Top 10 Amazing Card Tricks To Impress Your Mom

Recall that the cardinality of a set is the number of elements that it has, at least for finite sets. However, this extends in somewhat nontrivial ways for infinite sets, at which point we must formalize our intuitive definition of size.

Definition 8.1. *$|A| \leq |B|$ when there is an injection $f : A \to B$.*

Definition 8.2. *$|A| \geq |B|$ when there is a surjection $f : A \to B$.*

Definition 8.3. *Two sets are **equinumerous**; i.e., they have equal cardinality, when there exists a bijection between them.*

Example: We will construct a bijection from $\mathbb{N}$ to $\mathbb{Z}$. Let

$$f(n) := \begin{cases} n/2 & 2 \mid n, \\ -(n-1)/2 & \text{otherwise.} \end{cases}$$

Injectivity: Notice that for any n, $f(n) < 0$, if and only if n is odd. This is because even naturals are mapped to positive numbers, and odd naturals are mapped to nonpositive numbers.

Let $a, b \in \mathbb{N}$ such that $f(a) = f(b)$. In the first case, assume that $f(a)$ and $f(b)$ are positive. Then a and b must both be even, meaning that $a/2 = f(a) = f(b) = b/2$, so $a = b$.

In the second case, assume that $f(a)$ and $f(b)$ are nonpositive. Then a and b must both be odd, so $-(a-1)/2 = f(a) = f(b) = -(b-1)/2$, so $a = b$.

Surjectivity: Let $a \in \mathbb{Z}$. If a is positive, then $f(2a) = a$. If a is nonpositive, then $f(-2a+1) = a$.

Therefore f is bijective, so $|\mathbb{N}| = |\mathbb{Z}|$.

Example: We will construct a bijection from $\mathbb{N}$ to $\mathbb{Q}^+$, the set of positive rationals.

This time, before a difficult proof, I will present the idea first. This is not common of literature, but for now, I think it is helpful to include.

The idea is this: Consider a 2D grid, that starts from the top-left and extends infinitely to the right and below. In row i and column j of this grid, I will write i/j. Then I will consider all the diagonals that go from the bottom-left to the top-right. If I join all of them together, in order of increasing diagonal size, I expect to end up with all the rationals on an infinite line. Now all that is left is to delete the duplicates, and I have an infinite sequence of all my positive rationals.

Definition 8.4. *A finite sequence on an arbitrary set A is a function $f : [n] \to A$, for some $n \in \mathbb{N} \cup \{0\}$. We say that $\{a\}$ is a finite sequence of length n where $a_i := f(i)$.*

Definition 8.5. *An infinite sequence is a function from $\mathbb{N}$ to an arbitrary set A.*

Definition 8.6. *If $\{a\}$ and $\{b\}$ are a finite sequence on a set A with n and m elements respectively, then their composition is a finite sequence with $n + m$ elements, and is defined by the function $f : [n+m] \to A$, where*

$$f := \begin{cases} a_i & 1 \leq i \leq n, \\ b_{i-n} & n+1 \leq i \leq n+m. \end{cases}$$

Lemma 8.7. *Composing an infinite sequence of finite sequences yields an infinite sequence.*

Proof. Let A be an arbitrary set, and let B be the set of finite sequences on A. Let $\{b\}$ be an infinite sequence on B, and let $\{l\}$ be a sequence of lengths of sequences in $\{b\}$. Now let c be the composition of all sequences in $\{b\}$.

(I will interject with some helpful information. To visualize c, the first l_1 elements are going to be the sequence b_1, so that would be $(b_1)_1, (b_1)_2, ..., (b_1)_{l_1}$. Then you will see l_2 elements, i.e., the elements of b_2, and so forth).

Let $S : \{0\} \cup \mathbb{N} \to \{0\} \cup \mathbb{N}$ be a function, where $S(0) = 0$, and $S(i) = S(i-1) + l_i$, which is to say, S is a prefix sum of the lengths of sequences in $\{b\}$. Then we can define c_i explicitly:

$$c_i = (b_{j+1})_{i-S(j)}, \text{ where } j = \max(\{x \mid S(x) < i\}).$$

The idea is that once i exceeds a new $S(j)$, we should switch to sequence b_{j+1} and find the correct index to use in that sequence.

c is infinite, because if it had a finite number of elements, N, then there would be no elements from b_{N+1} onwards.

□

We have a bazooka of a lemma - now it is time to fire.

Proposition 8.8. *There is a bijection from $\mathbb{N}$ to $\mathbb{Q}^+$.*

Proof. Let $\{b\}$ be a sequence of sequences of positive rational numbers. Define b_i to be a sequence of positive rational numbers whose numerators and denominators sum to i, such that they have not appeared in any b_j, for $j < i$. Let c be the composition of sequences in $\{b\}$. Now we will prove c is a bijection.

Injectivity: Suppose $c_x = c_y$. Then $c_x = p/q = c_y$ is a rational number, in lowest terms. Notice that for any integer fraction i/j, the sum of the numerator and denominator is minimal when the rational is in lowest terms. Thus p/q must appear in b_{p+q}, as there is no smaller index k such that b_k could contain p/q. So both c_x and c_y appear in the same sequence b_{p+q}, but b_{p+q} by definition should not contain duplicate elements. Therefore $x = y$.

Surjectivity: Let p/q be a positive rational number in lowest terms. We already know that a rational number in lowest terms must appear in b_{p+q}, so it necessarily appears somewhere between $c_{1+S_{p+q-1}}$ and $c_{S_{p+q}}$, inclusively. □

Now we know that $|\mathbb{N}| = |\mathbb{Q}^+|$.

Definition 8.9. *A set is **countable** if it is either finite or equinumerous with the naturals. In the latter case, we say that it is **countably infinite**.*

Definition 8.10. *A set is **uncountable** if it has cardinality greater than the naturals.*

Theorem 8.11. $|\mathbb{R}| > |\mathbb{N}|$.

Note 8.12. *This is a sketchy proof, but here it is anyways.*

Proof. There is an injection from $\mathbb{N}$ to $(0, 1)$: $f(n) = 1 - 1/(n+1)$. So $|\mathbb{N}| \leq |(0, 1)|$. Similarly, $|(0, 1)| \leq |\mathbb{R}|$, if we let $f(x) = x$.

Now let $f : \mathbb{N} \to (0, 1)$ be any function, and let $\{d\}_i$ be the infinite sequence of digits representing the decimal expansion of $f(i)$. Construct a number $x \in (0, 1)$, where the i^{th} digit of the decimal expansion of x differs from d_{ii}.

This means that $x \neq f(i)$ for any i, which means that x is not in the image of f. Therefore, f is not surjective. Since there is no surjection from $\mathbb{N}$ to $(0, 1)$, $|\mathbb{N}| < |(0, 1)|$, which means $|\mathbb{N}| < |\mathbb{R}|$. □

Axiom 8.13. *The Continuum Hypothesis: There exists a set $\mathcal{C}$ such that $|\mathbb{N}| < |\mathcal{C}| < |\mathbb{R}|$. We write $|\mathbb{R}| = \mathfrak{c}$ (`\mathfrak{c}`) (read as "cardinality of the continuum").*

Note 8.14. *It turns out that the Continuum Hypothesis (CH) can either be true or false, and normal set theory remains consistent either way. We say that this type of mathematical statement is **independent** of our logical system.*

Theorem 8.15 (Cantor). *For any set X, $|X| < |\mathcal{P}(X)|$.*

Proof. There is a trivial injection from X to $\mathcal{P}(X)$: namely, for each $x \in X$, $x \mapsto \{x\}$. Hence $|X| \leq \mathcal{P}(X)$. Now towards a contradiction suppose that there is a surjection $f : X \to \mathcal{P}(X)$. Now consider the set $A := \{x \in X \mid x \notin f(x)\}$. Since f is onto and $A \in \mathcal{P}(X)$, it follows that there exists an $a \in X$ such that $f(a) = A$. However, if $a \in A$, then $a \notin f(a) = A$ by the definition of A, and this is impossible; if $a \notin A$, then $a \in f(a) = A$ again by definition of A and this is also impossible. The contradiction has arrived and the proof of Cantor's theorem is complete. □

Note 8.16. *The last sentence of the above proof is from Halmos' Naive Set Theory, which you should definitely read if you have the chance. It was just too good of a sentence not to write.*

Homework

1. There is an error in Lemma 8.7, similar to the last time I pointed out my own error. Find it, fix the statement of the lemma, and amend the proof to adapt to this. Discuss in Discord.

2. **(Pigeonhole Principle).**

   (a) Show that there is no injection from $[n+1]$ to $[n]$, for any nonnegative integer.

   (b) † Suppose I give you 100 naturals. Prove that it is always possible to pick a subset of size 15 such that the difference of any two is a multiple of 7.

3. Exhibit a bijection from $\mathbb{Z}$ to $\mathbb{Q}$.

4. Show that if a set A has a bijection to a subset of $\mathbb{N}$, then it is countable. Conclude that if $|A| \leq |\mathbb{N}|$, then it is countable.

5. (a) Suppose A_1, A_2 are countable sets. Show that there is an injection $f : A_1 \times A_2 \to \mathbb{N}$. [Hint: Fundamental theorem of Arithmetic.]

   (b) Generalize to any countable $A_1 \times A_2 \times \cdots \times A_n$.

   (c) Use parts (a) and/or (b) to get another proof that $\mathbb{Q}$ is countable.

6. (a) Suppose that $\mathcal{A}$ is a countable collection of countably infinite sets. That is, there are countably many sets contained in $\mathcal{A}$. Show that $\bigcup_{A \in \mathcal{A}} A$ is countable.

   (b) Deduce that the collection of all finite subsets of $\mathbb{N}$ is countable.