1 Diagonalisation

Theorem 1.1

$P(\mathbb{N})$ is uncountable.

Proof.

Suppose $P(\mathbb{N})$ is countable. Thus, there is a surjective function $f : \mathbb{N} \to P(\mathbb{N})$.

Let $D = \{i \in \mathbb{N} \,|\, i \notin f(i)\} \in P(\mathbb{N})$.

Since f is surjective, there exists $j \in \mathbb{N}$ such that $f(j) = D$.

Then for all $i \in \mathbb{N}$ $i \in f(j)$ if and only if $i \in D$, and thus iff $i \notin f(i)$.

Since $j \in \mathbb{N}$, by specialisation $j \in f(j)$ IFF $j \notin f(j)$, which is a contradiction.

Therefore, $P(\mathbb{N})$ is uncountable. □

Now, let $S \subseteq \{1, 2, 3, 4\}$. Note that S can be represented by a binary sequence S_1, S_2, S_3, S_4, where $S_i = \begin{cases} 1, i \in S \\ 0, i \notin S. \end{cases}$

Each S_i is called a *characteristic vector* of the set S.

In thus way, for example, $0, 1, 1, 0$ denotes $\{2, 3\}$ and $0, 0, 0, 0$ denotes $\emptyset$.

Consider a list of all subsets of $\mathbb{N}$, possibly with duplications, in the form of an infinite two-dimensional Boolean array M, where $M[i, j] = f(i)_j$:

$$\begin{pmatrix} f(0) : f(0)_0 & f(0)_1 & \cdots & f(0)_j & \cdots \\ f(1) : f(1)_1 & f(1)_1 & \cdots & f(1)_j & \cdots \\ & \vdots & \ddots & & \end{pmatrix}$$

The characteristic vector of D is the complement of the diagonal of the matrix M.

Note that the characteristic vector of D does not agree with row i of M in column i. The characteristic vector is equal to 1 if and only if $i \notin f(i)$. Thus, M does not contain D, which contrandicts that f is surjective.

Theorem 1.2

The set of all functions from $\mathbb{N}$ to $\mathbb{N}$ is uncountable.

Proof.

Suppose $\mathcal{F}$ is countable. Then there is a surjective function $f : \mathbb{N} \to \mathcal{F}$.

f_i is a function from $\mathbb{N}$ to $\mathbb{N}$. Construct an infinite two-dimensional matrix where row i corresponds to $f_i \in f$. Define $g(n) = f(n) + 1$. Note that $g \in \mathcal{F}$, since for all $n \in \mathbb{N}$, $f_n(n) \in \mathbb{N}$ and $\mathbb{N}$ is closed under addition.

Since f is surjective, then $g = f_n$ for some $n \in \mathbb{N}$. Then $g(n) = f_n(n)$. By definition, $g(n) = f_n(n) + 1 \neq f_n(n)$. This is a contradiction, and therefore $\mathcal{F}$ is uncountable. □

If Σ is a finite set of letters, let Σ^* be a set of all finite strings of letters from Σ.

For example, $\{0, 1\}^*$ is the set of all finite length binary strings.

Note that there are 2^k binary strings of length $k \in \mathbb{N}$.

Theorem 1.3
$\{0,1\}^*$ is countable.

Proof.

Exercise. Construct a surjective function f from $\mathbb{N}$ to $\{0,1\}^*$. $\square$

In general, if $|\Sigma| = s$, then there are s^k strings of length k in Σ^*.

The set of all finite strings of ASCII characters is countable.

Example 1.4
The set of all syntactically correct C programmes is countable, since it is a subset of ASCII*.

There is a function G that determines whether a given ASCII string P is a syntactically correct C function:

$$G : \text{ASCII}^* \to \{0,1\}, \tag{1}$$

and thus

$$G(P) = \begin{cases} 1, & \text{if P is a syntactically correct C function} \\ 0, \text{otherwise} \end{cases} \tag{2}$$

Consider the function $H : \text{ASCII}^* \times \text{ASCII}^* \to \{0,1\}$ such that

$$H(P,x) = \begin{cases} 1\text{if P is a syntactically correct C program that eventually returns an input } X \\ 0 \text{ otherwise.} \end{cases}$$

In this way, $H(P,x)$ returns 0 if $P$is not syntactically correct or P runs forever on input X.

The halting problem is solvable if such a C function H exists.

Theorem 1.5
The halting problem is not solvable.

Proof.

We proceed by contradiction and diagonalisation.

By way of contradiction, assume that such a function H exists.

Consider the syntactically correct C-function D defined by the following program:

D(x); {

if (H(x,x))

while (1) { };

else return 1; }

When D runs on input D, if $H(D, D) = 0$, then D returns on input D. If $H(D, D) = 1$, then D goes into an infinite loop on input D.

By the definition of H, if D returns on input D, then $H(D, D) = 1$.

If D goes into an infinite loop on input D, then $H(D, D) = 0$.

These are contradictory, and thus the halting problem is unsolvable and hence such a function H does not exist.

$\square$