Countable and Uncountable Sets

Let us now consider the intuitive notion of the number of elements in a set. At first there seems to be nothing complicated about the concept. Clearly, the number of elements in the set \{a, b, c\} is three, and the number of elements in \{x, y\} is two. But how many elements are in the set \(\mathbb{N}^+\)? The layperson would probably say "infinity," but for our purposes this is far too simplistic. Infinity is not a number in our normal counting system. Instead, the term infinity reflects the concept of a set having more elements than can be represented by any traditional number. Moreover, we are about to see that sets containing infinitely many elements, called infinite sets, do not all contain the same amount of elements. The sizes of two infinite sets can be different just as the sizes of two finite sets can be different. Thus, there are levels of infinity, with some infinite sets being larger than others.

Because there are no numbers in our traditional counting system to represent the size of an infinite set, it is necessary to extend our system to account for such sets. In this extended system we refer to the size of a set as its cardinality. The cardinality of a finite set corresponds to our traditional notion of the number of elements in the set, but the cardinality of an infinite set is not a number in the usual sense. Rather, the cardinality of an infinite set is a number, called a cardinal number, that exists only in our extended number system. We represent the cardinality of a set \(A\) by \(|A|\).

To complete our cardinality system we need to establish a way of comparing the cardinalities of different sets, that is, we need to define what it means for one cardinality to be less than another. To this end we agree to say the cardinality of the set \(X\) is less than or equal to the cardinality of the set \(Y\), written \(|X| \leq |Y|\), if and only if each element of \(X\) can be paired with a unique element of \(Y\). In other words, \(|X| \leq |Y|\) if and only if there is a one-to-one function mapping \(X\) into \(Y\). Note that if \(X\) and \(Y\) are finite sets, this definition of less than or equal to corresponds to the traditional definition: \(|X| \leq |Y|\) if and only if \(|X| \leq |Y|\) because \(x\) can be paired with the element \(r\) while \(y\) can be paired with \(s\).

Next we say the cardinality of the set \(X\) is equal to the cardinality of the set \(Y\), written \(|X| = |Y|\), if and only if there is a one-to-one function mapping \(X\) onto \(Y\). (The Schröder–Bernstein Theorem, whose details need not concern us, confirms that these definitions agree with our intuition. It states that if \(|X| \leq |Y|\) and if \(|Y| \leq |X|\), then \(|X| = |Y|\).) Note that \(|\mathbb{N}| = |\mathbb{N}^+|\), where a suitable one-to-one function is the function that associates each \(x\) in \(\mathbb{N}\) with the number \(x + 1\) in \(\mathbb{N}^+\). Finally, we define \(|X| < |Y|\) to mean \(|X| \leq |Y|\) and \(|X| \neq |Y|\).
In our discussion, the relationship between a set and its power set is extremely important. In the case of a finite set $X$, we have already shown that there are more elements in $\mathcal{P}(X)$ than in $X$. (In fact, if $X$ contains $n$ elements, then $\mathcal{P}(X)$ will contain $2^n$ elements.) The following theorem extends this relationship between a set and its power set to infinite sets.

**THEOREM 0.1**
If $X$ is any set, then $|X| < |\mathcal{P}(X)|$.

**PROOF**
Clearly, $|X| \leq |\mathcal{P}(X)|$ because the function mapping each element $x$ in $X$ to the set $\{x\}$ provides the required one-to-one function. (If $X$ is empty, then every element in $X$ can be mapped to an element in $\mathcal{P}(X)$ because there are no such elements in $X$.)

Our task, then, is to show that $|X| \neq |\mathcal{P}(X)|$. We can do this by showing that there is no function mapping $X$ onto $\mathcal{P}(X)$. Suppose $f$ is any function from $X$ to $\mathcal{P}(X)$ and consider the set $Y = \{x: x \in X$ and $x \notin f(x)\}$. Note that $Y$ is a subset of $X$ and therefore an element in $\mathcal{P}(X)$. Thus, if $f$ is onto $\mathcal{P}(X)$, there must be some $y$ in $X$ such that $f(y) = Y$.

If such a $y$ exists, however, then either $y \in f(y)$ or $y \notin f(y)$—both of which lead to contradictions. If $y \in f(y)$, then the definition of $Y$ would imply that $y \notin Y$, which contradicts our claim that $f(y) = Y$. Likewise, if $y \notin f(y)$, then the definition of $Y$ would imply that $y \in Y$, which also contradicts the assumption that $f(y) = Y$.

We conclude that there is no $y \in X$ such that $f(y) = Y$. Consequently, $f$ cannot be onto $\mathcal{P}(X)$ and hence $|X| < |\mathcal{P}(X)|$.

We are now in a position to support our claim that infinite sets can have different cardinalities. We need merely select any infinite set $X$ and compare its cardinality to that of its power set $\mathcal{P}(X)$. By Theorem 0.1, the cardinality of the latter must be greater than that of the former. In fact, the process of forming power sets leads to a hierarchy of infinite sets because the cardinality of $\mathcal{P}(\mathcal{P}(X))$ must be greater than the cardinality of $\mathcal{P}(X)$, and so forth.
That is,

\[ |X| < |\mathcal{P}(X)| < |\mathcal{P}(\mathcal{P}(X))| < \cdots \]

A consequence of this hierarchy is that there is no largest infinite cardinal. Given any infinite set, its power set will always be larger.

There is, however, a smallest infinite cardinal. It is the cardinality of \( \mathbb{N} \). This claim agrees with our intuitive feeling that if \( X \) is an infinite set then we should be able to extract elements one at a time without exhausting the set; that is, we could extract a “zero” element, then a “first” element, followed by a “second,” etc., and hence \( X \) must contain at least \( |\mathbb{N}| \) elements. However, this intuitive argument is based on a case-by-case approach which, as we agreed in our discussion of induction, fails to provide valid proof. Therefore, we present the following formal theorem and proof. It is based on the Axiom of Choice, which states that given any collection of nonempty sets there is a function \( g \) whose domain is the collection of sets, and for each set \( X \) in the collection, \( g(X) \in X \). That is, when given a set \( X \) from the collection as input, the function will return an element of \( X \) as its output.

**THEOREM 0.2**

The cardinality of the set of natural numbers is less than or equal to the cardinality of any infinite set.
PROOF
We must show that given any infinite set \( X \), there is a one-to-one function \( f \) from \( \mathbb{N} \) into \( X \). For this purpose we let \( g \) represent a function whose domain is the collection of nonempty subsets of \( X \), and for each nonempty subset \( Y \) of \( X \), \( g(Y) \) is an element of \( Y \). (The existence of such a function is based on the Axiom of Choice.) Based on this association between nonempty subsets of \( X \) and elements, we now define the function \( f \) by induction. We define \( f(0) \) to be \( g(X) \). Then, if \( n \) is a natural number for which \( f(n), f(n - 1), \ldots, f(0) \) have been defined, we define \( f(n + 1) \) to be the element \( g(X - \{f(0), f(1), \ldots, f(n)\}) \). Note that according to our definition of \( g \), \( f(n + 1) \) is chosen from the set \( X - \{f(0), f(1), \ldots, f(n)\} \), which is nonempty since \( X \) is infinite and \( \{f(0), f(1), \ldots, f(n)\} \) is finite. Therefore, \( f(n + 1) \) must be distinct from \( f(0), f(1), \ldots, f(n) \). Thus \( f \) is a one-to-one function from \( \mathbb{N} \) into the set \( X \). We conclude that the cardinality of the natural numbers is not greater than that of \( X \).

Theorem 0.2 shows that the set \( \mathbb{N} \) is one of the smallest infinite sets. We say it is one of the smallest because there are many sets of this same size (just as there are many sets of size three). For example, we have already seen that \( \mathbb{N}^+ \) is the same size as \( \mathbb{N} \).

Finally, we should introduce the concepts of countable and uncountable sets as promised earlier. Here it is helpful to recall the process we normally refer to as counting. To count the elements of a set means to assign the values 1, 2, 3, \ldots, to the set's elements. We may even pronounce the words "one, two, three, \ldots" as we point to the objects we are counting. In short, the counting process assigns positive integers to the elements of a set. We have seen, however, that there are infinite sets with more elements than there are positive integers. Thus, these sets cannot be counted, because there are not enough positive integers to go around. Such sets are said to
be uncountable. In contrast, any set whose cardinality is less than or equal to that of the positive integers is said to be countable (also enumerable). The set of natural numbers is countable; its power set is not. In fact, Theorems 0.1 and 0.2 combined imply that the power set of any infinite set is uncountable.

One way to show that an infinite set is countable is to demonstrate that there is a process for listing its elements as a sequence in such a way that each element in the set will ultimately appear in the list. Such a listing is a way of counting the elements: the first entry in the list is assigned one, the second is assigned two, the third is assigned three, etc.

As an example, let us show that the set $\mathbb{N}^+ \times \mathbb{N}^+$ is countable. We do this by describing a listing of all the elements in $\mathbb{N}^+ \times \mathbb{N}^+$. This list consists of all the pairs whose components add to two, followed by pairs whose components add to three, followed by those pairs whose components add to four, etc. We arrange the pairs within each of these groupings in the order corresponding to their first components. Thus, the list has the form $((1, 1), (1, 2), (2, 1), (1, 3), (2, 2), (3, 1), \ldots)$. (See Figure 0.3.) Note that this list will ultimately contain each element of $\mathbb{N}^+ \times \mathbb{N}^+$. (The pair $(m, n)$ will appear as the $m^n$th entry in the portion of the list that contains the pairs whose components add to $m + n$.) Finally, we observe that this listing is actually a counting of the elements of $\mathbb{N}^+ \times \mathbb{N}^+$—we have assigned one to $(1, 1)$, two to $(1, 2)$, three to $(2, 1)$, etc. Consequently, we can conclude that $\mathbb{N}^+ \times \mathbb{N}^+$ is countable.

![Diagram](image)

**Figure 0.3** Listing the elements of $\mathbb{N}^+ \times \mathbb{N}^+$ in a sequence

pairs that add to 2

pairs that add to 3

pairs that add to 4

pairs that add to 5

(1, 1), (1, 2), (2, 1), (1, 3), (2, 2), (3, 1), (1, 4), (2, 3), \ldots
So What?

Let us close this section by relating our discussion to a typical computing environment. Suppose we have a program ready to run on an actual computer. The program is designed to accept some input (perhaps a list of names to be sorted) and produce some output (such as the sorted list). Regardless of what the input and output are, each is merely a string of bits from the machine's point of view. Thus, we can consider the input and output as natural numbers represented in binary notation. (We can imagine an additional 1 placed at the leftmost end of these bit strings so that any leading 0s in the original strings will be significant.) From this perspective, the program accepts an input number and, based on the value of that number, produces an output number. That is, the action of the program is to compute a function from $\mathbb{N}$ to $\mathbb{N}$. In turn, each function from $\mathbb{N}$ to $\mathbb{N}$ suggests a program we may at some time wish to write.

How many such functions are there? Clearly there are no more functions from $\mathbb{N}$ to $\{0, 1\}$ than there are functions from $\mathbb{N}$ to $\mathbb{N}$, since the latter provides more potential output values. But there are as many functions from $\mathbb{N}$ to $\{0, 1\}$ as there are elements in the power set of $\mathbb{N}$. Indeed, for each subset $X$ of $\mathbb{N}$ there is a function $f$, called the characteristic function of $X$, from $\mathbb{N}$ to $\{0, 1\}$ defined by

$$f(n) = \begin{cases} 1 & \text{if } n \in X \\ 0 & \text{if } n \notin X \end{cases}$$

We conclude that there are at least as many functions from $\mathbb{N}$ to $\mathbb{N}$ as there are elements of $\mathcal{P}(\mathbb{N})$. Thus, there are uncountably many functions for which we may want to write programs.
Now, consider your favorite programming language. There are a finite number of symbols from which any program in that language is constructed. Let us establish an "alphabetical" order for these symbols. Then, we could list all programs in the language that have a length of one symbol (if there are any) in alphabetical order; following this we could list all the programs of length two in alphabetical order; then, all programs of length three in alphabetical order; etc. Such a listing would ultimately contain any program that could be written in the language. Thus, this listing procedure implies that the set of all programs that can be written in the language is countable.

What have we shown? There are only countably many programs that can be written in your favorite programming language, but there are uncountably many functions that you may want to compute with a program. Because each program computes only one function, you are bound to come up short. Thus, there are problems you might want to solve using a computer, but for which no program in your favorite programming language can be written!

What are some of these problems? Could you solve such a problem by changing to a different programming language? Could such problems be solved if we built a bigger computer? Even if you are able to produce a program for solving a problem, will today's machine be able to execute it fast enough to produce an answer in your lifetime? Would tomorrow's computer be able to produce an answer in your children's lifetime? These are some of the questions addressed directly or indirectly in the following chapters.