Subsets of Countable Sets

A function $f : A \to B$ is called a *one-to-one correspondence* (between A and B) if it is one-to-one and onto.

Theorem.

> Every subset of a countable set is countable.

Proof. It is sufficient to show that subsets of $\mathbf{P}$ are countable. Let A be a subset of $\mathbf{P}$.

If A is finite it is countable by definition.

Suppose A is infinite. We define a one-to-one correspondence f from $\mathbf{P}$ to A by recursion:

1. Let $f(1)$ be the smallest element of A.

2. If $n > 1$, then $f(n)$ is defined to be the smallest element of $A \setminus \{f(1), \ldots, f(n-1)\}$.

It can easily be verified that f is one-to-one and onto. ∎

Note that the above proof uses the so-called *well-ordering principle* of the natural numbers:

> *Every non-empty subset of* $\mathbf{N}$ *has a smallest element.*

Cartesian Products of Countable Sets

Theorem.

The set $\mathbf{P} \times \mathbf{P}$ is countable.

Sketch of proof. We define a one-to-one correspondence between $\mathbf{P}$ and $\mathbf{P} \times \mathbf{P}$ by "enumerating" all ordered pairs of positive natural numbers as follows:

$$\begin{array}{cccc} (1,1) & (1,2) & (1,3) & (1,4) & \ldots \\ (2,1) & (2,2) & (2,3) & (2,4) & \ldots \\ (3,1) & (3,2) & (3,3) & (3,4) & \ldots \\ (4,1) & (4,2) & (4,3) & (4,4) & \ldots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$

■

Corollary

> The Cartesian product of two countable sets is countable.

Proof. Let A and B be countable sets. Thus there are one-to-one correspondences f between A and $\mathbf{P}$ and g between B and $\mathbf{P}$. But then the function h defined by $h(x, y) = (f(x), g(y))$ is a one-to-one correspondence between $A \times B$ and $\mathbf{P} \times \mathbf{P}$.

It follows immediately from the definition of countability that if there is a one-to-one correspondence between two sets X and Y, then one set is countable if and only if the other is countable.

We already know that $\mathbf{P} \times \mathbf{P}$ is countable. Consequently $A \times B$ is also countable. ∎

Examples of Countable Sets

The set of integers $\mathbf{Z}$ is countable. A suitable bijection from $\mathbf{Z}$ to $\mathbf{P}$ is the function f, defined by:

$$f(n) = \begin{cases} 2n+1 & \text{if } n \geq 0 \\ -2n & \text{if } n < 0 \end{cases}$$

Surprisingly, the set of rational numbers $\mathbf{Q}$ is also countable.

Proof. The set of integers $\mathbf{Z}$ is countable. Hence by the above theorem, the set $\mathbf{Z} \times \mathbf{Z}$ is also countable.

But the set of rational numbers $\mathbf{Q}$ is a subset of $\mathbf{Z} \times \mathbf{Z}$, and therefore is also countable. ∎

Countability of Formal Languages

Theorem.

> The set Σ^* of all strings over an alphabet Σ is countable.

Proof. We use the fact that

$$\Sigma^* = \bigcup_{k \in \mathbf{N}} \Sigma^k,$$

where Σ^k denotes the set of all strings of length k.

Since all sets Σ^k are countable, there are corresponding *one-to-one* functions $f_k : \Sigma^k \to \mathbf{N}$.

We define a function $f : \Sigma^* \to \mathbf{N} \times \mathbf{N}$ by:

$$f(w) = (f_{|w|}(w), |w|).$$

The function f is one-to-one. (If $f(w) = f(v)$, then $|w| = |v|$ and $f_{|w|}(w) = f_{|v|}(v) = f_{|w|}(v)$. But since $f_{|w|}$ is one-to-one, we may conclude that $w = v$.)

By the theorems we proved previously, Σ^* is countable.

∎

Note that the proof does not depend on the assumption that Σ is finite, but shows that the statement is valid for infinite sets Σ as well.

The Diagonalization Principle

We next discuss a mathematical proof technique that has important applications in the theory of computation.

The Diagonalization Principle.

> Let R be a binary relation on a set A, and let D, the *diagonal set* for R, be $\{a \in A \ : \ (a, a) \notin R\}$. Furthermore, for each $a \in A$, let R_a be the set $\{b \in A \ : \ (a, b) \in R\}$.
>
> Then the set D is distinct from each set R_a.

We illustrate this principle by an example.

Example of Diagonalization

For example, let R be the binary relation

$$\{(a,b),(a,d),(b,b),(b,c),(c,c),(d,b),(d,c),(d,e),(e,e)\}.$$

This relation can be represented by a table:

	a	b	c	d	e
a		x		x	
b		x	x		
c			x		
d		x	x		x
e					x

We have

$$\begin{aligned} R_a &= \{b,d\} \\ R_b &= \{b,c\} \\ R_c &= \{c\} \\ R_d &= \{b,c,e\} \\ R_e &= \{e\} \end{aligned}$$

and $D = \{a,d\}$.

Note that these sets correspond to the rows in the above table. The set D is represented by a sequence of boxes

x			x	

that is different from each row in the above table.

Application of Diagonalization: Uncountable Sets

Theorem.

The powerset of $\mathbf{N}$ is uncountable.

Proof. We prove the theorem by contradiction. Suppose $\mathcal{P}(\mathbf{N})$ is countable. Then there is a one-to-one correspondence f between $\mathbf{N}$ and $\mathcal{P}(\mathbf{N})$.

We first define a binary relation

$$R = \{(i, j) \in \mathbf{N} \times \mathbf{N} \ : \ j \in f(i)\}.$$

The set R_i, as defined in the statement of the diagonalization principle, is equal to the set $f(i)$. In other words, each subset of $\mathbf{N}$ is equal to one of the sets R_i.

Now consider the diagonal set for R,

$$D = \{n \in \mathbf{N} \ : \ n \notin R_n\}.$$

By the diagonalization principle, the set D is distinct from each set R_i.

But D is a subset of $\mathbf{N}$, and since f is a one-to-one correspondence between $\mathbf{N}$ and $\mathcal{P}(\mathbf{N})$, we must have $D = R_k$ for some k.

In short, the assumption that $\mathcal{P}(\mathbf{N})$ is countable leads to a contradiction. Thus we have proved that $\mathcal{P}(\mathbf{N})$ is not countable. ∎