Math 2150 Notes - July 11, 2022

Today we venture into proofs, which will take up the second half of the summer term. You have all solved calculus and algebra problems, often getting a numerical or algebraic "answer.". Now the focus will shift dramatically. Instead of "getting an answer", we will be interested in **why** the mathematics works the way it does. This involves writing *proofs* of mathematical statements, which are logical arguments given in English which should convince the reader (sufficiently well-versed in logic and mathematics) that what you assert is, in fact, true. The first type of proof I will introduce is that of *direct proof*; we given the general idea below.

Definition 1 (Direct Proof)**.** *To prove a statement of the form* $\forall x_1 \forall x_2 \cdots \forall x_n (P(x_1, x_2, \ldots, x_n) \to Q(x_1, x_2, \ldots, x_n))$ *directly, do the following:*

1. *Let* $x_1, x_2, \ldots, x_n$ *be arbitrary members of their respective domains,*
2. *assume that* $P(x_1, \ldots, x_n)$ *is true, and then*
3. *deduce that* $Q(x_1, \ldots, x_n)$ *must be true as well.*

A word about why this works. The first step follows what I've said previous in predicate logic: when given a sequence of universally quantified variables, let them be arbitrary, and then ask (even though you don't know what the values actually are) if what follows is necessarily true. Now, suppose that you have completed steps 2. and 3. above. Then it cannot be that $P(x_1, x_2, \ldots, x_n)$ is true and $Q(x_1, x_2, \ldots, x_n)$ is false, since we have shown that assuming that $P(x_1, \ldots, x_n)$ to be true, then $Q(x_1, \ldots, x_n)$ **must** also be true. In other words, $(P(x_1, x_2 \cdots, x_n) \to Q(x_1, x_2, \ldots, x_n))$ is true. Because $x_1, x_2, \ldots, x_n$ were arbitrary, it follows that $\forall x_1 \forall x_2 \cdots \forall x_n (P(x_1, x_2, \ldots, x_n) \to Q(x_1, x_2, \ldots, x_n))$ is also true.

So now that we have this technique, let's look at a couple of examples. First, we introduce some definitions.

Definition 2. *The set* $\{, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ *is the set of* ***integers****. An integer* x *is* ***even*** *if* $x = 2n$ *for some integer* n*;* x *is* ***odd*** *if* $x = 2m + 1$ *for some integer* m*.*

We are almost ready to do a proof. But first, we state some assumptions we will make in proofs without justification; this should become clear shortly. We will add to our list of assumptions as we uncover more mathematics.

Assumptions

1. basic algebra[1]
2. the sum, difference, product, and negatives of integers are integers,
3. every integer is either even or odd,
4. no integer is both even and odd,
5. $1 \neq 0$,
6. for all real numbers a, b, and c: if $a < b$, then $a + c < b + c$,
7. for all real numbers a, b, and c: if $a < b$ and $c > 0$, then $ac < bc$,
8. for all real numbers a, b, and c: if $a < b$ and $b < c$, then $a < c$, and
9. for all real numbers a, b, and c: exactly one of $a = b$, $a < b$, $b < a$ holds.
10. every rational number can be expressed in reduced form.
11. the product of two nonzero real numbers is nonzero.

You will see what I mean by this in the proofs to follow.

Example 1. *Prove that the sum of two even integers is even.*

Before we do the proof, let's do a "preformalization" by converting what we have to prove into a formula (involving some English). This is intended to be somewhat informal, but the purpose is so you can see precisely how to apply steps 1.-3. in Definition 1 above.

$\forall x \forall y((x \text{ is even} \wedge y \text{ is even}) \to x + y \text{ is even})$. [Note that you of course could have used x_1 and x_2 here, but x and y are a bit more natural] Note that the domain for x and the domain for y is the set of all integers. It is VERY important to be able to do the preformalizations correctly, or else you won't know how to proceed through steps 1. - 3. above. So now let's write the proof. Note how I am following steps 1. - 3. above.

Proof. Let x and y be arbitrary integers. Assume that x and y are even. We must show that $x + y$ is even. Since x is even, $x = 2n$ for some integer n; since y is even, $y = 2m$ for some integer m. Hence $x + y = 2n + 2m = 2(n + m)$. By assumption 2., $n + m$ is an integer. Hence $x + y$ is even. □

Remark 1. *A few comments about the above proof. First, note that EVERY LETTER THAT WAS INTRODUCED IN THE PROOF WAS DESCRIBED – FOR EXAMPLE, I DIDN'T JUST WRITE "x" and "y" above; I stated that they were integers. In general, every letter introduced in a proof should be described as above. Also, note the use of COMPLETE SENTENCES. Finally, observe that to be even, it is not enough to merely be $2\cdot$ some number; the "some number" must be an INTEGER. For example, $1 = 2 \cdot \frac{1}{2}$, but 1 is NOT even. This is the reason for justifying that $n + m$ above is an integer: it must be in order for $x + y$ to be even. Lastly, note that we let $x = 2n$ and $y = 2m$; since x and y were picked at random, it's virtually certain that x and y are NOT equal, and this necessitates using the **different** letters m and n (of course, you could have used, say, a and b instead).*

Let's do two more examples.

Example 2. *Prove that the sum of an even integer and an odd integer is odd.*

First, let's preformalize: $\forall x \forall y((x \text{ is even and } y \text{ is odd}) \to x + y \text{ is odd})$. [The domain for x and y is the set of integers]

[1] When you do basic algebra, you need NOT say "by assumption 1."; you can just do it in the course of a proof.

Proof. Let x and y be arbitrary integers. Assume that x is even and y is odd. We must show that $x + y$ is odd. Because x is even and y is odd, $x = 2n$ for some integer n and $y = 2m + 1$ for some integer m. Thus $x + y = 2n + 2m + 1 = 2(n + m) + 1$. By assumption 2, $n + m$ is an integer. Hence $x + y$ is odd. □

Remark 2. *Again, observe that we want to justify that $n + m$ is an* ***integer*** *because the definition of "odd" requires us to be two times an integer plus one.*

Example 3. *Prove that if x is an odd integer, then so is x^2.*

Preformalization: $\forall x(x \text{ is odd} \rightarrow x^2 \text{ is odd})$.

Proof. Let x be an arbitrary integer. Assume that x is odd. We must show that x^2 is odd. Since x is odd, $x = 2n + 1$ for some integer n. Thus $x^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$. It follows from assumption 2 that $2n^2 + 2n$ is an integer, and so x^2 is odd. □

We now introduce a new proof technique - proof by contraposition. We have introduced and studied basic properties of even and odd integers; today, we will introduce the basic order properties on the collection of real numbers. Though I will define the set of real numbers more formally later, the set of real numbers includes all numbers that are not imaginary.

Before introducing the proof technique of contraposition, I'd like to give you an example illustrating a shortcoming of direct proofs. Let's try to prove the statement below using a direct proof:

Example 4. *Prove that for every integer n: if n^2 is even, then n is even.*

Preformalization: $\forall n(n^2 \text{ is even} \rightarrow n \text{ is even})$.

Proof. Let n be an arbitrary integer. Assume that n^2 is even. We most prove that n is even. Since n^2 is even, $n^2 = 2k$ for some integer k. Taking the square root of both sides, $|n| = \sqrt{2k}$. But this is about as far as we can get. Remember that we want for n to have the form $2m$ for some integer m. As of now, there's no obvious way for us to get there, and so we appear to be stuck... □

But there is a way out, and the way out is to use a new proof technique called *proof by contraposition*. Before I introduce this technique, I want to remind you that the **contrapositive** of $(p \rightarrow q)$ if $((\neg q) \rightarrow (\neg p))$. The important fact about the contrapositive is that it is logically equivalent to the original if-then statement $(p \rightarrow q)$ (we established this via a truth table back in propositional logic). Because of this logical equivalence, if you know that a statement of the form $((\neg q) \rightarrow (\neg p))$ is true, then it automatically follows that $(p \rightarrow q)$ is true. Now let's formally introduce the technique.

Definition 3 (Proof by Contraposition)**.** *To prove a statement of the form $\forall x_1 \forall x_2 \cdots \forall x_n(P(x_1, x_2, \ldots, x_n) \rightarrow Q(x_1, x_2, \ldots, x_n))$ by contraposition, do the following:*

1. *Let $x_1, x_2, \ldots, x_n$ be arbitrary members of their respective domains,*
2. *assume that $(\neg Q(x_1, \ldots, x_n))$ is true, and then*
3. *deduce that $(\neg P(x_1, \ldots, x_n))$ must be true as well.*

Let's now revisit the previous example above, but with this technique in hand. NOTICE THAT I'VE ADDED SOME ITEMS TO THE ASSUMPTIONS LIST.

Example 5. *Prove that for every integer n: if n^2 is even, then n is even.*

Preformalization: $\forall n(n^2 \text{ is even} \rightarrow n \text{ is even})$

Proof. Let n be an arbitrary integer. Assume that n is not even (note that this is the "not q"). We must show that n^2 is not even (this is the "not p"). By assumption (3), since n is not even, n is odd. Thus $n = 2k+1$ for some integer k. Squaring both sides, $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. By assumption (2), $2k^2 + 2k$ is an integer, and hence n^2 is odd. By assumption (4), we see that n^2 is not even, concluding the proof. □

Next, I will introduce the basic properties of the usual order $<$ on the real line (these have also been added to our list of assumptions). IN ANY HOMEWORK PROBLEMS, PLEASE REFER TO THE NUMBERS IN THE ASSUMPTION LIST IN YOUR PROOFS, AND NOT TO THE LETTERS BELOW.

(a) $1 \neq 0$,

(b) for all real numbers a, b, and c: if $a < b$, then $a + c < b + c$,

(c) for all real numbers a, b, and c: if $a < b$ and $c > 0$, then $ac < bc$,

(d) for all real numbers a, b, and c: if $a < b$ and $b < c$, then $a < c$, and

(e) for all real numbers a and b: exactly one of $a = b$, $a < b$, $b < a$ holds.

Before proving the next example, recall that, for real numbers x and y, $x > y$ means $y < x$.

Example 6. *Prove that for all real numbers a, b, and c: if $a < b$ and $c < 0$, then $ac > bc$.*

Preformalization: $\forall a \forall b \forall c((a < b \wedge c < 0) \rightarrow ac > bc)$. We will use a direct proof this time. Notice how I'm following the algorithm I've given you for doing a direct proof.

Proof. Let a, b, and c be arbitrary real numbers. Assume that $a < b$ and that $c < 0$. We must prove that $ac > bc$. By assumption (6) ((b) above), $c + -c < 0 + -c$, that is $0 < -c$. But this means that $-c > 0$. Now by assumption (7) (assumption (c) above), we see that $a(-c) < b(-c)$, that is, $-ac < -bc$. Applying assumption (6) again ((b) above, we may add $ac + bc$ to both sides of $-ac < -bc$ to get $bc < ac$. But this means that $ac > bc$, and this was what we had to show. □

Next, for real numbers x and y, we define $x \leq y$ to mean "$x < y$ or $x = y$" and $x \geq y$ to mean "$x > y$ or $x = y$". We will use another proof by contraposition for our final example.

Example 7. *For all real numbers a, b, and c: if $a \leq b$, then $a + c \leq b + c$.*

Preformalization: $\forall a \forall b \forall c(a \leq b \rightarrow a + c \leq b + c)$.

Proof. Let a, b, and c be arbitrary real numbers. Assume it is not the case that $a + c \leq b + c$. We must show that it is false that $a \leq b$. Since it is false that $a + c \leq b + c$, it is false that either $a + c < b + c$ or $a + c = b + c$. By assumption (9) above ((e) above), we deduce that $b + c < a + c$. Recall that we must show that it is false that $a \leq b$. Again, by assumption (9) above, this is equivalent to showing that $b < a$. By assumption (6) ((b) above), we may add $-c$ to both sides of $b + c < a + c$ above to obtain $b < a$, and this is what we wanted to show. □