Bijections and Cardinality

We now turn to the connection between functions and cardinality of sets. We begin in the realm of finite sets, where things are intuitively clearer.

Let's consider the two finite sets $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. It's pretty easy to see which one of these sets is the *larger* one, right? Just to make sure we're all on the same page, write the name of the larger set here: ____ .

Why is this set larger? Well, it has *more* elements in it; its cardinality is greater. We can make similar comparisons between sets of the same size. Consider A as above, and $C = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$. Obviously these two sets are the same size, since they have the same cardinality.

In order to make "standardized" comparisons of size between sets, let's define a standard "yard-stick" against which we can compare any finite set. Namely, let's make the

Definition. Let $n \in \mathbb{N}$. We define the set $[n]$ by

$$[n] = \{1, 2, 3, ..., n\}.$$

We also let $[0] = \emptyset$. These sets are our standardized tools (our "lab equipment," if you will) for measuring sets: they give us sets of any finite size.

If these are our tools, how do we use them? That is, what does our measuring procedure look like?

(Re)definition. The *cardinality* of a finite set A, denoted $|A|$, is the *unique* value $n \in \mathbb{N}$ such that there is a bijection from A to $[n]$.

Notes. We need to check that this definition is *well-defined*; that is, that there really is a *unique* value n that can be assigned in this fashion. Also, we need to explain why we're redefining the seemingly perfectly adequate definition of cardinality that we came up with before (based merely upon counting). We'll take the first issue first, since it's simpler. The second takes us to a massive and useful generalization.

To establish the uniqueness of the number n assigned as the cardinality of a given set A, we need two facts:

Fact 1. There is a bijection between $[m]$ and $[n]$ if and only if $m = n$.

Proving this fact is quite difficult and technical, we'll set it aside for now. Meanwhile, we have

Fact 2. Prove that if $f : A \to B$ and $g : B \to C$ are both bijections, then the composition $g \circ f : A \to C$ is also a bijection.

Now we put these facts together:

Exercise 3. Prove that the definition of the cardinality of a finite set A, as given above, is well-defined.

Not only do we now have the means to establish when two sets have the same size, we've also got a tool for establishing when one set is larger than another:

Corollary. The finite set A is larger than the finite set B (*i.e.*, $|A| > |B|$) if and only if there is a bijection between B and a proper subset of A.

Okay, are you ready to see *why* we went to the trouble to redefine cardinality as we just did?

Definition. Suppose now that A and B are *infinite* sets. We say that A and B *have the same cardinality*, denoted $|A| = |B|$, if there is a bijection from A to B.

Thus our means of comparing the sizes of sets extends *completely naturally* to infinite sets!

Example. Prove that $|\,\mathbb{N}\,| = |\,\mathbb{Z}\,|$ by establishing a bijection $f : \mathbb{N} \to \mathbb{Z}$. (*Hint*: the easiest way to come up with such a function is to first "graph it out" on a number line, and then find a formula for f by using the first several values.)

The above example is kind of counterintuitive: there are seemingly *more* elements in $\mathbb{Z}$ than in $\mathbb{N}$, yet by our definition these sets are the same size. This common size comes up often enough for us to give it a special name:

Definition. We say that the set A is *countable* (or *countably infinite*) if there is a bijection $f : A \to \mathbb{N}$.

Thus $\mathbb{Z}$ is a countable set, as of course is $\mathbb{N}$. Here's another surprising

Example. Prove that the set $\mathbb{N} \times \mathbb{N}$ is countable. (*Hint*: This is a "picture proof"!)

Second proof. Consider the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(m, n) = 2^{m-1}(2n - 1)$ for all $(m, n) \in \mathbb{N} \times \mathbb{N}$. Let's use the space below to argue that this is an explicit bijection:

Now let's take note of a familiar set which is *not* countable (we call such sets, not surprisingly, *uncountable*):

Theorem. The unit interval $[0, 1]$ is not countable.

Proof.

It was relatively clear with finite sets that if there's a bijection from A to a subset of B then $|A| \leq |B|$; this holds true for infinite sets, too, though the proof is somewhat trickier. Thus we have

Corollary. $|\mathbb{N}| < |[0,1]| \leq |\mathbb{R}|$. In fact, equality holds in this last instance, since $f : (0,1) \to \mathbb{R}$ by $f(x) = \tan^{-1}(2x - \pi)$ is a bijection.

What about $\mathbb{Q}$? We've left the rationals out of the action so far.

Note that the set $\mathbb{Q}$ is "kind of" a subset of $\mathbb{Z} \times \mathbb{Z}$ in a natural fashion; after all, every rational $\frac{p}{q}$ corresponds to the pair of integers (p, q). To make this more precise, let's define an equivalence relation q on the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by

$$(a, b) \sim_q (c, d) \Leftrightarrow ad = bc,$$

where the multiplication is as usual. (Notice that if we think of (a, b) and (c, d) as fractions, this is saying that $\frac{a}{b}$ and $\frac{c}{d}$ are equivalent if and only if when we cross multiply we get equality!)

Definition. The set of *rational numbers*, $\mathbb{Q}$, is defined to be

$$\mathbb{Q} = \{[(a, b)]_q \mid (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}.$$

Note this means that $\mathbb{Q}$ is even "smaller" than $\mathbb{Z} \times \mathbb{Z}$, since we're not even using all of $\mathbb{Z}$ in the second coordinate, and we're "collapsing" a lot of pairs using our equivalence classes. On the other hand, it's clear that $\mathbb{Q}$ has got to be at least as big as $\mathbb{N}$, since $\mathbb{N} \subseteq \mathbb{Q}$.

The upshot is the following fact:

Theorem. $|\mathbb{N}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, so all of these sets have the same cardinality and are therefore all countable.

Finally, here's one last fact that enables us to prove that there are infinitely many sizes of infinity:

Theorem. Let S be any set (finite or infinite). Then $|S| < |\mathcal{P}(S)|$.

Proof. If S is finite, we're done, since $|\mathcal{P}(S)| = 2^{|S|}$. Otherwise, suppose BWOC there is a bijection $\phi : S \to \mathcal{P}(S)$ and consider the set $A = \{s \in S \mid s \notin \phi(s)\} \subseteq S$.

Here's the \$64,000-dollar question: what $a \in S$ maps onto A?

Corollary. There are infinitely many sizes of infinity.

Proof. Let $S_1 = \mathbb{N}$ and let define S_{n+1} *recursively* by $S_{n+1} = \mathcal{P}(S_n)$. Using induction and the above theorem,

$$|S_1| < |S_2| < \cdots < |S_n| < |S_{n+1}| < \cdots.$$