_1a_2a_3a_4 \dots$  such that  $\forall i \geq 0: a_i \neq g(i)$ . But  $a$  is one of the numbers, i.e. for some  $j: g(j) = a$ , but then  $a$  has to have  $a_j$  different than the  $j$ th digit of  $g(j) = a$ , i.e.  $a_j$ , a contradiction.

Therefore there is no correspondence between  $\mathbb{N}$  and  $\mathbb{R}$ .  $\square$

## The Halting Problem

We show that  $A_{TM} = \{(M, w) \mid M \text{ is a Turing machine and } M \text{ accepts } w\}$  is undecidable.

Note:  $A_{TM}$  is trivially Turing-recognizable: simulate  $M$  on  $w$ , if it accepts – accept; otherwise – either reject or loop forever.

Given a finite  $\Sigma$ , there is a correspondence between  $\mathbb{N} \rightarrow \Sigma^*$ . Therefore we can enumerate all encodings of a Turing machine and inputs – we go over all strings lexicographically and check if they are valid; same goes for input: it has an enumeration.

So if  $A_{TM}$  was decidable, we could have check if a machine halts. If so – simulate it and return whether it accepts or rejects, and if it doesn't halt – reject. Therefore we can construct the EXACT opposite machine, and that machine will appear as an input at some index  $j$  – and then the machine at position  $j$ , with a given input word of itself, it will do what it doesn't do – a contradiction.

So: there are Turing machines  $M_1, M_2, M_3, \dots$  and input words  $w_1, w_2, w_3, \dots$ . Consider the table:

	$M_1$	$M_2$	$M_3$		$M_j$
$M_1$	acc	rej	rej	...	...
$M_2$	acc	rej	acc		...
$M_3$	rej	acc	acc		...
...					
$M_j$	rej	acc	rej		???

There are also languages that are not even Turing-recognizable. Consider a lexicographic enumeration of all possible inputs over  $\{0,1\}^*$ , and the characteristic vector of any possible TM such that at any position  $i$  is has 0 if it rejects  $w_i$  and 1 otherwise. We will continue next week.