

Appendix: Countability

Often we want to know the *size* of a set. On the one hand, there are the finite sets. On the other hand, there are the infinite sets. The infinite sets are bigger than the finite sets.

There is more to it, of course. There is the 0-element set, the empty set. There are the 1-element sets, the singletons (like $\{8\}$). There are the 2-element sets, the doubletons (like $\{0, 8\}$). And so forth and so on. Finite sets come in all sizes.

Something similar happens with the infinite sets. All the infinite sets are big, but some are bigger than others. We want to make sense of this idea, by extending some concepts (that are familiar in the finite case) to infinite sets.

For sets A and B , say that A is the *same size* as B (written $A \approx B$) if there is a one-to-one correspondence between them, that is, if there is a one-to-one function f whose domain is A and whose range is B . (In this situation, f^{-1} is a one-to-one function whose domain is B and whose range is A . Hence B is also the same size as A , so the concept is symmetric.)

Applied to finite sets, this concept tells us nothing much that is new. For infinite sets, the situation is more interesting. The possibly surprising fact about infinite sets is that they are *not* all the same size.

One infinite set is the set $\mathbb{N} = \{0, 1, 2, \dots\}$ of all natural numbers. We can use natural numbers to give an exact characterization of finiteness: A set is finite iff there is a natural number n such that the set is the same size as $\{x \in \mathbb{N} \mid x < n\}$, that is, the same size as $\{0, 1, \dots, n-1\}$. (For the empty set, $n = 0$.)

Definition: A set is said to be *countable* if it the same size as some subset of \mathbb{N} . That is, a set S is countable if there is a one-to-one function $f : S \rightarrow \mathbb{N}$ mapping S into the natural numbers, so that $S \approx \text{ran } f$. Otherwise, the set is said to *uncountable*.

Thus for a set S to be countable, there must be a way to assign each member of S a unique natural number. For example, any finite set is countable, because it has the same size as $\{0, 1, \dots, n-1\}$, for some n . And \mathbb{N} itself is countable, as are each of its subsets.

Example: The set of all finite sequences of natural numbers is countable. In Chapter 2 we defined the bracket notation:

$$\begin{aligned} [] &= 1 \\ [x] &= 2^{x+1} \\ [x, y] &= 2^{x+1}3^{y+1} \\ [x, y, z] &= 2^{x+1}3^{y+1}5^{z+1} \\ \dots & \\ [x_0, x_1, \dots, x_k] &= 2^{x_0+1}3^{x_1+1} \dots p_k^{x_k+1} \end{aligned}$$

The function

$$\langle x_0, x_1, \dots, x_k \rangle \mapsto [x_0, x_1, \dots, x_k]$$

maps the set of sequences of natural numbers into \mathbb{N} , and it is one-to-one by the uniqueness of prime factorization.

Theorem: Any infinite countable set has the same size as \mathbb{N} .

Thus the countable sets consist of the finite sets,

$$\{s_0, s_1, \dots, s_{n-1}\}$$

plus the sets

$$\{s_0, s_1, \dots, \}$$

that are the same size as \mathbb{N} .

Proof. Assume that S is an infinite set that is countable, so that there is a one-to-one function $f : S \rightarrow \mathbb{N}$. We want a new function $g : S \rightarrow \mathbb{N}$ that is both one-to-one and *onto* \mathbb{N} . That is, we know that $\text{ran } f \subseteq \mathbb{N}$ and we want $\text{ran } g = \mathbb{N}$. The idea is push down $\text{ran } f$, to squeeze out all the holes.

First of all, $\text{ran } f$ contains some least member, say $f(s_0)$. (Because f is one-to-one, s_0 is unique.) We define $g(s_0) = 0$. More generally, for each n , there is a unique s_n in S for which $f(s_n)$ is the $(n + 1)$ st member of $\text{ran } f$. We define $g(s_n) = n$. This gives us the function g we want: $\text{dom } g = S$ and $\text{ran } g = \mathbb{N}$. \dashv

Theorem: (a) Any subset of a countable set is countable.

(b) The union of two countable sets is countable

(c) The Cartesian product of two countable sets is countable.

(d) If A is a countable set, then the set A^* of all finite sequences of members of A is countable.

(e) The union of countably many countable sets is countable.

Proof: The preceding example proves part (d) in the special case where $A = \mathbb{N}$. The argument can be adapted to cover any countable A .

As a special case of part (c), the set $\mathbb{N} \times \mathbb{N}$ is countable; we can map the ordered pair $\langle x, y \rangle$ to $2^{x+1}3^{y+1}$ as before. (And there are other possible “pairing functions,” as noted on page 214. For a start, we could use 2^x3^y , which is a bit simpler.)

Again, the argument can be adapted to cover the Cartesian product $A \times B$ of any countable sets A and B . Where f and g are one-to-one functions with $f : A \rightarrow \mathbb{N}$ and $g : B \rightarrow \mathbb{N}$, we can map the ordered pair $\langle a, b \rangle$ to $2^{f(a)}3^{g(b)}$.

Moreover, in this situation the union $A \cup B$ is countable. We can map x to $2f(x)$ whenever $x \in A$, and to $2g(x) + 1$ when $x \notin A$. Thus we get part (b).

Part (a) of the theorem is easy to see.

Part (e) means the following: Assume that \mathcal{A} is countable, and that each member of \mathcal{A} is a countable set (so in particular, \mathcal{A} is a set of sets). Then part (e) says that $\bigcup \mathcal{A}$, the result of dumping all the members of \mathcal{A} together, is countable.

We may suppose that \mathcal{A} is infinite (otherwise we can simply apply part (b) several times) so there is some function $f : \mathcal{A} \rightarrow \mathbb{N}$ that is both one-to-one and onto \mathbb{N} :

$$\mathcal{A} = \{f(0), f(1), \dots, f(n), \dots\}$$

For each n , the set $f(n)$ is countable, so there exists some function mapping it one-to-one into \mathbb{N} . We need to *choose* some such function g_n for each n . Then for each x in $\bigcup \mathcal{A}$, we take the smallest n for which $x \in f(n)$ and map x to the natural number $2^n 3^{g_n(x)}$. The map described in this way maps $\bigcup \mathcal{A}$ one-to-one into \mathbb{N} . \dashv

For example, the set \mathbb{Z} of all integers (positive, negative, and zero) is a countable set. And the set \mathbb{Q} of all rational numbers is countable. Part (d) tells us that over a countable alphabet A , the set A^* of all words is countable.

But not every set is countable. And by part (a) of the theorem, any set having an uncountable subset must be uncountable.

Cantor's theorem (1873): (a) The set \mathbb{R} of all real numbers is uncountable.

(b) The set $\mathcal{P}\mathbb{N}$ of all subsets of \mathbb{N} is uncountable.

(c) The set of all infinite binary sequences (i.e., the set of all functions from \mathbb{N} into $\{0, 1\}$) is uncountable.

(d) The set $\mathbb{N}^{\mathbb{N}}$ of all function from \mathbb{N} into \mathbb{N} is uncountable.

Proof: This theorem is proved by the classical "Cantor diagonal argument." To show that a set is uncountable, it suffices to show that each countable subset fails to exhaust the set.

For part (a), consider an arbitrary countable set of real numbers, for example:

$$\begin{aligned} s_0 &= 236.001\dots \\ s_1 &= -7.777\dots \\ s_2 &= 3.1415\dots \end{aligned}$$

To show that this list fails to exhaust \mathbb{R} , we need only produce one new real number z not on the list. Here is one: Its integer part is 0, and for each n , its $(n + 1)$ st decimal place is 7 unless the $(n + 1)$ st decimal place of s_n is 7, in which case the $(n + 1)$ st decimal place of z is 5. So in the example shown, $z = 0.757\dots$. Then z cannot have been on the list, because it differs from each s_n in its $(n + 1)$ st decimal place.

To prove part (b), consider an arbitrary countable subset

$$\{S_0, S_1, \dots\}$$

of $\mathcal{P}\mathbb{N}$. To show that this collection does not exhaust $\mathcal{P}\mathbb{N}$, we seek to come up with a new subset of \mathbb{N} . Here is one: $A = \{n \in \mathbb{N} \mid n \notin S_n\}$. This set could not equal S_{17} , because either

$$17 \in S_{17} \ \& \ 17 \notin A \quad \text{or} \quad 17 \notin S_{17} \ \& \ 17 \in A.$$

The set in part (c) has the same size as the set in part (b); simply pair up each subset of \mathbb{N} with its characteristic function. Or to prove part (c) directly, consider any countable set $\{s_0, s_1, \dots\}$ of infinite binary sequences. Then we can make a new binary sequence f by defining $f(n) = 1 \div s_n(n)$ for each n .

The set in part (d) is at least as big as the set in part (c). That is, the set in part (c) is a subset of the set in part (d). \dashv

A particularly relevant example for our purposes is the set \mathcal{S} of all register-machine programs. This set is countable. One way to see this fact is to represent \mathcal{S} as a set of finite sequences over a certain finite alphabet. But a more direct proof uses the function $\mathcal{P} \mapsto \# \mathcal{P}$ assigning to each program its Gödel number. This function maps \mathcal{S} one-to-one into \mathbb{N} .

Consequently, the set of all computable partial functions is countable. We can map each such function to the least Gödel number of a program that computes it.

The set of *all* partial functions (computable or not) is uncountable. By part (d) of the preceding theorem, even the set of total functions is uncountable. So the set of *non-computable* total functions is uncountable. That is, there are uncountably many non-computable functions.