Cardinality

Shivanshu Kumar

January 29, 2025

Introduction

This article introduces the reader to the fundamental notion of cardinality in set theory, typically introduced in a first course on discrete mathematics. Basic background in set theory is assumed.

The idea of assigning cardinalities is to essentially compare infinite sets in terms of "size". For **finite** set S, we define its cardinality to be the number of elements in it, by definition of finite sets, this is a natural number and is well-defined. Since one can't count the number of elements in an infinite set, we think a bit differently.
Observe that two finite sets A and B have a bijection between them **if and only if** they have the same number of elements i.e., same cardinality.
Well, infinite sets don't seem to have issues with functions so we define:

Definition: Two sets A and B have the same cardinality iff $\exists$ a bijection from A to B and we write $|A| = |B|$

Notice that the definition matches our notion for the finite case as well. Also note that if a bijection exists from A to B, the inverse of this function is also a bijection, from B to A.

In most of the cases, we will try to get an explicit bijection between A and B, i.e., we will construct a map f such that every element in A maps to a unique element in B (one-one) and every element in B is mapped to some element in A, under f(onto).

The following definition gives the notion of one set being strcitly larger than the other, in cardinality

Defintion If there exists a one-one function from A to B, but no bijection, we write $|A| < |B|$. This means that there are enough elements in B that can be mapped to those in A, but the other way is not true.

Natural numbers though infinite, are well ordered, i.e., you take a bunch of them (infinitely many also work!) you can always set them in a line of "increasing order". Any set which has the same cardinality as $\mathbb{N}$, is also well ordered since now you can just take this order according to the bijection with $\mathbb{N}$.
We assume throughout that $\mathbb{N}$ contains 0

Results on Cardinality and Countablity

Definition A set S is said to be **countable** if it is finite or $|S| = |\mathbb{N}|$

Theorem 1 The set of all finite binary strings is countable.

Proof Consider the function, $f : (0,1)* \to \mathbb{N}$ defined by $f(s) = 2^{|s|} - 1 + t$, where $|s|$ denotes the length of s and t denotes its value in binary.
The intuition is to list down strings first in the order of length and then in the order of binary value. For length k, $1 + 2 + ...2^{k-1} = 2^k - 1$ strings appear before them and then we list them till $2^k - 1 + 2^k = 2^{k+1} - 1$ starting from 000...(k)..000

Thus observe that for string with length k,

$$2^k - 1 \leq f(s) < 2^{k+1} - 1$$

It is easy to see that two strings with same length will always have different values and hence map to a different number. Now consider two strings s_1, s_2 and WLOG $|s_1| > |s_2|$, clearly

$$f(s_2) < 2^{|s_2|+1} - 1 \leq 2^{|s_1|} - 1 \leq f(s_1)$$

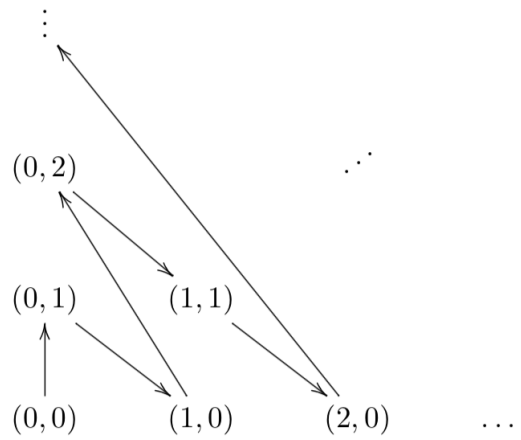
Thus for $s_1 \neq s_2, f(s_1) \neq f(s_2)$, and f is one-one.

Now consider any $n \in \mathbb{N}$. $\exists l, 2^l - 1 \leq n < 2^{l+1} - 1$. By defintion of f the binary string with length l and value $n - (2^l - 1)$ maps to n, proving that f is onto and hence bijective.

Q.E.D.

There are some cool sets related to the natural numbers whose cardinality might be of interest to us.
What about the rationals? Well it might seem that they are a bigger set, since they are very closely related to $\mathbb{N}^2$ (they are defined via pairs), but it turns out that the later too is countable! Lets see how.

Theorem 2 $|\mathbb{N}^2| = |\mathbb{N}|$
Proof



Similar to above, the intuition is to keep moving diagonally across pairs with a fixed sum and give them a "coarse" order, since there are finitely many of them, this ordering can be made finer by ordering them amongst themselves.

Formally, define $f : \mathbb{N}^2 \to \mathbb{N}$ as

$$f(i,j) = (t+2)(t+1)/2 - (j+1)$$

, where $t = i + j$. Observe as before

$$(t+1)(t+2)/2 - (t+1) \leq f(i,j) < (t+1)(t+2)/2$$

$$\Rightarrow t(t+1)/2 \leq f(i,j) < (t+1)(t+2)/2$$

Here t is playing the part of *length*. By a similar set of arguments one can prove that $(i_1, j_1) \neq (i_2, j_2) \Rightarrow f(i_1, j_1) \neq f(i_2, j_2)$ and that f is onto.

Q.E.D.

Note that WLOG, this theorem can be extended to any countable set S, if we are equipped with the following lemma (proof omitted)

Lemma 1 For given sets A, B, C if $\exists$ a bijection $f : A \to B$ and a bijection $g : B \to C$, then $\exists$ bijection $h = gof : A \to C$. i.e., $|A| = |B|$ and $|B| = |C| \Rightarrow |A| = |C|$

Well, this clearly indicates that $\mathbb{Q}$ should be countable too, and it is as we will show, but the following lemma will make things more formal.

Lemma 2 Any subset A of a countable S is countable.
Proof
The proof is trivial when A is finite

Suppose A is infinite. Since S is countable, $\exists f : S \to \mathbb{N}$
Define

$$a_0 = \text{a} \in A, \text{ st } f(a) < f(a') \forall a' \in A, a' \neq a$$

$$a_{k+1} = \text{a} \in A, \text{ st } f(a) < f(a') \forall a' \in A / \{a_0, a_1 .. a_k\}.$$

Since $f(a)$ is finite, $\forall a \in A, a = a_i$ for some $i \leq f(a)$.

Now let $g : A \to \mathbb{N}$ by

$$g(a_i) = i$$

Essentially, we are giving an order to A, based on the elements it got mapped to, under f.

Suppose $a_i \neq a_j$. WLOG $a_i > a_j$ and hence $g(a_i) > g(a_j)$. Thus g is one one. For any $n \in \mathbb{N}, \exists a$ st a $= a_n$, for otherwise, A would be finite. Hence g is onto.

Q.E.D.

Theorem 3 $|\mathbb{Q}| = |\mathbb{N}|$
Proof We will use the previous results to prove this in one-shot!

Define $h : \mathbb{Q} \to \mathbb{N}^2$ by

$$h(p/q) = (p, q)$$

where $\gcd(p, q) = 1$.

Define $S = h(\mathbb{Q}) = \{(i,j) \text{ st } f(x) = (i,j) \text{ for some } x \in \mathbb{Q}\}$.
Now define $h' : \mathbb{Q} \to S$ by $h'(x) = h(x)$, all we have done, is to get a bijection by putting the gun on the shoulders of h.
Since h is one-one and any $(i,j) \in S$ is mapped to something in $\mathbb{Q}$, by definition, h' is one-one and onto. Combining Lemma 1 and 2, we can thus show that $\mathbb{Q}$ is countable.

Q.E.D.

Theorem 2 is a lot more general result than we might think it is!

Theorem 4 for any $k > 1 \in \mathbb{N}, |\mathbb{N}^k| = |\mathbb{N}|$
Proof
We prove by induction on k. The base case $k = 2$ is proven above. (Of course we could have considered $k = 1$ for a more general base case)

Suppose $|\mathbb{N}^k| = |\mathbb{N}|$ for some k. Define $f : \mathbb{N}^k \to \mathbb{N}$ to be the corresponding bijection.
Define $g : \mathbb{N}^{k+1} \to \mathbb{N}^2$ as

$$g(n_1, n_2, ...n_{k+1}) = (f(n_1, n_2, ...n_k), n_{k+1})$$

The intuition is to first use the fact the a $k+1$-tuple is essentially a pair between a k tuple and the last element.

Now consider two different elements $x = (m_1, m_2, ...m_{k+1})$ and $y = (p_1, p_2, ...p_{k+1})$. If $m_{k+1} \neq p_{k+1}$, then $g(x) \neq g(y)$. If $m_{k+1} = p_{k+1}$, $(m_1, m_2, ...m_k) \neq (p_1, p_2, ...p_k)$, and from the one-one ness of f, it follows that $g(x) \neq g(y)$, proving g is one-one.

g is onto since given any $(i,j) \in \mathbb{N}^2$ $\exists (n_1, n_2, ...n_k)$ st $i = f(n_1, n_2, ...n_k)$. Letting $j = n_{k+1}$, we have $g(n_1, n_2, ...n_{k+1}) = (i,j)$, hence $|\mathbb{N}^{k+1}| = |\mathbb{N}^2| = |\mathbb{N}|$.

Q.E.D.

Recall Theorem 1. The set of finite binary strings is a **countable** union of finite sets, since the union is over the length of the strings and for a given length we can count them.
How about the countable (infinite) union of countable sets? Note that we are talking about taking an infinite union, where each set in itself is infinite, unlike theorem 1. The following theorem says it is true and due to the might of its statement we call it the "Holy Grail" theorem.

Theorem 5(Holy Grail) Let $\mathcal{P}_f(\mathbb{N})$ denote the set of all finite subsets of $\mathbb{N}$.

$$|\mathcal{P}_f(\mathbb{N})| = |\mathbb{N}|$$

Proof Let $\mathbb{N}_i$ denote the set of all subsets with size i. Observe that if elements are converted to tuples, $\mathbb{N}_i$ has all the i tuples, but without repeating, where as $\mathbb{N}^i$ has them with repetitions. Thus following from the argument given for $\mathbb{Q}$ and $\mathbb{N}^2$, we can say that $\mathbb{N}_i$ is countable $\forall i \in \mathbb{N}$.

$$\mathcal{P}_f(\mathbb{N}) = \bigcup_{i \in \mathbb{N}} \mathbb{N}_i$$

Thus for any element $x \in \mathcal{P}_f(\mathbb{N}), x \in \mathbb{N}_i$ for some i.

Let "the" bijection between $\mathbb{N}_i$ and $\mathbb{N}$ be f_i.

Define $g : \mathcal{P}_f(\mathbb{N}) \to \mathbb{N}^2$ as $g(x) = (i, f_i(x))$, where i is specified above.

Here we are trying to separate two layers of countability and translate that into $\mathbb{N}^2$, which is countable!

g is one-one, since every x has a unique member $\mathbb{N}_i$ it belongs to and $f_i(x)$ is one-one.
g is onto since, for any (m, n) $\exists \mathbb{N}_m$ and since f_m is onto, there exists $x \in \mathbb{N}_m$ st $f_m(x) = n$. Thus by defintion $\exists x$ st $g(x) = (m, n)$. Hence we have shown that $|\mathcal{P}_f(\mathbb{N})| = |\mathbb{N}^2| = |\mathbb{N}|$, from Theorem 2 and Lemma 1.

Q.E.D.

We've been getting lucky all along, but not now, Power sets are notoriously larger than their generator sets. We illustrate this in the following remarkable theorem.

Theorem 6(Cantor's theorem) For any set S, there doesnot exist a bijection from S to $\mathcal{P}(S)$.

Proof For finite sets the result is easy to see, since the latter has $2^n > n$ elements whenever $|S| = n$. For infinite sets this is not so straightforward, given the results we just saw.

We will prove by contradiction. Suppose there exists a bijection $f : S \to \mathcal{P}(S)$. Notice that $f(x)$ is a subset of S. Since f is onto, we can ask for $\hat{x}$ st $f(\hat{x}) = T$ where $T \subseteq S$ st

$$T = \{x \in S, x \notin f(x)\}$$

if $f(\hat{x}) = T$, two cases arise,

1. $\hat{x} \in T = f(\hat{x}) \Rightarrow \hat{x} \notin T$
2. $\hat{x} \notin T = f(\hat{x}) \Rightarrow \hat{x} \in T$

Both follow from the way T is defined and lead to a contradiction. Therefore an onto function and hence a bijection, between S and $\mathcal{P}(S)$ is not possible.

Q.E.D.

The proof in some way is trying to say that there arent enough elements in S that the elements of $\mathcal{P}(S)$ can be squeezed into, even when it is infinite.

Of course it follows that a naturally uncountable set is $\mathcal{P}(\mathbb{N})$. But reals turn out to be huge. In fact, the interval $(0, 1)$ is sufficient to cover the whole of $\mathcal{P}(\mathbb{N})$! This means that u cant pick up reals and order them in a line, this happens because real numbers have geometric/continuous origins and are not discretely spaced out as naturals or rationals.

Theorem 7 $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

Proof Define $f : (0, 1) \to \mathbb{R}$ as

$$f(x) = \tan\left(\pi(x - \frac{1}{2})\right)$$

f is bijective by definition of tan.

Let S be the set of infinite binary sequences. Define $g : (0, 1) \to S$, such that

$$g(x) = a_0a_1a_2...$$

where $0.a_0a_1a_2...$ is the binary expansion of $0 < x < 1$.

Define $h : S \to \mathcal{P}(\mathbb{N})$ as $h(a_0a_1a_2...) = \{n \in \mathbb{N}, a_n = 1\}$. Here, we are trying to pick up those indices in the binary expansion of x, that have a 1. These sets will give us all possible subsets of $\mathbb{N}$.

Formally, g is one-one since two different numbers have a different expansion and hence different strings, it is onto since given any binary string a number $0.a_0a_1a_2...$ exists in $(0, 1)$. h is one-one since, two different binary strings differ by at least one bit and hence $h(x)$ differs by at least one element. h is onto because given $T \subset \mathbb{N}$, the binary string x given by $a_0a_1a_2...$where $a_i = 1, i \in T\}$ and 0 otherwise, is such that $h(x) = T$, by definition.

Thus, g and h are both bijections and using lemma 1 we can say that $|(0, 1)| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$

Q.E.D.

Conclusion

We saw some fundamental results on cardinality in set theory. Infinite sets tend to behave counter-intuitively possibly because of way we think about/define them. Although some of the details have been skipped to avoid verbosity, we hope that the reader had fun!