Countable and Uncountable Sets

In this section we extend the idea of the "size" of a set to infinite sets. It may come as somewhat of a surprise that there are different "sizes" of infinite sets. At the end of this section we show that there are infinitely many different such "sizes". For the most part we focus on a classification of sets into two categories: the sets whose elements can be listed (countable sets) and those for which there is no list containing all of the elements of the set (uncountable sets).

Definition (sets can be put into 1-1 correspondence). Let A and B be sets and $f : A \to B$ be a 1-1 correspondence. Then, by Propositions F12 and F13 in the Functions section, f is invertible and f^{-1} is a 1-1 correspondence from B to A. Because of the symmety of this situation, we say that *A and B can be put into 1-1 correspondence*.

It is easy to see that any two finite sets with the same number of elements can be put into 1-1 correspondence. Conversely, if A and B are finite sets that can be put into 1-1 correspondence, then we know from Corollary F6 in the section on Functions that A and B have the same number of elements.

Definition (two sets have the same cardinality, cardinality n). We say that two sets A and B *have the same cardinality* (or size), and write $|A| = |B|$, if they can be put into 1-1 correspondence. We say that a set A has *cardinality* n, and write $|A| = n$, if there exists a natural number n such that A can be put into 1-1 correspondence with $\{1, 2, \ldots, n\}$.

The cardinality of a finite set is just the number of elements it contains (by Corollary F6), so the definition agrees with previous use of the notation $|A|$. (Notice that $\{1, 2, \ldots, n\}$ is empty when $n = 0$.)

Notice that the above definition opens the door to talking about infinite sets having the same cardinality (when they can be put into 1-1 correspondence), or not (when they can't). Thus, the definition allows for the possiblity that not all infinite sets have the same cardinality. This turns out to be true, but it will take some time before we have developed enough results and techniques to demonstrate it.

Example (infinite sets having the same cardinality). Let $S = \{n^2 : n \in \mathbf{Z}^+\}$. The function $f : \mathbf{Z}^+ \to S$ defined by $f(n) = n^2$ is a 1-1 correspondence. (**Exercise**: prove it.) Therefore, $|S| = |\mathbf{Z}^+|$. Thus the set S of squares of positive integers is the same "size" as the set $\mathbf{Z}^+$ of positive integers. This may seem confusing since $S \subset \mathbf{Z}^+$. Such a situation can not arise for finite sets, it is a consequence of the sets being infinite. One definition of an infinite set is a set which can be put into 1-1 correspondence with a proper subset of itself. For aother example the formula $f(n) = n + 1$ is a 1-1 correspondence from $\mathbf{N}$ to $\mathbf{Z}^+$. (This implies $|\mathbf{N}| = |\mathbf{Z}^+|$.)

Exercise. Prove that $|\mathbf{Z}| = |\mathbf{Z}^+| = |E|$, where $E = \{0, 2, 4, 6, \ldots\}$ is the set of even positive integers. Hint: one way to do this is for the function $f : \mathbf{Z}^+ \to \mathbf{Z}$ to be defined according to two cases – the even positive integers map to the non-negative integers, and the odd positive integers map to the negative integers.

Example (infinite sets having the same cardinality). Let $f : (0,1) \to (1,\infty)$ be defined by $f(x) = 1/x$. Then f is a 1-1 correspondence. (**Exercise**: prove it.) Therefore, $|(0,1)| = |(1,\infty)|$.

Exercise. Show that $|(0,\infty)| = |(1,\infty)| = |(0,1)|$. Use this result and the fact that $(0,\infty) = (0,1) \cup \{1\} \cup (1,\infty)$ to show that $|(0,1)| = |\mathbf{R}|$.

Definition (countably infinite set, countable set, uncountable set). A set A is called *countably infinite* if it can be put into 1-1 correspondence with $\mathbf{Z}^+$. A set is called *countable* if it is finite or countably infinite. A set which is not countable is called *uncountable*.

By what has been shown – or at least indicated – above, the sets $S, E, \mathbf{N}$, and $\mathbf{Z}$ are all countably infinite, and therefore countable. A set is countable if it is finite, or it has the same cardinality as Z^+. Since a composition of 1-1 correspondences is also a 1-1 correspondence, any set that can be put into 1-1 correspondence with a countable set is itself countable. That is, to prove that a set os countable it is enough to show that it can be put into 1-1 correspondence with any set that is known to be countable (so sets like $E, S, \mathbf{N}$ and $\mathbf{Z}$ can be used in place of $\mathbf{Z}^+$, so long as the above proviso about compositions is quoted). It is a good **exercise** to write down a formal proof of what has just been discussed: *if A is a countably infinite set and there is a 1-1 correspondence $f : A \to B$, then B is countably infinite.*

Proposition CS1: Any subset of $\mathbf{Z}^+$ is countable.

Proof.

Let $X \subseteq \mathbf{Z}^+$. If X is finite, then it is countable. Suppose that X is infinite. Define $f : \mathbf{Z}^+ \to X$ by $f(n)$ is the smallest element in $X - \{f(1), f(2) \ldots, f(n-1)\}$ (i.e. $f(n)$ is the n-th smallest element in X). To see that f is 1-1, observe that if $i < j$ then $f(j)$ is the smallest element in a set that does not contain $f(i)$; thus $f(i) \neq f(j)$. To see that f is onto, note that the positive integer k is larger than at most $k-1$ elements of X, hence if $k \in X$ then one of $f(1), f(2), \ldots, f(k)$ equals k. The function f is therefore a 1-1 correspondence, and X is countable. ∎

Our next goal is to show that a set is countable if and only if there is a sequence in which every element of the set appears (at least once). Once we have proved this statement to be true, in order to prove a set is countable it will suffice to display such a list. This is usually less cumbersome than working directly with 1-1 and onto functions, even though it is what's happening in the background.

Definition (sequence). An *infinite sequence* of elements of a set X is a function $f : \mathbf{Z}^+ \to X$. The images of the positive integers are usually displayed in list format: $f(1), f(2), f(3), \ldots$. Sometimes we write f_i instead of $f(i)$, so that the list becomes $f_1, f_2, f_3 \ldots$.

Notice that, conversely, if there is an infinite sequence $x_1, x_2, x_3 \ldots$ of elements of the set X, then then a function $f : \mathbf{Z}^+ \to A$ is obtained by defining $f(i) = x_i,\ i = 1, 2, \ldots$. Therefore, infinite sequences and functions whose domain is $\mathbf{Z}^+$ are really the same thing.

Exercise. Formulate a precise definition of a finite sequence.

A countably infinite set is one that can be put into 1-1 correspondence with $\mathbf{Z}^+$. By the definitions of infinite sequence and 1-1 correspondence, **a set X is countably infinite if there is an infinite sequence (function $f : \mathbf{Z}^+ \to X$) in which every element of X appears exactly once** (1-1 and onto function). After doing some examples, we will show that the condition *every element of X appears exactly once* can be replaced by *every element of X appears* (at least once), which is easier to use.

Example (proving countable using sequences). The infinite sequence $1, -1, 3, -3, 5, -5, \ldots$ contains every odd integer exactly once (the positive odd integer $2k+1$ appears in position $2k+1$ and the negative odd integer -(2k+1) appears in position $2k$). Thus, the set of odd integers is countable.

Exercise. Prove that the set of multiples of three (positive, negative and zero) is countable.

Example (proving countable using sequences). We show that the set of all finite binary sequences is countable. Let ϵ denote the empty sequence (the sequence with no terms). Then, the infinite sequence $\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots$ in which the binary sequences of length 0 are listed, then the binary sequences of length 1 are listed in increasing numeric order, then the binary sequences of length 2 are listed in increasing numeric order, and so on, contains every finite binary sequence exactly once.

Definition (subsequence). An *subsequence* of an infinite sequence $f : \mathbf{Z}^+ \to X$ of elements of the set X is a restriction of f to a subset of $\mathbf{Z}^+$.

You can imagine a subsequence as being formed by crossing out some (possibly infinitely many) elements of an infinite sequence. Note that there is no requirement in the definition of subsequence that the restriction be to an infinite subset of $\mathbf{Z}^+$. Thus, a subsequence of an infinite sequence might be finite. By Proposition CS1, an infinite subsequence is itself an infinite sequence (the domain of the restriction can be put into 1-1 correspondence with $\mathbf{Z}^+$, so function composition gives a function with domain $\mathbf{Z}^+$ and range the set of elements in the infinite subsequence).

Example (subsequence). Consider the infinite sequence $1, 2, 3, 4, 5, \ldots$. (The function is $f(n) = n$ with domain and codomain equal to $\mathbf{Z}^+$.) One subsequence is $2, 4, 8, 16, \ldots$. It is obtained by restricting f to $\{2^k : k = 1, 2, \ldots\}$. Another subsequence is $2, 3, 5, 7, 11, 13, \ldots$. It is obtained by restricting f to the prime numbers. A third subsequence is $1, 4, 9, 12$. it is obtained by restricting f to $\{1, 4, 9, 12\}$.

Theorem CS2. A set X is countable if and only if there is an infinite sequence in which every element of X appears at least once.

Proof.

($\Rightarrow$) Let X be a countable set. If X is finite, say $X = \{x_1, x_2, \ldots, x_n\}$, then such a sequence is $x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n, \ldots$. Suppose that X is infinite. Then, since X is countably infinite, there is an infinite sequence in which every element appears exactly once. Every element of X appears at least once in this sequence.

($\Leftarrow$) Suppose there is an infinite sequence $f_1, f_2, \ldots$ in which every element of X appears at least once. If X is finite, it is countable. Suppose that X is infinite. We construct an infinite subsequence in which every element of X appears exactly once. For each $x \in X$, let i_x be the smallest subscript for which $f_{i_x} = x$. Let $I = \{i_x : x \in X\}$. The restriction of f to I is the desired subsequence. ∎

The subsequence in the above proof can be viewed as having been constructed from $f_1, f_2, \ldots$ by, for each element x, crossing out all occurances of x after the first one.

Example (Theorem CS2). The sequence $1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5 \ldots$, call it f, contains every element of $\mathbf{Z}^+$. (It contains the positive integer n exactly n times.) The subsequence in the proof of the theorem is $1, 2, 3, \ldots$. It is obtained by restricting f to $\{1, 2, 4, 7, \ldots\} = \{1 + \binom{n+1}{2} : n \geq 0\}$ (note that elements of this set are the positions in the sequence where an element occurs for the first time).

Example (proving countable using Theorem CS2). The set E^* of positive even integers is countable since its elements can be listed as $2, -2, 4, -4, 6, -6, \ldots$. The set T^* of positive multiples of three is countable since its elements can be listed as $3, -3, 6, -6, \ldots$. To see that $E^* \cup T^*$ is countable, form an infinite sequence containing every element of $E^* \cup T^*$ by choosing elements alternately from each list: $2, 3, -2, -3, 4, 6, -4, -6, 6, 9, -6, -9, \ldots$.

Exercise. Prove that if A and B be countably infinite sets, then $A \cup B$ is countably infinite.

The idea of forming a subsequence by selecting special elements of a sequence can be used to prove the following proposition and corollary.

Proposition CS3. Any subset of a countable set is countable.

Proof.

Exercise. ∎

Corollary CS4. Any subset of $\mathbf{Z}$ is countable.

Proof.

Exercise. ∎

Note that there is a small but important difference between Theorem CS5 below and the exercise above Proposition CS3. The theorem applies when one or both of the sets are finite.

Theorem CS5. If A and B are countable sets, then $A \cup B$ is a countable set.

Proof.

If A and B are both finite, then so is $A \cup B$, and any finite set is countable.

Suppose A is finite and B is countably infinite. Then there are sequences $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots$ that contain every element of these sets, respectively. Thus, $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots$ is an infinite sequence that contains every element of $A \cup B$, so $A \cup B$ is countable.

Similarly, if B is finite and A is countably infinite then $A \cup B$ is countable.

Finally, suppose that A and B are both countably infinite. Then there are infinite sequences $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ that contain every element of these sets, respectively. Thus, $a_1, b_1, a_2, b_2, \ldots$ is an infinite sequence that contains every element of $A \cup B$, so $A \cup B$ is countable. ∎

The idea of the proof of Theorem CS5 can be used together with mathematical induction to prove that:

for $n \geq 2$, if $A_1, A_2, \ldots, A_n$ are countable sets, then so is $A_1 \cup A_2 \cup \cdots \cup A_n$.

In the induction step, note that $A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1} = A_1 \cup A_2 \cup \cdots \cup (A_n \cup A_{n+1})$, then use Theorem CS5 and the induction hypothesis.

A stronger result than the above generalization of Theorem CS5 is true. It turns out that the union of countably many countable sets is itself a countable set.

Theorem CS6. If $A_1, A_2, \ldots$ is a collection of countably many countably infinite sets, then $\bigcup_{i=1}^{\infty} A_i$ is also a countable set.

Proof.

By the above, we may assume that the collection contains countably infinitely many sets. For each positive integer i there is an infinite sequence $a_{i,1}, a_{i,2}, \ldots$ that contains every element of A_i at least once. Then $a_{1,1}, a_{1,2}, a_{2,1}, a_{1,3}, a_{2,2}, a_{3,1}, a_{1,4}a_{2,3}, \ldots$ is an infinite sequence that contains every element of $\bigcup_{i=1}^{\infty} A_i$ at least once. (The elements $a_{i,j}$ are listed in non-decreasing order of $i+j$, and if $i+j = r+s$ then $a_{i,j}$ is listed before $a_{r,s}$ if and only if $i < r$.) By Theorem CS2, $\bigcup_{i=1}^{\infty} A_i$ is countable. ∎.

The technique used in the above proof is called *diagonal sweeping*, since it corresponds to writing the sequences in a 2-dimensional array and then consructing the sequence by sweeping down consecutive back diagonals starting from the top left corner. Exactly the same argument can be used to prove the following without using Theorem CS6.

Example (Q is countable). For each positive integer i, let A_i be the set of rational numbers with denominator equal to i. Then, every element of A_i occurs in the sequence $\{a_{i,j}\}_{j=1}^{\infty} = 0/i, 1/i, -1/i, 2/i, -2/i, \ldots$. Thus, A_i is countable. Since $\mathbf{Q} = \bigcup_{i=1}^{\infty} A_i$, the set $\mathbf{Q}$ of rational numbers is countable by Theorem CS6.

Exercise. Prove that $\mathbf{Z}^+ \times \mathbf{Z}^+$ is countable.

The uncountable sets are the infinite sets which can not be put into 1-1 correspondence with the positive integers. By Theorem CS5, this is the same as saying that they are the sets for which there is no sequence $x_1, x_2, \ldots$ that containing every element of the set at least once. We will prove later that the real numbers is an example of such a set. The main idea of the proof is to assume that such a squence exists and derive a contradiction by "finding" an element which does not appear in the sequence. The existence of uncountable sets means that not all infinite sets have the same cardinality.

Proposition CS7. The set S of all infinite binary sequences is uncountable.

Proof.

The proof is by contradiction. Suppose that S is countable. Since S is clearly not a finite set, this means that there is an infinite sequence $f_1, f_2, \ldots$ that contains every element of S at least once. We will obtain a contradiction by exhibiting an element τ of S that, by its definition, can not be f_n for any positive integer n. For each positive integer i, let f_i be the infinite binary sequence $b_{i,1}, b_{i,2}, \ldots$. The infinite binary sequence $\tau = t_1, t_2, t_3, \ldots$ is defined by $t_i = 1 - b_{i,i}$, for $i = 1, 2, \ldots$.

We claim that τ can not be f_n for any positive integer n. For every positive integer n, the n-th element of the sequence τ is (defined so that it is) different from $b_{n,n}$, the n-th element of f_n. This establishes the contradiction mentioned above, and therefore there can not be an infinite sequence $f_1, f_2, \dots$ that contains every element of S at least once. Hence, S is uncountable. ∎

The technique used in the proof of proposition CS7 is known as "Cantor Diagonalization" because the sequence τ arises from changing the "diagonal elements" $b_{i,i}$.

The technique of Cantor Diagonalization can also be used to prove that the set of real numbers is uncountable. Before we do this, we need to review a concept. Every real number has an infinite decimal expansion. Most real numbers have only one of these, but some have two. Any number with a finite decimal expansion has one infinite decimal expansion that ends in an infinite sequence of zeros and a second infinite decimal expansion that ends in an infinite sequence of nines. For example, $3.2700000\ldots = 3.269999\ldots$. These are the only numbers with more than one infinite decimal expansion. We will need to make use of this in our proof.

Theorem CS8. The set $\mathbf{R}$ of real numbers is uncountable.

Proof.

The set $\mathbf{R}$ is clearly infinite. Suppose it is countable. Then, there exists an infinite sequence $f_1, f_2, \dots$ that contains every element of $\mathbf{R}$. We obtain a contradiction by finding $x \in \mathbf{R}$ such that x is not f_n for any positive integer n.

For each positive integer i, suppose that the part of the decimal expansion of f_i following the decimal point is $.d_{i,1}d_{i,2}d_{i,3}\ldots$, where each $d_{i,j}$ is one of $0, 1, \dots, 9$. The real number $x = 0.x_1x_2x_3\ldots$ is defined by

$$x_i = \begin{cases} 5 & \text{if } d_{i,i} \neq 5 \\ 6 & \text{if } d_{i,i} = 5 \end{cases}$$

for each positive integer i.

We claim that x can not be f_n for any positive integer n. First of all, x differs from f_n in the the n-th digit after the decimal point (i.e., $x_i \neq d_{i,i}$). And, secondly, x is a number with only one infinite decimal expansion so it can not simply be a second representation of a number that is f_n for some n. This proves the claim, and contradicts the existence of the sequence $f_1, f_2, \dots$

Therefore, $\mathbf{R}$ is uncountable. ∎

Since the real numbers are uncountable and the rational numbers are countable, it follows that irrational numbers exist. It is not difficulty to show (but you don't have to do it) that $n^{1/k}$ is irrational unless n is the k-th power of some integer. In particular, $\sqrt{2}$ is irrational. A slightly more advanced argument can be used to show that e, the base of the natural logarithms, is irrational, and a much more complicated argument is required to show that π is irrational. So far we have described only countably many irrational numbers. But the set of irrational numbers must be uncountable because otherwise $\mathbf{R}$ would be the union of two countable sets, and would therefore be countable.

It is unknown whether there is a set whose cardinality lies "between" $|\mathbf{Z}^+|$ and $|\mathbf{R}|$. This is known as *the continuum hypothesis*, partly because the cardinality of the real numbers is sometimes called the continuum. The continuum hypothesis is known to be beyond proof in our system of logic.

Since $\mathbf{Z}^+ \subseteq \mathbf{R}$, we would be justified in writing $|\mathbf{Z}^+| < |\mathbf{R}|$. However, you should not believe that the continuum is the largest possible cardinality of an infinite set. There is an infinite heirarchy of cardinalities of infinite sets because of the following fact. Note that, since the set A in the statement may not be countable, we must use the definition of two sets having the same cardinality rather than the methods we have used in dealing with countable sets.

Theorem CS9. For any set A, $|A| < |\mathcal{P}(A)|$.

Proof.

First of all, $|A| \leq |\mathcal{P}(A)|$, since A can clearly be put into 1-1 correspondence with the subset of $\mathcal{P}(A)$ consisting of the singleton subsets, $\{\{x\} : x \in A\}$.

Suppose $|A| = |\mathcal{P}(A)|$. Then there is a 1-1 correpsondence $f : A \to \mathcal{P}(A)$. We obtain a contradiction to the fact that f is onto by exhibiting a subset X of A such that $X \neq f(a)$ for any $a \in A$.

For every $a \in A$, either $a \in f(a)$, or $a \notin f(a)$. The definition of X is slippery: let $X = \{a \in A : a \notin f(a)\}$.

Consider $a \in A$. If $a \in f(a)$ then $a \notin X$ (by definition of X), so $f(a) \neq X$. On the other hand, if $a \notin f(a)$ then $a \in X$ (by definition of X), so $f(a) \neq X$. Therefore, $X \neq f(a)$ for any $a \in A$, a contradiction. Hence, $|A| < |\mathcal{P}(A)|$. ∎

By Theorem CS9, $|\mathbf{R}| < |\mathcal{P}(\mathbf{R})| < |\mathcal{P}(\mathcal{P}(\mathbf{R}))| < \cdots$.

Exercises. For practice problems you should do Exercises A-3, page A-34, 1-6, and 8 (Grimaldi, 4th ed.). All of these can be done using the techniques and results described here. Answers to the odd numbered exercises are in the text.

Solutions to even numbered problems in Grimaldi, 4th ed.

2. (a) $f(n) = n^2$.   (b) $f(n) = 4n - 2$.

4. The set I is uncountable. If I were countable then $\mathbf{R}$ would be the union of two countable sets and therefore countable, a contradiction.

6. There is an infinite sequence in which each element of $\mathbf{Z}^+ \times \mathbf{Z}^+ \times \mathbf{Z}^+$ appears exactly once: $(1,1,1), (1,1,2), (1,2,1), (2,1,1), (1,1,3), \ldots$. The elements are ordered by non-decreasing sum of the components. The elements whose components have the same sum appear in dictionary order.

8. (a) $f(x) = 3x$.   (b) $f(x) = 5x + 2$.   (c) $f(x) = (b - a)x + a$

More Problems

9. Let Σ be a finite set. Show that the set of all sequences of elements of Σ of finite length is countable.

10. Is the set $\mathbf{Q} - \mathbf{N}$ countable or uncountable? Why? What about $\mathbf{R} - \mathbf{Z}$?

11. Argue that the set of all computer programs is a countable set, but the set of all functions is an uncountable set. (Since each program computes a function, this means there must be things it isn't possible to write a program to do.)

12. Let X be an uncountable set. Prove that if there is a 1-1 correspondence $f : A \to X$, then A is uncountable.

13. Let C be a countable subset of an uncountable set X. Is $X - C$ countable or uncountable? Why?