

Day 15

Tuesday June 12, 2012

1 Properties of Function

So far we have talked about different things we can talk about with respect to a function. So far if $f : A \rightarrow B$ we have the following features:

- A domain: the function only allows inputs from this set, and gaurentees for each input there will be only one, unique output. In the above, the domain is A .
- A codomain: the function promises that all outputs will lie here. In the above, the codomain is B .
- The image: these are the values of the function that that function will actually hit in the codomain.

A natural question why would you want to make your codomain larger than the image?

1. One reason is that it is easier to generalize certain results. For instance, you might have a theorem that pertains to all $f : \mathbb{R} \rightarrow \mathbb{R}$; you might be able to use this theorem to tell you something about your function, even if yours actually only maps into \mathbb{R}^+ or $(0, 1)$.
2. The second reason is simply that it's often hard to calculate the image of a function. You can see this in programming. You often specify that an output of some subroutine is an `int` even though the function never outputs negatives and 0.
3. Similar to the second, it often doesn't matter. Your codomain acts as a gaurentee to the person using your function. You may be able to say, "I promise this will be a real number, except it's never an even natural or a decimal number with a finite number of 2's," but your end user (the person using the function) would probably be just happy knowing that you promise that it's a real.

We also know, if $f : A \rightarrow B$ and $A' \subseteq A$ and $B' \subseteq B$ then

- $f[A']$ is the image of f under A' ; it is the set of values in B that can be achieved using values in A' .
- $f^{-1}[B']$ is the pre-image (or inverse image) of B' ; it is the set of values in A that would land in B' .

We will make use of all these notions in our definitions of properties, so it's best that we are pretty fluent in them.

1.1 Properties of Images and Pre-Images

There's some very basic properties of the image and preimage that we will not prove, but you should check:

Theorem 1. *If $f : A \rightarrow B$ then*

1. $f[A] \neq \emptyset$.
2. $f^{-1}[B] \neq \emptyset$.

A very useful property of the pre-image is the following

Theorem 2. *If $f : A \rightarrow B$ and $X, Y \subseteq B$ then*

$$f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y]$$

Proof. (\subseteq) Take an $x \in f^{-1}[X \cap Y]$. Then we know there is some $y \in X \cap Y$ such that $f(x) = y$. As $y \in X \cap Y$, we know it is in X and Y . Thus $x \in f^{-1}[X]$ and $x \in f^{-1}[Y]$ as there is some element of X , namely y , that x hits, and similarly for Y .

(\supseteq) Take $x \in f^{-1}[X] \cap f^{-1}[Y]$. Then $x \in f^{-1}[X]$ and $x \in f^{-1}[Y]$. So we know there is some $y \in X$ such that $f(x) = y$ and some $z \in Y$ such that $f(x) = z$. But, as f is a function, $z = y$, so $y \in X \cap Y$. Therefore, as $f(x) = y$ we know $x \in f^{-1}[X \cap Y]$ \square

Theorem 3. If $f : A \rightarrow B$ and $X, Y \subseteq B$ then

$$f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y]$$

Proof. (\subseteq) Take $x \in f^{-1}[X \cup Y]$. Then there is some $y \in X \cup Y$ such that $f(x) = y$. If $y \in X$ then $x \in f^{-1}[X]$. Otherwise, $y \in Y$, and so $x \in f^{-1}[Y]$. Regardless, $x \in f^{-1}[X] \cup f^{-1}[Y]$.

(\supseteq) Take $x \in f^{-1}[X] \cup f^{-1}[Y]$. If $x \in f^{-1}[X]$ then there is some $y \in X$ such that $f(x) = y$. Thus, $y \in X \cup Y$ and so $x \in f^{-1}[X \cup Y]$. Otherwise, $x \in f^{-1}[Y]$, which is analogous. \square

Remark 1. Less details are being presented in these proofs as they would normally as we are expected to be good at the mechanics of a double containment proof. You should not omit these details until you reach a point of fluency.

Like any language, fluency in creation always comes after fluency in comprehension.

There are analogous theorems of the forward image of a set

Theorem 4. If $f : A \rightarrow B$ and $X, Y \subseteq A$ then

- $f[A \cup B] = f[A] \cup f[B]$
- $f[A \cap B] \subseteq f[A] \cap f[B]$

We won't prove these, but you should prove them on your own for practice.

1.2 Injections

Consider the following application for functions: A and B are sets of codewords, and $f : A \rightarrow B$ is a channel that is used to communicate between two people. f sends messages with codes from A through the channel to the other person, who reads the codewords in B .

Question 1. Why might this be a bad thing?

Answer 1. Well, if two code words in A get sent to the same codeword of B , then person two will not be able to always discern what codeword was actually sent along the channel.

This leads us to our first property of a function, which is called **injectivity**. A function is injective, essentially, when it is an encoding of elements from the domain into elements of the codomain, with the restriction that value encoded is recoverable.

Another, perhaps simpler way to say it, is two values in the domain do not get sent to the same place in the codomain.

Definition 1. $f : A \rightarrow B$ is **injective** or **1-1** iff

$$\forall x, y \in A \cdot x \neq y \rightarrow f(x) \neq f(y)$$

or, alternatively, by looking at the contrapositive

$$\forall x, y \in A \cdot f(x) = f(y) \rightarrow x = y$$

Question 2. Can you think of an alternative definition for injective using preimages?

Answer 2. $\forall y \in B \cdot f^{-1}[\{y\}]$ either has 0 or 1 element in it, or, perhaps better, $\forall y \in f[A] \cdot f^{-1}[\{y\}]$ is a singleton

Example 1. The prototypical example of a non-injective function is $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$. Here, -1 and 1 get sent to the same point. Therefore, if you know the function outputted 1 , it is impossible to discern whether the input was 1 or -1 .

Another non-example is $\sin(x)$, from $\mathbb{R} \rightarrow \mathbb{R}$. We have that $f(0) = f(2\pi)$. Or, said another way, if you knew the output of the function was 0 it would be impossible to discern what angle was plugged in.

Remark 2. Injectivity is very much tied to what the domain is. For instance, in the above, if we looked at x^2 with domain \mathbb{R}^+ , or $\sin(x)$ with domain $[-\frac{\pi}{2}, \frac{\pi}{2}]$, they would be injective.

Many functions that we encounter are injective however.

Example 2. Consider the function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by

$$f(n, m) = 2^n(2m + 1) - 1$$

We claim this is an injection. Take $n_1, n_2, m_1, m_2 \in \mathbb{N}$ and suppose $f(n_1, m_1) = f(n_2, m_2)$; want to show that $n_1 = n_2$ and $m_1 = m_2$.

So we have

$$2^{n_1}(2m_1 + 1) - 2^{n_2}(2m_2 + 1) = 0$$

Suppose that $n_1 \neq n_2$. Without loss of generality, $n_2 > n_1$, so

$$2^{n_1}((2m_1 + 1) - 2^{n_2 - n_1}(2m_2 + 1)) = 0$$

The interior of the parenthetical must be 0, so

$$(2m_1 + 1) - 2^{n_2 - n_1}(2m_2 + 1) = 0$$

If $n_2 - n_1 > 0$ then the left part of the difference is even, and thus the difference will be odd, which cannot happen as it is 0. Thus $n_2 - n_1 = 0$, and so $n_2 = n_1$.

Thus we have $n_1 = n_2$. Now we need only show that $m_1 = m_2$. We now have:

$$2^{n_1}(2m_1 + 1) = 2^{n_1}(2m_2 + 1)$$

This is just as true over the rationals over the integers, so we may divide by 2^{n_1} , subtract one, and then divide by 2. What we are left with is $m_1 = m_2$.

1.3 Surjection

Let's say that we are in the same example as above with A and B being codewords, f being some channel, and one person communicating to another through f . Let's imagine that the receiver of the message wants to send a message along this channel. It would be bad if he had codewords that have no translation in A .

Said a little bit differently, it would be bad if an English-Spanish dictionary did not contain all the Spanish words that one would expect to hear, since the dictionary should act as both a way to translate into Spanish, but also out of Spanish.

This leads us to our next property of a function, which is **surjectivity**. A function is surjective when it actually hits everything in its codomain.

Definition 2. A function $f : A \rightarrow B$ is **surjective** or **onto** iff

$$\forall y \in B. \exists x \in A. f(x) = y$$

Question 3. Can you think of an alternative definition for surjective using images?

Answer 3. $\text{im}(f) = \text{cod}(f)$.

Example 3. One again, the first example usually given of a non-surjective function is $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$ is not surjective. The reason being that -1 is never actually hit by the function; so if you were trying to code -1 to communicate it along the channel of f as the message receiver, you'd have serious trouble.

The other example I gave above of $\sin(x)$ from $\mathbb{R} \rightarrow \mathbb{R}$ is also not surjective. 2 is not struck by $\sin(x)$ but it is in the codomain.

Remark 3. Surjectivity is very much tied to what the codomain is. For instance, in the above, if we looked at x^2 with codomain \mathbb{R}^+ , or $\sin(x)$ with codomain $[-1, 1]$ they would be surjective.

Example 4. Consider $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ by $[x]_4 \mapsto [x]_2$. You can check this is well defined. We claim that it is surjective. As $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ we need only show both of these get hit, and they certainly do, by $[0]_4$ and $[1]_4$.

This is not injective. $f([1]_4) = f([3]_4) = [1]_2$.

Example 5. Consider $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$ by $g(x, y) = x - y$. We claim this is surjective. Take an arbitrary $n \in \mathbb{Z}$. If $n \geq 0$ then n is natural, so then $g(n, 0) = n - 0 = n$, so n gets hit. Otherwise, $n < 0$. Then $-n$ is natural, so then $g(0, -n) = 0 - (-n) = n$, so n gets hit

This is not injective. $g(1, 1) = g(2, 2) = 0$.

Example 6. Let P be the set of functions \mathbb{R} to \mathbb{R} which are polynomials (what do you suppose this set looks like?). Define the function $D : P \rightarrow P$, defined by $f \mapsto f'$, that is a polynomial maps to its derivative. This is surjective but not injective. Can you see why?

Example 7. Let A be a nonempty set. Consider $f : A \rightarrow \wp(A)$ by $x \mapsto \{x\}$. This is injective. Take $a, b \in A$, and suppose that $f(a) = f(b)$. Then $\{a\} = \{b\}$. But, this means everything in the left is in the right; as a is in the left, it is in the right. As only b is in the right, $a = b$.

This is not surjective. What set in the codomain surely doesn't get hit?

Example 8. Consider the function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by

$$f(n, m) = 2^n(2m + 1) - 1$$

. We claim this is a surjection. To show surjective, we are trying to show that every $x \in \mathbb{N}$, there is some $(n, m) \in \mathbb{N} \times \mathbb{N}$ such that $f(n, m) = x$. We prove this by induction.

If $x = 0$, then we can set $(n, m) = (0, 0)$ and this works.

$x \in \mathbb{N}$, $x > 0$, and assume that for all $y < x$ we know that y is hit by f . So for every $y < x$ we get some n_y and m_y such that $f(n_y, m_y) = y$.

We do cases on whether x is even or odd.

If x is even, then $x = 2y$ for some $y \in \mathbb{N}$. Then $f(0, y) = 2^0(2y + 1) - 1 = 2y = x$.

If x is odd, then $x = 2y + 1$ for some $y \in \mathbb{N}$. By induction hypothesis, $f(n_y, m_y) = y$ as $y < x$.

Scratch work:

$$y = 2^{n_y}(2m_y + 1) - 1$$

$$2y = 2^{n_y+1}(2m_y + 1) - 2$$

$$2y + 1 = 2^{n_y+1}(2m_y + 1) - 1$$

We claim that $f(n_y + 1, m_y)$ works. Well,

$$\begin{aligned} f(n_y + 1, m_y) &= 2^{n_y+1}(2m_y + 1) - 1 \\ &= 2^{n_y+1}(2m_y + 1) - 2 + 1 \\ &= 2(2^{n_y}(2m_y + 1) - 1) + 1 \\ &= 2y + 1 \end{aligned}$$

1.4 Composition

Thinking of $f : A \rightarrow B$ and $g : C \rightarrow D$ as machines, we might want to compute what f does to some A , and then feed the result of this computation directly to g . But, of course, this isn't always possible. It might be possible of course that f 's output would be bananas, and g 's inputs would be coconuts. In this case, it's not possible to send in f 's outputs to g .

Definition 3. If $f : A \rightarrow B$ and $g : C \rightarrow D$ and $B \subseteq C$ then the g **composed with** f is

$$g \circ f : A \rightarrow D$$

And this is defined by

$$(g \circ f)(x) = g(f(x))$$

Remark 4. The order of composition (whether it is $f \circ g$ or $g \circ f$) is a little contentious. It used to be moreso. Currently, in almost all branches of math and applications this is the way that composition is done. The contention nowadays usually lies in should function application be a “rightward” action, or a “leftward” action. We won’t make a fuss about this, but you might see it come up, especially in an algebra course.

Usually, you can tell by context which it is anyway as the codomain of the function you perform first must be a subset of the domain of the second.

To remember which order $g \circ f$ is, you should pronounce it in one of the following way:

- g following f of ...
- first f then g of ...

Example 9. We are very well acquainted with compositions already. For instance, Consider $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$, and $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = \sin(x)$. Then we can ask for $f \circ g$, which is “first do g then do f ,” so it would be

$$f \circ g = (\sin(x))^2$$

Which is (regrettably) usually written $\sin^2(x)$. Other composition the other way however is $g \circ f$ which is “first do f then do g ,” so it would be

$$g \circ f = \sin(x^2)$$

We can see then that function composition is not commutative.

Remark 5. Function composition is associative!

$$f \circ (g \circ h) = (f \circ g) \circ h$$

This is a completely trivial fact if one thinks about what it means, but it’s importance is often overlooked. It’s one of those things that is trivial when thought about, but really this is a truly beautiful thing that occurs in mathematics.

Theorem 5. Let $f : A \rightarrow A$. Then the following are equivalent:

- (a) f surjective.
- (b) $f \circ f$ is surjective.

Proof. ((a) \implies (b)) Suppose that f is surjective. Want to show that $f \circ f$ is surjective. Well, To do this, we take $a \in A$, and want to find a $b \in A$ such that $f(f(b)) = a$. Well, we know, as f is surjective we know there is some $c \in A$ such that $f(c) = a$. Moreover, we know there is some $b \in B$ such that $f(b) = c$. Therefore, $f(f(b)) = f(c) = a$.

((b) \implies (a)) suppose that $f \circ f$ is surjective. We want to show that f is surjective. So, take $a \in A$, and we want to find a $b \in A$ such that $f(b) = a$. Well, Well, we $f \circ f$ is surjective, we can find a $c \in B$ such that $f(f(c)) = a$. Then, letting $b = f(c)$, we see that $f(f(c)) = f(b) = a$. \square