Undecidability

1. What is undecidability?

There is a specific problem that is unsolvable by an algorithm. In one type of unsolvable problem, you are given a computer program and a precise specification of what the program is supposed to do. So, you need to verify that the program performs as specified.

The undecidability of a specific language highlights the problem of determining whether a Turing Machine accepts a given input string.

Let $A_{TM} = \{ \langle M, w \rangle \mid M \text{ is a TM and } M \text{ accepts } w \}$

2. The diagonalization method. (Un)countable sets

The proof of the undecidability is based on a technique called diagonalization, discovered by George Cantor in 1873. Cantor was concerned with the problem of measuring the sizes of infinite sets. If we have two infinite sets, how can we tell whether one is larger than the other or whether they are of the same size? For finite sets, we simply count the elements and the resulting number is its size.

Cantor proposed a rather nice solution to this problem. He observed that two finite sets have the same size if the elements of one set can be paired with the elements of the other set. We can extend this idea to the infinite sets.

We call injective function if $f(a) \neq f(b)$ whenever $a \neq b$.

We call surjective function if $f: A \to B$ and for every $b \in B$ there is an $a \in A$ so that $f(a) = b$.

If a function is both injective and surjective, then we call it bijective or correspondance. In a correspondance, every element of set A maps to a unique element of set B.

Example:

Let $\mathbb{N}$ be $\{1, 2, 3 \dots\}$, the set of natural numbers.

Let $\mathcal{E}$ be the set of even natural numbers $\{2, 4, 6 \dots\}$

Using Cantor's method the sets have the same size because of the mapping function from $\mathbb{N}$ to $\mathcal{E}$: $f(n) = 2n$.

We can visualize f in the above table.

n	$f(n)$
1	2
2	4
3	6
$\vdots$	$\vdots$

Pairing each member of $\mathbb{N}$ with its own $\mathcal{E}$ is possible, so we declare these sets to be the same size.

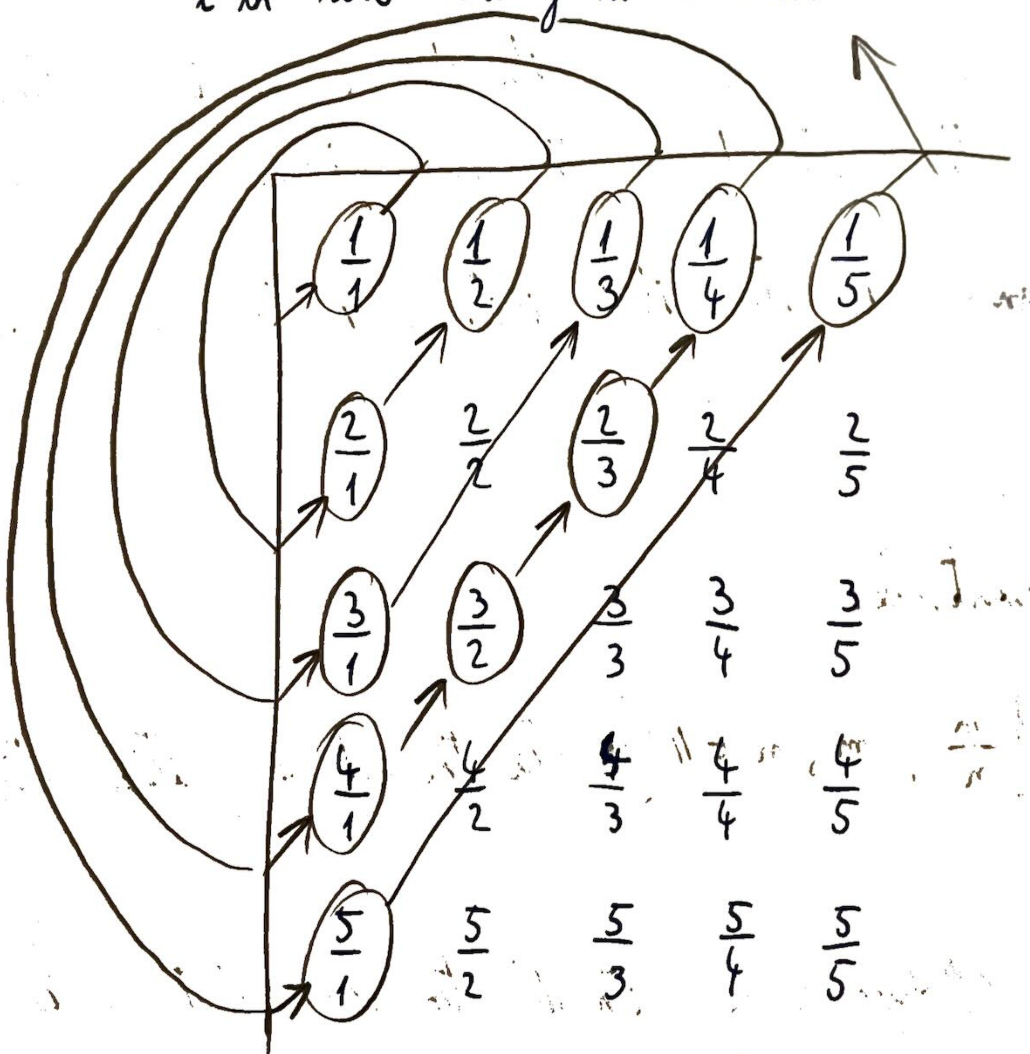
A set is **countable** if either it is finite or has the same size as $\mathbb{N}$.

3. Q is countable.

Let $Q = \left\{ \frac{m}{n} \mid m, n \in \mathbb{N} \right\}$ be the set of positive rational numbers.

We give a correspondence with $\mathbb{N}$ to show that Q is countable. One easy way to do this is list all the elements of Q. Then we pair the first element on the list with the number 1 from $\mathbb{N}$, the second element on the list with number

2 from $\mathbb{N}$, and so on. To get this list, we make an infinite matrix containing all the positive rational numbers, as shown below. The i-th row contains all numbers with numerator i and the j-th column has all numbers with denominator j. So, the number $\frac{i}{j}$ occurs in the i-th row and j-th column.



The first diagonal contains the single element $\frac{1}{1}$, and the second diagonal contains the two elements $\frac{2}{1}$ and $\frac{1}{2}$. So the first three elements are $\frac{1}{1}$, $\frac{2}{1}$ and $\frac{1}{2}$ in the list. In the third diagonal, a complication arises. It contains $\frac{3}{1}$, $\frac{2}{2}$ and $\frac{1}{3}$. But $\frac{2}{2} = \frac{1}{1}$, so we have a repetition. We avoid doing so by skipping an element when it would cause a repetition. So we add only the two elements $\frac{3}{1}$ and $\frac{1}{3}$. Continuing this way, we obtain a list of all elements of $\mathbb{Q}$.

However, for some infinite sets, no correspondence with $\mathbb{N}$ exists. These sets are simply too big. Such sets are called uncountable.

4. $\mathbb{R}$ is uncountable

In order to show that $\mathbb{R}$ is uncountable, we show that there is no correspondence between $\mathbb{N}$ and $\mathbb{R}$. The proof is by contradiction. Suppose that a correspondence f exists between $\mathbb{N}$ and $\mathbb{R}$. We must find an $x \in \mathbb{R}$ that is not paired with anything from $\mathbb{N}$.

We choose each digit of x to make x different from one of the real numbers that is paired with an element of $\mathbb{N}$. In the end, we are sure that x is different from any real number that is paired.

Suppose that the correspondence f exists.

$f(1) = 3.14159...$

$f(2) = 55.5555....$

$f(3) = ...$ and so on

The table below shows the correspondance between $\mathbb{N}$ and $\mathbb{R}$.

n	$f(n)$
1	$3.\underline{\underline{1}}4159...$
2	$55.5\underline{\underline{5}}55...$
3	$0.12\underline{\underline{3}}45...$
4	$0.500\underline{\underline{0}}0....$
$\vdots$	$\vdots$

$x = 0.4641....$

Our objetive is to ensure that $x \neq f(n)$ for any n.

$x \neq f(1)$ only if the first digit of x is different from the first fractional digit 1 of $f(1) = 3.\underline{\underline{1}}4159$. Arbitrarily, we let it be 4

We continue the same way. $f(2) = 55.\underline{\underline{5}}5555\ldots$ so the second digit of x must be different from the second digit of $f(2)$. Arbitrarily we let it be 6. Continuing this way down the diagonal of the table for f we obtain all the digits of x as shown in the table. We know that x is not $f(n)$ for any n because it differs from $f(n)$ in the n-th fractional digit.

So there is no $f(n) = x$, that means there is no correspondence between $\mathbb{N}$ and $\mathbb{R}$. This proves that $\mathbb{R}$ is uncountable.

5. Some languages are not Turing-recognizable

The set of all Turing machines is countable because each Turing machine M has an encoding into a string $\langle M \rangle$.

The set of all infinite binary sequences in uncountable. Let B be the set of all infinite binary sequences. We can prove that B is uncountable with the same method used for the $\mathbb{R}$ set.

Let $\mathcal{L}$ be the set of all languages over alphabet Σ. We show that $\mathcal{L}$ is uncountable by giving a correspondence with B. Let $\Sigma^* = \{s_1, s_2, s_3 \ldots\}$. Each language $A \in \mathcal{L}$ has a unique sequence in B. The i-th bit of that sequence is a 1 if $s_i \in A$ else is a 0. This is called characteristic sequence of A. For example, if A were the language of all strings with a 0 over the alphabet $\{0, 1\}$, its characteristic sequence X_A would be:

$$\Sigma^* = \{ \varepsilon, 0, 1, 00, 01, 10, 11, 000, 001 \dots \}$$

$$A = \{ \quad , \underline{\underline{0}}, \quad , \underline{\underline{00}}, \underline{\underline{01}}, \quad , \quad , \underline{\underline{000}}, \underline{\underline{001}} \dots \}$$

$$X_A = 0 \ \underline{\underline{1}} \ 0 \ \underline{\underline{1}} \ \underline{\underline{1}} \ 0 \ 0 \ \underline{\underline{1}} \ \underline{\underline{1}} \dots$$

The function $f : \mathcal{L} \rightarrow \mathcal{B}$ where $f(A)$ equals the characteristic sequence of A, is bijective, and hence is a correspondence. Therefore, as $\mathcal{B}$ is uncountable, $\mathcal{L}$ is uncountable as well.

Thus, the set of all languages cannot be put in a correspondance with the set of all Turing machines.

6. A_{TM} is undecidable

$A_{TM} = \{ \langle M, w \rangle \mid M$ is a TM and M accepts $w \}$

We assume that A_{TM} is decidable and obtain a contradiction.

Suppose we have a decider H for A_{TM} and behaves the following way:

$$H(\langle M, w \rangle) = \begin{cases} \text{accept} & \text{if } M \text{ accepts } w \\ \text{reject} & \text{if } M \text{ does not accept } w \end{cases}$$

Let D be a new TM that calls H to determine what M does when the input to M is its own description $\langle M \rangle$. So, D acts the opposite. It rejects if M accepts and accepts if M rejects.

$$D(\langle M \rangle) = \begin{cases} \text{accept} & \text{if } M \text{ does not accept } \langle M \rangle \\ \text{reject} & \text{if } M \text{ accepts } \langle M \rangle \end{cases}$$

The same happens if we run D on its own description $\langle D \rangle$

$$D(\langle D \rangle) = \begin{cases} \text{accept} & \text{if } D \text{ does not accept } \langle D \rangle \\ \text{reject} & \text{if } D \text{ accepts } \langle D \rangle \end{cases}$$

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	....	$\langle D \rangle$
M_1	accept	reject	accept	reject		accept
M_2	accept	accept	accept	accept	....	accept
M_3	reject	reject	reject	reject		reject
M_4	accept	accept	reject	reject		accept
⋮						
D	reject	reject	accept	accept		?

Suppose $H(\langle M_1, \langle M_1 \rangle \rangle) = \text{accept}$, $H(\langle M_1, \langle M_3 \rangle \rangle) = \text{accept}$ and so on for all $M_{i \in [1,4]}$ on the table. The other cases are the opposite , so there is a rejection.

Now we introduce D in the table. The point is that $D\langle M_i\rangle$ is accept if $H(\langle M_i, \langle M_i\rangle\rangle)$ is reject and the opposite. So, we look in the table on the diagonal and deny the entry on line and column i. For example, if $H(\langle M_1, \langle M_1\rangle\rangle)$ is accept then $D\langle M_1\rangle$ is reject and so on for every i. We continue this process until we reach $D(\langle D\rangle)$ which by its definition it must be the opposite of itself. This is a contradiction, so we proved that A_{TM} is undecidable.