20200113

Another example of **P**roof by **M**inimal **C**ounter **E**xample:

Claim: Every integer ≥ 7 can be written as $2a + 3b$ where a and b are positive integers

PMCE: Suppose the claim is not true. Let k be the smallest integer such that $k \geq 7$ and k ***cannot*** be written as $2a + 3b$ where a and b are positive integers. (i.e. k is the minimum counter-example.) This means all integers x where $7 \leq x < k$ ***can*** be written as $2a + 3b$

In this proof we will begin by showing that k cannot be 7 or 8

We see that 7 = 2*2 + 3*1, so k $\neq$ 7

We see that 8 = 2*1 + 3*2, so k $\neq$ 8

Thus k $\geq$ 9

Since k $\geq$ 9, k-2 $\geq$ 7 ..... so 7 $\leq$ k-2 < k

Since k is the minimum counter-example, k-2 is **not** a counter-example.

Thus $k - 2 = 2 * x + 3 * y$ for some positive integers x and y

But that means $k = 2(x + 1) + 3y$, so k is not a counter-example at all $\otimes$

Therefore the claim is true.

This proof may elicit a "where did that come from?" reaction ... it seems like there is no motivation for establishing that $k \geq 9$, and even less reason for looking at $k - 2$. Let me try to fill in a bit of the thinking that goes on here.

We can start by looking at the thing we are trying to prove, and how we might attack it. Remember, in PMCE we are going to have two things to work with:

- the claim is **false** for the minimum counter-example k
- the claim is **true** for all members of the set that are < k

and from these we will create a contradiction.

We are trying to prove that every integer ≥ 7 can be written as $2a + 3b$, and we know that we are going to be supposing the existence of a minimum counter-example k. We can guess that our contradiction is going to be that the (supposed) minimum counter-example k is not a counter-example at all (this is very often the contradiction that we reach). We will probably do this by finding a way to write k as $k = 2x + 3y$ for some positive integers x and y. We will also be using the knowledge that since k is the **minimum** counter-example, each value $< k$ in the set can be written as $.2a + 3b$ for some positive integers a and b

So we ask "How can we use the information that numbers $< k$ can be written as $2a + 3b$ to show that k can also be written in this way?" The numbers that are $< k$ are $k - 1, k - 2, k - 3$ etc.

Let's think about $k - 1$ We know it can be written as $k - 1 = 2a + 3b$ for some positive integers a and b. This gives us $k = 2a + 3b + 1$ ..... but that looks like a dead end. There's no easy way to get rid of the $+1$.

So now we might try thinking about $k - 2$. We know $k - 2 = 2a + 3b$ for some positive integers a and b (we know this because $k - 2$ is not a counterexample). This gives us $k = 2a + 3b + 2$ .... which is great because we can rewrite it as $k = 2(a + 1) + 3b$.

Now we are onto something. If we can be sure that $k - 2$ can be written as $k - 2 = 2a + 3b$, then k is not a counter-example.

But remember, we need $k - 2$ to be a member of the set we are dealing with, and that set starts at 7. So we need $k - 2 \geq 7$ ..... which means k ≥ 9. This means that our logic about relating k to $k - 2$ can only be applied for values ≥ 9. For the values in the set that are < 9 (ie 7 and 8) we need to prove that they can be written as $2a + 3b$ in some other way. Fortunately, it is easy to prove these facts directly: 7 = 2*2 + 3*1 and 8 = 2*1 + 3*2

Now let's revisit the proof and annotate it.

Claim : all integers ≥ 7 can be written as $2a + 3b$ where a and b are positive integers.

PMCE: Assume k is the minimal counter-example (*applying the well-ordering principle*)

7 = 2*2 + 3*1 and 8 = 2*1 + 3*2 (*direct proof of the claim for these small values*)

$\Rightarrow k \geq 9$ (*establishing the least possible value for k*)

$\Rightarrow k - 2 \geq 7$ (*establishing that k-2 is in the set*)

$\Rightarrow k - 2 = 2a + 3b$ for some a and b (*because k is the* ***minimum*** *counter-example*)

$\Rightarrow k = 2(a + 1) + 3b$

$\Rightarrow k$ is not a counter-example $\otimes$

Thus the assumption that the claim is false has led to a contradiction.

$\therefore$ the claim is true

<Is this theorem really interesting? Who cares that we can write almost all positive integers as $2a + 3b$ for some positive integers a and b? Well, it turns out that this type of result is important in robotics. Some machines have limits on their movement, due to the way they are constructed. We can certainly imagine a robot that can take a step of length 2, or a step of length 3, but no other length of step. This theorem proves that the robot can move forward any exact distance ≥ 7 with some combination of 2-steps and 3-steps.

Note that the problem changes if we allow a and b to possibly have the value 0 – this might be more realistic for the robot application.>

PMCE is a form of Proof by Contradiction, but it is also very closely related to Proof by Induction. In both PMCE and PBI we use the assumption that the claim is true for small values to prove that it is also true for large values.

I often find that PMCE is easier than PBI because it actually gives us more to work with: we have the knowledge that the claim is true up to $k - 1$ (which is what we have in PBI) and we also have the assumption that the claim is false for k (which is not usually part of PBI). Putting those things together to find a contradiction is often easier than constructing an inductive proof that the claim is true for k.

However, it is a matter of choice. Both proof techniques are valid – you should become comfortable with both. You will eventually find your own preference.

Exercises:

1. Use PMCE to prove that all integers ≥ 11 can be written as $2a + 5b$ where a and b are positive integers

2. Use PMCE to prove that all integers ≥ 29 can be written as $4a + 7b$ where a and b are positive integers.

3. Based on the proof we worked out above and the previous 2 exercises, what you think is the largest integer that ***cannot*** be written as $3a + 4b$ where a and b are positive integers? Prove that your answer is correct.

4. Using the definition of even integers (an integer x is **even** if it can be written as $x = 2k$ where k is an integer) and the definition of odd integers (an integer x is **odd** if it can be written as $x = 2k + 1$ where k is an integer), use PMCE to prove that every element of $\mathbb{N}$ is either even or odd.

Function Composition

We reviewed the concept of **function composition**.

Let f : A $\rightarrow$ B and g : B $\rightarrow$ C be functions (ie. f is a function from set A to set B, and g is a function from set B to set C) then we write the **composition of g and f as g $\circ$ f .** g $\circ$ f is a function from A to C (in notation g $\circ$ f : A $\rightarrow$ C) such that $\forall$ a $\in$ A, (g $\circ$ f) (a) = g(f(a))

In plain English, when we see **g $\circ$ f** we just have to remember that it means, "apply f, then apply g to the result of that". The key thing to remember is that the first function we apply is the last one listed.

Example : let $f : \mathbb{N} \rightarrow \mathbb{N}$ be defined by $f(x) = x + 3$ and let $g : \mathbb{N} \rightarrow \mathbb{N}$ be defined by $g(x) = 2x$

Consider **g $\circ$ f (5).** We know this is equivalent to $g(f(5))$. Since $f(5) = 5 + 3 = 8$, our answer is $g(8)$, which is 16. But now consider f $\circ$ g(5) ... this equals $f(g(5))$, which is $f(10)$ ... so the answer is 13. This demonstrates that **g $\circ$ f** and **f $\circ$ g** are not the same.

Note that when g $\circ$ f is well-defined, f $\circ$ g may not be defined at all. To compose two functions, the "target set" of the first one we apply must match the "input set" of the second one we apply.

Here's an example: A = {1,2,3}, B = {Kingston, Ottawa, Beijing, Damascus}, C = {bananas, strawberries, oranges, grapes} Now we can create a function $f : A \rightarrow B$ and a function $g : B \rightarrow C$ (the details of the functions are not important) and we know we can compose g with f – that is, we know $g \circ f$ is well-defined. f takes any element of A as input and returns an element of B, and then g takes that element of B and returns an element of C. It makes perfect sense to think of $g \circ f$ as a function that maps A to C. We can write $(g \circ f) : A \rightarrow C$. However $f \circ g$ is not defined, since g produces elements of C as output, and f can only be applied to elements of A.

Let's expand on this idea a bit. Suppose we have two sets A and B, and two functions $f : A \rightarrow B$ and $g : B \rightarrow A$. Now we are guaranteed that $f \circ g$ and $g \circ f$ are both well-defined. We can write $(f \circ g) : B \rightarrow B$ and $(g \circ f) : A \rightarrow A$. Make sure you understand why this is true.

And one step further. Let A be a set and let f be a function $f : A \rightarrow A$. It should be clear that $f \circ f$ is also a function from A to A ... and it is reasonable to write $f \circ f$ as f^2

To illustrate this, consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x - 1$

Then

$$f^2(x) = (f \circ f)(x) = f(f(x)) = f(2x - 1) = 2(2x - 1) - 1 = 4x - 3$$

In the same way, we can define $f^3(x) = (f \circ f \circ f)(x) = f(f(f(x))) = 8x - 7$ and so on.

Exercise: prove that $f^i(x) = 2^i x - (2^i - 1) \quad \forall i \geq 1$

By this point it should be clear that composition gives us a way to combine functions to create new functions, and it is similar in some ways – and different in some ways – to the way that we use arithmetic operations to combine numbers to create new numbers. It may seem restrictive that there exist functions that cannot be composed with each other, but this is actually an indication that the set of all functions is more complex than the set of all numbers.

The idea of using $f^i(x)$ to represent the operation of composing a function with itself might make us wonder if we can extend this notation to using non-positive integers for i. For example, can we come up with a meaningful definition for $f^0(x)$? What about $f^{-1}(x)$ or $f^{-2}(x)$? It turns out that sometimes we can … as we will see when we start to study the class of functions called permutations.