CS 70 Discrete Mathematics for CS
Spring 2008 David Wagner

Note 23

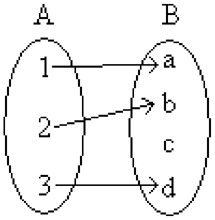
Infinity and Countability

Consider a function (or mapping) f that maps elements of a set A (called the *domain* of f) to elements of set B (called the *range* of f). For each element $x \in A$ ("input"), f must specify one element $f(x) \in B$ ("output"). Recall that we write this as $f : A \to B$. We say that f is a *bijection* if every element $a \in A$ has a unique *image* $b = f(a) \in B$, and every element $b \in B$ has a unique *pre-image* $a \in A$ such that $f(a) = b$.

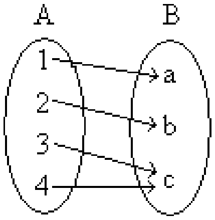
f is a *one-to-one function* (or an *injection*) if f maps distinct inputs to distinct outputs. More rigorously, f is one-to-one if the following holds: $\forall x,y \,.\, x \neq y \Rightarrow f(x) \neq f(y)$.

The next property we are interested in is functions that are *onto* (or *surjective*). A function that is onto essentially "hits" every element in the range (i.e., each element in the range has at least one pre-image). More precisely, a function f is onto if the following holds: $\forall y\ \exists x \,.\, f(x) = y$. Here are some examples to help visualize one-to-one and onto functions:

One-to-one



Onto



Note that according to our definition a function is a bijection iff it is both one-to-one and onto.

Cardinality

How can we determine whether two sets have the same *cardinality* (or "size")? The answer to this question, reassuringly, lies in early grade school memories: by demonstrating a *pairing* between elements of the two sets. More formally, we need to demonstrate a *bijection* f between the two sets. The bijection sets up a one-to-one correspondence, or pairing, between elements of the two sets. We know how this works for finite sets. In this lecture, we will see what it tells us about *infinite* sets.

Are there more natural numbers $\mathbb{N}$ than there are positive integers $\mathbb{Z}^+$? It is tempting to answer yes, since every positive integer is also a natural number, but the natural numbers have one extra element $0 \notin \mathbb{Z}^+$. Upon more careful observation, though, we see that we can generate a mapping between the natural numbers and the positive integers as follows:

$$\begin{array}{lcccccccc}
\mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & \dots & \\
\downarrow & \searrow & \searrow & \searrow & \searrow & \searrow & \searrow & & \\
\mathbb{Z}^+ & & 1 & 2 & 3 & 4 & 5 & 6 & \dots
\end{array}$$

Why is this mapping a bijection? Clearly, the function $f : \mathbb{N} \to \mathbb{Z}^+$ is onto because every positive integer is hit. And it is also one-to-one because no two natural numbers have the same image. (The image of n is $f(n) = n+1$, so if $f(n) = f(m)$ then we must have $n = m$.) Since we have shown a bijection between $\mathbb{N}$ and $\mathbb{Z}^+$, this tells us that there are as many natural numbers as there are positive integers! Informally, we have proved that "$\infty + 1 = \infty$."

What about the set of *even* natural numbers $2\mathbb{N} = \{0, 2, 4, 6, ...\}$? In the previous example the difference was just one element. But in this example, there seem to be twice as many natural numbers as there are even natural numbers. Surely, the cardinality of $\mathbb{N}$ must be larger than that of $2\mathbb{N}$ since $\mathbb{N}$ contains all of the odd natural numbers as well. Though it might seem to be a more difficult task, let us attempt to find a bijection between the two sets using the following mapping:

$$\begin{array}{llllllll} \mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 2\mathbb{N} & 0 & 2 & 4 & 6 & 8 & 10 & \dots \end{array}$$

The mapping in this example is also a bijection. f is clearly one-to-one, since distinct natural numbers get mapped to distinct even natural numbers (because $f(n) = 2n$). f is also onto, since every n in the range is hit: its pre-image is $\frac{n}{2}$. Since we have found a bijection between these two sets, this tells us that in fact $\mathbb{N}$ and $2\mathbb{N}$ have the same cardinality!

What about the set of all integers, $\mathbb{Z}$? At first glance, it may seem obvious that the set of integers is larger than the set of natural numbers, since it includes negative numbers. However, as it turns out, it is possible to find a bijection between the two sets, meaning that the two sets have the same size! Consider the following mapping:

$0 \to 0$, $1 \to -1$, $2 \to 1$, $3 \to -2$, $4 \to 2$, $\dots$, $124 \to 62$, $\dots$

In other words, our function is defined as follows:

$$f(x) = \begin{cases} \frac{x}{2}, & \text{if } x \text{ is even} \\ \frac{-(x+1)}{2}, & \text{if } x \text{ is odd.} \end{cases}$$

We will prove that this function $f : \mathbb{N} \to \mathbb{Z}$ is a bijection, by first showing that it is one-to-one and then showing that it is onto.

Proof (one-to-one): Suppose $f(x) = f(y)$. Then they both must have the same sign. Therefore either $f(x) = \frac{x}{2}$ and $f(y) = \frac{y}{2}$, or $f(x) = \frac{-(x+1)}{2}$ and $f(y) = \frac{-(y+1)}{2}$. In the first case, $f(x) = f(y) \Rightarrow \frac{x}{2} = \frac{y}{2} \Rightarrow x = y$. Hence $x = y$. In the second case, $f(x) = f(y) \Rightarrow \frac{-(x+1)}{2} = \frac{-(y+1)}{2} \Rightarrow x = y$. In both cases $f(x) = f(y) \Rightarrow x = y$, so taking the contrapositive, f must be one-to-one.

Proof (onto): If $y \in \mathbb{Z}$ is positive, then $f(2y) = y$, and $2y \geq 0$. Therefore, y has a pre-image in $\mathbb{N}$. If y is negative, then $f(-(2y+1)) = y$, and $-(2y+1) \geq 0$. Therefore, y has a pre-image in $\mathbb{N}$ in this case, too. Thus every $y \in \mathbb{Z}$ has a pre-image, so f is onto.

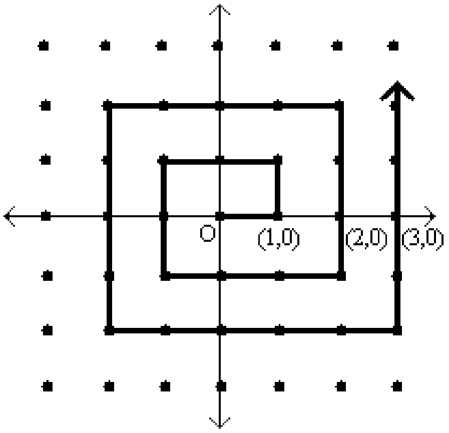
Since f is a bijection, this tells us that $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality.

Now for an important definition. We say that a set S is **countable** if there is a bijection between S and $\mathbb{N}$ or some subset of $\mathbb{N}$. Thus any finite set S is countable (since there is a bijection between S and the subset $\{0, 1, 2, \dots, m-1\}$, where $m = |S|$ is the size of S). And we have already seen three examples of countable infinite sets: $\mathbb{Z}^+$ and $2\mathbb{N}$ are obviously countable since they are themselves subsets of $\mathbb{N}$; and $\mathbb{Z}$ is countable because we have just seen a bijection between it and $\mathbb{N}$.

What about the set of all rational numbers? Recall that $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{Z},\, y \neq 0\}$. Surely there are more rational numbers than natural numbers? After all, there are infinitely many rational numbers between any two natural numbers. Surprisingly, the two sets have the same cardinality! To see this, let us introduce another way of comparing the cardinality of two sets:

If there is a one-to-one function $f : A \to B$, then the cardinality of A is less than or equal to that of B. Now to show that the cardinality of A and B are the same we can show that $|A| \leq |B|$ and $|B| \leq |A|$. This corresponds to showing that there is a one-to-one function $f : A \to B$ and a one-to-one function $g : B \to A$. The existence of these two one-to-one functions implies that there is a bijection $h : A \to B$, thus showing that A and B have the same cardinality. The proof of this fact, which is called the Cantor-Bernstein theorem, is actually quite hard, and we will skip it here.

Back to comparing the natural numbers and the integers. First it is obvious that $|\mathbb{N}| \leq |\mathbb{Q}|$ because $\mathbb{N} \subseteq \mathbb{Q}$. So our goal now is to prove that also $|\mathbb{Q}| \leq |\mathbb{N}|$. To do this, we must exhibit a one-to-one function $f : \mathbb{Q} \to \mathbb{N}$. The following picture of a spiral conveys the idea of this function:



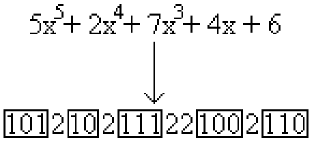
Each rational number $\frac{a}{b}$ can be represented by the point (a,b) on the grid. We can map every $\frac{a}{b}$ to the distance of the point (a,b) along this spiral starting at the origin (e.g., $(0,0) \mapsto 0$, $(1,0) \mapsto 1$, $(1,1) \mapsto 2$, $\ldots$). Why is this mapping one-to-one? We have to be extremely careful, since $f : \mathbb{Q} \to \mathbb{N}$ is not onto (think of all the points along the x-axis, which correspond to a division by zero). However, every rational number has an image, and f is a one-to-one mapping from the set of rational numbers in lowest terms to a subset of $\mathbb{N}$ (i.e., distinct rational numbers in lowest terms get mapped to distinct natural numbers, since no two rationals can have the same distance along the spiral). This tells us that $|\mathbb{Q}| \leq |\mathbb{N}|$. Since also $|\mathbb{N}| \leq |\mathbb{Q}|$, as we observed earlier, it must be the case that $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality.

Next, let us consider the set $\{0,1\}^*$ of all binary strings. In other words, each element of $\{0,1\}^*$ is some (finite) sequence of bits. This set is also countable, because it can be put into a one-to-one correspondence with $\mathbb{N}$. The basic idea is to associate the number n with its binary (base-2) representation.[1] So, the set of all bit strings is also countable.

Is the set of all polynomials with natural number coefficients countable? Remarkably, we will show that this set is also countable, even when the degree of the polynomials is not bounded. To see this, let us make a few observations about numeral systems in different bases. As an example, if we are working with ternary strings, then the number $2110_3 = 2 \times 3^3 + 1 \times 3^2 + 1 \times 3^1 + 0 \times 3^0 = 66_{10}$. Clearly, the following

[1] For a rigorous proof, we must attend to some technical details. Define $f(x)$ as follows: if x is a bit string, prepend a single 1 bit to it, and treat it as the binary representation of some natural number n; then define $f(x) = n$. For instance, $f(0) = 10_2 = 2_{10}$, $f(101) = 1101_2 = 13_{10}$, and $f(0111) = 10111_2 = 18_{10}$. In this way we obtain a bijection $f : \{0,1\}^* \to \mathbb{Z}^+$, and since $\mathbb{Z}^+$ is countable, it follows that $\{0,1\}^*$ is, too. Put another way, the function $f : \{0,1\}^* \to \mathbb{N}$ is one-to-one, so it follows that $|\{0,1\}^*| \leq \mathbb{N}$, so the set $\{0,1\}^*$ is countable.

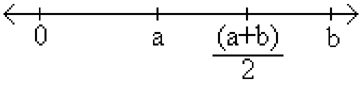
sets can all be put into a one-to-one correspondence: $\mathbb{N} \longleftrightarrow$ set of binary strings $\longleftrightarrow$ set of ternary strings. Let us see how these observations can be applied to polynomials. Say we have the polynomial $p(x) = 5x^5 + 2x^4 + 7x^3 + 4x + 6$. We can list the coefficients of $p(x)$ as follows: $(5,2,7,0,4,6)$. We can then write these coefficients as binary strings: $(101_2, 10_2, 111_2, 0_2, 100_2, 110_2)$. Now, we can construct a ternary string where a "2" is inserted between each binary coefficient (ignoring coefficients that are 0). We can map $p(x)$ to a ternary string as illustrated below:


$5x^5 + 2x^4 + 7x^3 + 4x + 6$
$\boxed{101}2\boxed{10}2\boxed{111}22\boxed{100}2\boxed{110}$

You may have noticed that the mapping $f : \{0,1,2\}^* \rightarrow \{\text{polynomials with coefficients} \in \mathbb{N}\}$ is not one-to-one. Taking the above example, we could have inserted superfluous leading 0's in the ternary string, all of which would still map to $p(x)$. This is not a major problem, since distinct polynomials map to distinct ternary strings according to our construction. This tells us that the number of polynomials is no larger than the number of ternary strings. Since the set of ternary strings is countable, it follows that the number of polynomials with natural number coefficients is also countable.

Cantor's Diagonalization

We have established that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ all have the same cardinality. What about the real numbers, the set of all points on the real line? Surely they are countable too? After all, the rational numbers are dense (i.e., between any two rational numbers there is a rational number):



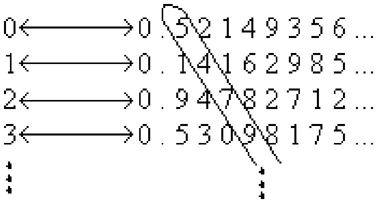
In fact, between any two real numbers there is always a rational number. It is really surprising, then, that there are more real numbers than rationals. That is, there is no bijection between the rationals (or the natural numbers) and the reals. In fact, we will show something even stronger, even the real numbers in the interval $[0,1]$ are uncountable!

Recall that a real number can be written out in an infinite decimal expansion. A real number in the interval $[0,1]$ can be written as $0.d_1d_2d_3$... Note that this representation is not unique; for example, $1 = 0.999$..., so the same real number can sometimes be expressed in two different ways.[2] For definiteness we shall assume that every real number is represented as a recurring decimal and we prefer to end with all 9's where possible (i.e., we choose the representation $.999\ldots$ rather than $1.000\ldots$).

[2] To see this, write $x = .999\ldots$. Then $10x = 9.999\ldots$, so $9x = 9$, and thus $x = 1$.

Theorem: The set $[0,1]$ of real numbers is not countable.

Cantor's Diagonalization Proof: Suppose towards a contradiction that there is a bijection $f : \mathbb{N} \rightarrow [0,1]$. This gives an infinite list of real numbers, namely, $f(0)$, $f(1)$, $\ldots$ We can enumerate the infinite list as follows:



$0 \longleftrightarrow 0.52149356\ldots$

$1 \longleftrightarrow 0.14162985\ldots$

$2 \longleftrightarrow 0.94782712\ldots$

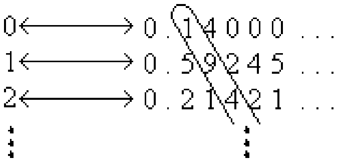
$3 \longleftrightarrow 0.53098175\ldots$

$\vdots \qquad \vdots$

The number circled in the diagonal is some real number r, since it is an infinite decimal expansion. Now consider the real number s obtained by modifying every digit of r, say by replacing each digit d with $d+5$ mod 10. (In the above picture, $r = 0.5479...$ and $s = 0.0924...$) We claim that s does not occur in our infinite list of real numbers. Suppose for contradiction that it did, and that it was the n^{th} number in the list. Then r and s differ in the n^{th} digit, since the n^{th} digit of s is the n^{th} digit of r plus 5 mod 10. So we have a real number s that is not in the range of f. But this contradicts the assertion that f is a bijection. Thus the real numbers are not countable.

Let us remark that the reason that we modified each digit by adding 5 mod 10 as opposed to adding 1 is that the same real number can have two decimal expansions; for example $0.999... = 1.000....$ But if two real numbers differ by more than 1 in any digit they cannot be equal.

With Cantor's diagonalization method, we proved that $\mathbb{R}$ is uncountable. What happens if we apply the same method to $\mathbb{Q}$, in a (futile) attempt to show the rationals are uncountable? Well, suppose for a contradiction that our bijective function $f : \mathbb{N} \rightarrow \mathbb{Q} \cap [0,1]$ produces the following mapping:



$0 \longleftrightarrow 0.14000\ \ldots$

$1 \longleftrightarrow 0.59245\ \ldots$

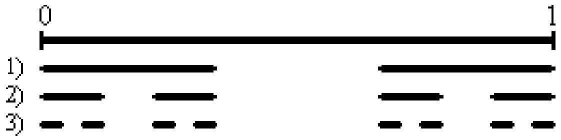
$2 \longleftrightarrow 0.21421\ \ldots$

$\vdots \qquad \vdots$

This time, let us consider the number q obtained by modifying every digit of the diagonal, replacing each digit d with $d+5$ mod 10. Then $q = 0.648...$, and we want to try to show that it does not occur in our infinite list of rational numbers. However, we do not know if q is rational (in fact, it is extremely unlikely for the decimal expansion of q to be periodic). This is why the method fails when applied to the rationals. When dealing with the reals, the modified diagonal number was guaranteed to be a real number—a number with an infinite decimal expansion.

The Cantor Set

The Cantor set is a remarkable set construction involving the real numbers in the interval $[0,1]$. The set is defined by repeatedly removing the middle thirds of line segments infinitely many times, starting with the original interval. For example, the first iteration would involve the removal of the interval $(\frac{1}{3},\frac{2}{3})$, leaving $[0,\frac{1}{3}]\cup[\frac{2}{3},1]$. The first three iterations are illustrated below:



The Cantor set contains all points that have *not* been removed: $C = \{x : x \text{ not thrown out}\}$. How much of the original unit interval is left after this process is repeated infinitely? Well, we start with 1, and after the first iteration we remove $\frac{1}{3}$ of the interval, leaving us with $\frac{2}{3}$. For the second iteration, we keep $\frac{2}{3}\times\frac{2}{3}$ of the original interval. As we repeat the iterations infinitely, we are left with:

$$1 \longrightarrow \frac{2}{3} \longrightarrow \frac{2}{3}\times\frac{2}{3} \longrightarrow \frac{2}{3}\times\frac{2}{3}\times\frac{2}{3} \longrightarrow \cdots \longrightarrow \lim_{n\to\infty}(\frac{2}{3})^n = 0$$

According to the calculations, it looks like we have removed everything from the original interval. It seems intuitive that the Cantor set C should be the empty set. In fact, not only is C not empty, but it is uncountable! To see why, let us first make a few observations about ternary strings. In ternary notation, all strings consist of digits (called “trits”) from the set $\{0,1,2\}$. All real numbers in the interval $[0,1]$ can be written in ternary notation ($\frac{1}{3}$ can be written as $.1_3$ and $\frac{2}{3}$ can be written as $.2_3$). Thus, in the first iteration, the middle third removed contains all ternary numbers of the form 0.1xxxxx...$_3$. The ternary numbers left after the first removal can all be expressed either in the form 0.0xxxxx...$_3$ or 0.2xxxxx...$_3$ (recall that $\frac{1}{3}$ = $.1_3$ = .02222...$_3$). The second iteration removes ternary numbers of the form .01xxxxx$_3$ and .21xxxxx$_3$ (i.e., any number with 1 in the second position). The third iteration removes 1’s in the third position. Therefore, what remains is all ternary numbers with only 0’s and 2’s. That is, $x \in C \iff \frac{x}{2}$ uses only 0’s and 1’s in its ternary representation (e.g., if $x = .0220_3$, then $\frac{x}{2} = 0.110_3$). But the set of all ternary numbers with only 0’s and 1’s can be put into one-to-correspondence with the set of all binary decimals .xxxxx...$_2$, and the latter set can be put into a one-to-one correspondence with the set $[0,1]$, which we proved earlier was uncountable. In other words, there is a bijection between C and the uncountable set $[0,1]$. Thus, since we found a bijection between the two sets, C must also be uncountable.

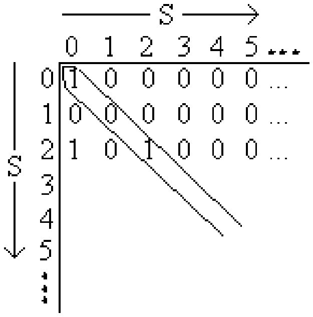
Higher Orders of Infinity

Let S be any set. Then the *power set* of S, denoted by $\mathscr{P}(S)$, is the set of all subsets of S. More formally, it is defined as: $\mathscr{P}(S) = \{T : T \subseteq S\}$. For example, if $S = \{1,2,3\}$, then $\mathscr{P}(S) = \{\{\},\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$.

What is the cardinality of $\mathscr{P}(S)$? If $|S| = k$ is finite, then $|\mathscr{P}(S)| = 2^k$. To see this, let us think of each subset of S corresponding to a k bit string. In the example above the subset $\{1,3\}$ corresponds to the string 101. A 1 in the i^{th} position indicates that the i^{th} element of S is in the subset and a 0 indicates that it is not. Now the number of binary strings of length k is 2^k, since there are two choices for each bit position. Thus $|\mathscr{P}(S)| = 2^k$. So for finite sets S, the cardinality of the power set of S is exponentially larger than the cardinality of S. What about infinite (countable) sets? We claim that there is no bijection from S to $\mathscr{P}(S)$, so $\mathscr{P}(S)$ is not countable. Thus for example the set of all subsets of natural numbers is not countable, even though the set of natural numbers itself is countable.

Theorem: Let S be countably infinite. Then $|\mathscr{P}(S)| > |S|$.

Proof: Suppose towards a contradiction that there is a bijection $f : S \rightarrow \mathscr{P}(S)$. Recall that we can represent a subset by a binary string, with one bit for each element of S. Consider the following diagonalization picture in which the function f maps natural numbers x to binary strings which correspond to subsets of S (e.g. $2 \rightarrow 10100... = \{0,2\}$):



	0	1	2	3	4	5 ...
0	1	0	0	0	0	0 ...
1	0	0	0	0	0	0 ...
2	1	0	1	0	0	0 ...
3						
4						
5						
⋮						

In this case, we have assigned the following mapping: $0 \rightarrow \{0\}$, $1 \rightarrow \{\}$, $2 \rightarrow \{0,2\}$, $\ldots$(i.e., for the n^{th} row, if there is a 1 in the k^{th} column, then include k in the set. If there is a 0, do not include k). Using a similar diagonalization argument, flip each bit along the diagonal: $1 \rightarrow 0$, $0 \rightarrow 1$, and let b denote this binary string. First, we must show that the new element is a subset of S. Clearly it is, since b is an infinite binary string which corresponds to a subset of S. Now suppose b were the n^{th} binary string. This cannot be the case though, since the n^{th} bit of b differs from the n^{th} bit of the diagonal (the bits are flipped). So it's not on our list, but it should be, since we assumed that the list enumerated all possible subsets of S. Thus, we have a contradiction, implying that if S is an infinite set, then $\mathscr{P}(S)$ is uncountable.

The idea of higher orders of infinity is encapsulated by the *aleph numbers*, which are a series of numbers that represent the cardinality of infinite sets. $\aleph_0$ (pronounced aleph null) represents the cardinality of countable sets, and we can continue and define $\aleph_1$, $\aleph_2$, and so on.