Proofs with Functions

Margaret M. Fleck

23 Feb 2009

Written up versions of proofs similar to those in lecture 15.

1 Recap

Recall that a function $f : A \rightarrow B$ is one-to-one (injective) if

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

and it is onto (surjective) if

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

A function that is both one-to-one and onto is called a *bijection* or a *one-to-one correspondence.*

Bijective functions are special for a variety of reasons, including the fact that every bijection f has an inverse function f^{-1}.

2 Proving that a function is one-to-one

Claim 1 *Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by $f(x) = 3x + 7$. f is one-to-one.*

Let's prove this using our definition of one-to-one.

> Proof: We need to show that for every integers x and y, $f(x) = f(y) \rightarrow x = y$.
>
> So, let x and y be integers and suppose that $f(x) = f(y)$. We need to show that $x = y$.

> We know that $f(x) = f(y)$. So, substituting in our formula for f, $3x + 7 = 3y + 7$. So $3x = 3y$ and therefore $x = y$, by high school algebra. This is what we needed to show.

When we pick x and y at the start of the proof, notice that we haven't specified whether they are the same number or not. Mathematical convention leaves this vague, unlike normal English where the same statement would strongly suggest that they were different.

You may have encountered the abbreviation QED at the end of a proof. This stands for "quod erat demonstrandum" which is simply the Latin for "this is what we needed to show." Some people put a little box or a little triangle of 3 dots at the end of the proof. It's good style to have something at the end of your proof which tells the reader that the proof is complete.

3 Proving that a function is onto

Now, consider this claim:

Claim 2 *Define the function g from the integers to the integers by the formula $g(x) = x - 8$. g is onto.*

> Proof: We need to show that for every integer y, there is an integer x such that $g(x) = y$.
>
> So, let y be some arbitrary integer. Choose x to be $(y + 8)$. x is an integer, since it's the sum of two integers. But then $g(x) = (y + 8) - 8 = y$, so we've found the required pre-image for y and our proof is done.

Notice that our function f from the last section wasn't onto. Suppose we tried to build a proof that it was.

> Proof: We need to show that for every integer y, there is an integer x such that $f(x) = y$.
>
> So, let y be some arbitrary integer. Choose x to be $\frac{(y-7)}{3}$. ...

If f was a function from the reals to the reals, we'd be ok at this point, because x would be a good pre-image for y. However, f's inputs are declared to be integers. For many values of y, $\frac{(y-7)}{3}$ isn't an integer. So it won't work as an input value for f.

4 Composing two functions

Suppose that $f : A \to B$ and $g : B \to C$ are functions. Then $g \circ f$ is the function from A to C defined by $(g \circ f)(x) = g(f(x))$. Depending on the author, this is either called the composition of f and g or the composition of g and f. The idea is that you take input values from A, run them through f, and then run the result of that through g to get the final output value.

Take-home message: when using function composition, look at the author's shorthand notation rather than their mathematical English, to be clear on which function gets applied first.

In this definition, notice that g came first in $(g \circ f)(x)$ and g also comes first in $g(f(x))$. I.e. unlike $f(g(x))$ where f comes first. The trick for remembering this definition is to remember that f and g are in the same order on the two sides of the defining equation.

For example, if we use our functions f and g defined above, the domains and co-domains of both functions are the integers. So we can compose the two functions in both orders.

$$(f \circ g)(x) = f(g(x)) = 3g(x) + 7 = 3(x - 8) + 7 = 3x - 24 + 7 = 3x - 17$$

$$(g \circ f)(x) = g(f(x)) = f(x) - 8 = (3x + 7) - 8 = 3x - 1$$

Notice that the order matters to the output value!

Frequently, the declared domains and co-domains of the two functions aren't all the same, so often you can only compose in one order. For example, consider the function $h : \{strings\} \to \mathbb{Z}$ which maps a string x onto its length in characters. (E.g. $h(\text{Margaret}) = 8$.) Then $f \circ h$ exists but $(h \circ f)$ doesn't exist because f produces numbers and the inputs to h are supposed to be strings.

5 A proof involving composition

Consider this claim:

Claim 3 *For any sets A, B, and C and for any functions $f : A \to B$ and $g : B \to C$, if f and g are injective, then $g \circ f$ is also injective.*

We can prove this with a direct proof, by being systematic about using our definitions and standard proof outlines. First, let's pick some representative objects of the right types and assume everything in our hypothesis.

> Proof: Let A, B, and C be sets. Let $f : A \to B$ and $g : B \to C$ be functions. Suppose that f and g are injective.
>
> We need to show that $g \circ f$ is injective.

To show that $g \circ f$ is injective, we need to pick two elements x and y in its domain, assume that their output values are equal, and then show that x and y must themselves be equal. Let's splice this into our draft proof. Remember that the domain of $g \circ f$ is A and its co-domain is C.

> Proof: Let A, B, and C be sets. Let $f : A \to B$ and $g : B \to C$ be functions. Suppose that f and g are injective.
>
> We need to show that $g \circ f$ is injective. So, choose x and y in A and suppose that $(g \circ f)(x) = (g \circ f)(y)$
>
> We need to show that $x = y$.

Now, we need to apply the definition of function composition and the fact that f and g are each injective:

> Proof: Let A, B, and C be sets. Let $f : A \to B$ and $g : B \to C$ be functions. Suppose that f and g are injective.
>
> We need to show that $g \circ f$ is injective. So, choose x and y in A and suppose that $(g \circ f)(x) = (g \circ f)(y)$
>
> Using the definition of function composition, we can rewrite this as $g(f(x)) = g(f(y))$. Combining this with the fact that g is injective, we find that $f(x) = f(y)$. But, since f is injective, this implies that $x = y$, which is what we needed to show.