Extra discussion

Kyle Miller

Jan 31, 2017

There were loose ends from Monday's discussion, and I wrote this note to do some of them justice. If you would like to discuss this more, please bring it up during discussion or office hours.

1 Images

For a function $f : X \to Y$, when $x \in X$, $y \in Y$, and $y = f(x)$, then y is called the *image* of x with respect to the function f. When thinking of f as a relation on $X \times Y$, then this is saying that $(x, y) \in f$.

Given a subset $A \subset X$, $f(A)$ denotes *image* of A with respect to f. By definition, $f(A) = \{f(x) : x \in A\}$. It is somewhat confusing to use essentially the same notation $f(x)$ and $f(A)$ to mean different things — you must know whether the argument to f is an element of X or an element of the powerset $\mathcal{P}(X)$. People who detest ambiguous notation sometimes write $f[A]$ instead.

If you are a fan of Python or functional programming, $f(A)$ is how we "map the function f over the set A." In Python, you might write `{f(x) for x in A}` or `map(f, A)` instead. In Mathematica, it is something like `f /@ A`.

Let us prove some statements about images. The first says that function application distributes over unions.

Theorem 1. *For $f : X \to Y$ and $A, B \subset X$, then $f(A \cup B) = f(A) \cup f(B)$.*

Proof. (We first give the proof in a more formal style.)

Claim: $f(A \cup B) \subset f(A) \cup f(B)$.

Let $y \in f(A \cup B)$ be arbitrary

By definition of set image, there is an $x \in A \cup B$ such that $y = f(x)$.

By definition of union, $x \in A \vee x \in B$.

Case I. $x \in A$.

By definition of set image, $f(x) \in f(A)$.

By a property of unions, $f(A) \subset f(A) \cup f(B)$.

Thus, $f(x) \in f(A) \cup f(B)$.

Case II. $x \in B$.

By definition of set image, $f(x) \in f(B)$.

By a property of unions, $f(B) \subset f(A) \cup f(B)$.

Thus, $f(x) \in f(A) \cup f(B)$.

Thus, $y \in f(A) \cup f(B)$.

Since y was arbitrary, $f(A \cup B) \subset f(A) \cup f(B)$.

Claim: $f(A) \cup f(B) \subset f(A \cup B)$.

Let $y \in f(A) \cup f(B)$ be arbitrary.

Case I. $y \in f(A)$.

There is an $x \in A$ such that $y = f(x)$.

By a property of unions, $x \in A \cup B$.

By definition of set image, $y \in f(A \cup B)$.

Case II. $y \in f(B)$.

There is an $x \in B$ such that $y = f(x)$.

By a property of unions, $x \in A \cup B$.

By definition of set image, $y \in f(A \cup B)$.
Thus, $y \in f(A \cup B)$.
Since y was arbitrary, $f(A) \cup f(B) \subset f(A \cup B)$.
Thus, $f(A \cup B) = f(A) \cup f(B)$.

(Now a more informal style, as would be seen in a textbook.)

First, we show $f(A \cup B) \subset f(A) \cup f(B)$. Let $y \in f(A \cup B)$ be arbitrary, and let $x \in A \cup B$ be such that $y = f(x)$. If $x \in A$, then $y \in f(A) \subset f(A) \cup f(B)$, and similarly if $x \in B$, then $y \in f(B) \subset f(A) \cup f(B)$. Thus, $y \in f(A) \cup f(B)$, and since y was arbitrary, the first claim follows.

Second, we show $f(A) \cup f(B) \subset f(A \cup B)$. This is logically equivalent to showing both $f(A) \subset f(A \cup B)$ and $f(B) \subset f(A \cup B)$. By symmetry, we only need to show the first. Let $y \in f(A)$ be arbitrary, and let $x \in A$ be such that $y = f(x)$. Then since $A \subset A \cup B$, it follows that $y = f(x) \in f(A \cup B)$. Since y was arbitrary, $f(A) \subset f(A \cup B)$.

Therefore, the two sets are equal. □

The next theorem says that function application almost distributes over intersection.

Theorem 2. *Let $f : X \to Y$ and $A, B \subset X$. Then $f(A \cap B) \subset f(A) \cap f(B)$.*

Proof. *(A more formal style.)*

Let $y \in f(A \cap B)$ be arbitrary.
By definition of set image, there is an $x \in A \cap B$ such that $y = f(x)$.
By definition of intersection, $x \in A$ and $x \in B$.
By definition of set image, $f(x) \in f(A)$ and $f(x) \in f(A)$.
By definition of intersection, $f(x) \in f(A) \cap f(B)$.
Thus, $y \in f(A) \cap f(B)$.
Thus, $f(A \cap B) \subset f(A) \cap f(B)$. □

It is impossible to prove the opposite set inclusion. This is because there is a counterexample. For instance, let $f : \mathbb{R} \to \mathbb{R}$ be the constant function $f(x) = 0$. Then $f([0,1] \cap [2,3]) = f(\emptyset) = \emptyset$ and $f([0,1]) \cap f([2,3]) = \{0\} \cap \{0\} = \{0\}$, which is not the empty set.

I'm pretty sure that if f is an injection (it is one-to-one), then it becomes an equality. I leave either proving this modification or finding a counterexample to it to you.

2 Countability

The idea of a set being *countable* (or *enumerable* or *denumerable*) is that you can list out every element one at a time, and eventually any particular entry of the set will appear in the list. There are two ways of reading "it means you can count everything in the set." It does not mean that eventually everything will be counted. Rather, it means everything will eventually be counted. (A different quantifier order, so to speak.)

A *finite* set is a set X such that there is a bijective function $f : n \to X$, where $n \in \mathbb{N}$ (remember, a number is commonly thought of a set having that many elements, so $n = \{0, 1, 2, \dots, n-1\}$). These are sets where eventually everything will be counted. The other option is a *countably infinite* set, which is a set X such that there is a bijective function $f : \mathbb{N} \to X$ (where $\mathbb{N} = \{0, 1, 2, \dots\}$ — we can actually think of $\mathbb{N}$ itself being a number! Though it is not a natural number since $\mathbb{N} \notin \mathbb{N}$).

In either case, the bijection lets us list every element of X one at a time. In pseudocode, it might look like:

```
i = 0
while i in domain(f):
  print "Element number", i, "is", f(i)
  i = i + 1
```

A function $f : n \to X$ is commonly thought of as a finite sequence $f_0, f_1, \dots, f_{n-1}$ (compare with vectors of $\mathbb{R}^n$ if you want), and a function $f : \mathbb{N} \to X$ is commonly thought of as an infinite sequence $f_0, f_1, \dots$. The function f being bijective means (1) it is surjective, so every element of X appears in the sequence at least once; and (2) it is injective, so the sequence has no repeats.

It makes the concept of counting easier if we say we don't want repeats in the sequence, but sometimes it is easier to show is that everything is eventually counted, possibly more than once (even possibly infinitely many times!). It actually turns out that if there is a surjection $f : n \to X$ or $f : \mathbb{N} \to X$, then you can make a bijection $g : n \to X$ or $g : \mathbb{N} \to X$, irrespectively, out of it. The idea is just to cross out repeats and renumber everything. For instance:

```
def g(i):
  seen = set()
  j = 0
  while len(seen) < i:
    x = f(j)
    seen.add(x)
    j = j + 1
  return x
```

The domain of g is determined by the following rule: any i which makes g get the value of f for j outside the domain, or which causes this program to enter an infinite loop, will be considered outside the domain of g. One example is the sequence $\star, \Diamond, \star, \Diamond, \star, \Diamond, \dots$ will result in the finite sequence $\star, \Diamond$.

The set $\mathbb{N}$ is itself countable because the identify function $f(n) = n$ is a bijection. Another example is $\mathbb{Z}$, the set of integers. There are many ways to count $\mathbb{Z}$, but one way is

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ -(n+1)/2 & \text{if } n \text{ is odd} \end{cases}$$

This is the same as

```
i = 0
while True:
  print "integer number", 2*i, "is", i
  print "integer number", 2*i+1, "is", -i-1
  i = i + 1
```

If X and Y are countable, so is the Cartesian product $X \times Y$. To make sure everything is eventually counted, there is a certain standard trick you can use, which I've heard called the "ω-ordering."

```
i = 0  # the numbering
j = 0  # we will print out pairs (f(k), f(j-k)), so k+(j-k)=k
while True:
  for k in range(0,j+1): # so 0 <= k <= j
    print "Element number", i, "is", (f(k), f(j-k))
    i = i + 1
  j = j + 1
```

The set $\mathbb{Q}$ of rational numbers is in correspondence with a subset of pairs in $\mathbb{Z} \times \mathbb{Z}$, where a/b corresponds to (a, b) when a/b is reduced. Since $\mathbb{Z} \times \mathbb{Z}$ is countable, so is $\mathbb{Q}$. More directly, this will print out every positive rational number eventually:

```
j = 1
while True:
  for b in range(1,j):
    a = j - b
    if gcd(a,b) == 1: # i.e., a/b is reduced
      print a,"/",b
  j += 1
```

3 Uncountability

A set X is *uncountable* if it is not finite and it is not countably infinite. We'll just focus on uncountability for the case where the set is not finite.

Notation: The set Y^X or $X \to Y$ is the set of functions with domain X and codomain Y. The exponential notation is because for finite sets, $|Y^X| = |Y|^{|X|}$.

One basic question is how big is the set of infinite sequences $X^{\mathbb{N}}$. Is the set of infinite sequences countable? Surely, if $|X| \geq 2$, then $X^{\mathbb{N}}$ is infinite, since if $a, b \in X$ are distinct, then $(a, b, b, b, \dots)$, $(b, a, b, b, \dots)$, $(b, b, a, b, \dots)$, and so on are distinct sequences.

For simplicity, let's just consider infinite sequences of 0 and 1, that is the set $2^{\mathbb{N}}$. If X has at least two elements, sequences in $2^{\mathbb{N}}$ can be faithfully represented in $X^{\mathbb{N}}$.

So, the answer is "No, $2^{\mathbb{N}}$ is not countable." The reason uses a common type of argument, called "diagonalization," and is the same kind of argument as for showing that $\{x : x \notin x\}$ is not a set.

We prove it by contradiction. Suppose $f : \mathbb{N} \to 2^{\mathbb{N}}$ were a bijection. We define a sequence $g : \mathbb{N} \to 2$ by $g(n) = 1 - f(n)(n)$ (so g gives the opposite of what f would give for the nth sequence's nth entry[1]). Since f is a bijection, it has an inverse. It is now time to wire everything into a big contradiction. The question is, what is $g(f^{-1}(g))$?

$$\begin{aligned} g(f^{-1}(g)) &= 1 - f(f^{-1}(g))(f^{-1}(g)) \\ &= 1 - g(f^{-1}(g)) \end{aligned}$$

This uses $f(f^{-1}(g)) = g$. But, $g(f^{-1}(g)) \in \{0, 1\}$, and the algebra seems to imply $g(g^{-1}(g)) = \frac{1}{2}$!. Therefore, there is no such bijection f. The set $2^{\mathbb{N}}$ is not countable.[2]

A question which came to my mind is to figure out how many different ways there are to count $\mathbb{N}$. That is, if $X = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a bijection}\}$, is X countable? First of all, just because $\mathbb{N}^{\mathbb{N}}$ is uncountable doesn't mean anything about X, which is merely a subset. But it turns out there is a way to put X in a one-to-one correspondence with $\mathbb{N}^{\mathbb{N}}$. Given an arbitrary sequence $g \in \mathbb{N}^{\mathbb{N}}$ we can make a bijection $f : \mathbb{N} \to \mathbb{N}$ using the following inductive definition:

$$\begin{aligned} f(0) &= g(0) \\ f(n+1) &= (\mathbb{N} \setminus f(\{0, 1, \dots, n\}))[g(n+1)] \end{aligned}$$

where $A[m]$ is *ad hoc* notation which means "take the mth smallest number in the set A". The set $\mathbb{N} \setminus f(\{0, 1, \dots, n\})$ is $\{m \in \mathbb{N} : m \neq f(0) \wedge m \neq f(1) \wedge \cdots \wedge m \neq f(n)\}$. I have not proved this for you that f is indeed a bijection and that every g produces its own unique f, and that every bijection can be obtained this way.

A standard set to show is uncountable is $\mathbb{R}$. Roughly speaking, all you need to do is take numbers in the interval $[0, 1)$, write them as infinite binary sequences, show that it gets every sequence in $2^{\mathbb{N}}$ except for at most countably many (for instance, $011111\dots$ won't happen since it would correspond to the same real number as $100000\dots$), and we showed $2^{\mathbb{N}}$ is uncountable.

4 Comprehension

Like how a proposition is something which is either true or false, a set is something which either has or does not have any particular thing. This is why $\{x : x \notin x\}$ should not be a set: is it an element of itself?

When A is a set and $p(x)$ is a predicate, the following is always a set: $X = \{x \in A : p(x)\}$, pronounced "the set of all x in A where $p(x)$ is true." This is a set because to determine whether $x \in X$, it is logically equivalent to saying that $x \in A$ and $p(x)$. Since A is a set, it is either true or false that $x \in A$, and since $p(x)$ is a proposition, it is either true or false that $p(x)$. Thus, it is either true or false that $x \in X$.

The empty set is a set because it definitively has no elements.

[1] What does $f(n)(n)$ mean? Well, $f(n) \in 2^{\mathbb{N}}$, and an element of $2^{\mathbb{N}}$ is a function $\mathbb{N} \to 2$. It might be clearer to write $(f(n))(n)$, or maybe $f_n(n)$, or even $f_{n,n}$.

[2] Another way to understand this is that a function $\mathbb{N} \to 2^{\mathbb{N}}$ is "the same" as a function $\mathbb{N} \times N \to 2$. That is to say, a table of 0's and 1's which extends infinitely far to the right and downward. The sequence g is the result of taking the diagonal of the table as a sequence, and substituting $0 \leftrightarrow 1$. Since g is a sequence, it appears as a row in the table, so row n, and the contradiction is that column n of this row will be the opposite of itself!