Day 6

Tuesday May 29, 2012

1 Basic Proofs

We continue our look at basic proofs. We will do a few examples of different methods of proving.

1.1 Proof Techniques

Recall that so far in class we have made two main distinctions: indirect and direct proofs. We've been using the "law of the excluded middle" frequently too. Now, we will never make explicit mention to this.

But, we still make a distinction between direct and indirect proofs. Direct proofs have the following characteristics:

- If you are proving an implication, you assume the hypotheses and prove the conclusion.
- If you are proving a universal statement, you take an arbitrary element in the domain of discourse, and prove the statement for that element.
- If you are proving an existential statement, you prove a the statement for a specific element of the domain of discourse.

Often, direct proofs are hard to do, and it's much easier to do indirect methods. There are two main indirect methods.

- Proof by Contraposition: If you are proving an implication, assume the negation of the conclusion and prove the negation of the hypotheses.
- Proof by Contradiction: You assume the negation of the statement you want to show, and derive a contradiction.

Question 1. I claim that any proof by contraposition can be rephrased into a proof by contradiction; why?

Answer 1. Well, say the statement is $A \to B$. You begin with assuming A, and you want to prove B. By contradiction, you assume $\neg B$ and then aim for a contradiction.

Compare this with how you would do a proof by contraposition. You would assume $\neg B$, and aim for $\neg A$.

If you could prove $\neg A$ just from $\neg B$, then that would also yield a contradiction in the proof by contradiction, since you are assuming A.

So, in a matter of speaking, you might as well do a proof by contradiction if you are going to do a proof by contraposition. This is actually many proofs by contraposition are found; you begin with a proof by contradiction, and then after you are done you realize you never use the assumption of A, so the proof is rewritten.

1.1.1 Direct Proof Examples

Question 2. Write a formula $\psi(x, y)$ such that for a given n and m integers, $\psi(n, m)$ is true if and only if n divides m.

Answer 2.

$$\psi(x, y) := \exists z \in \mathbb{Z} \,.\, m = z \cdot n$$

Example 1.

$$\exists m \in \mathbb{Z} \,.\, \forall n \in \mathbb{Z} \,.\, m \text{ divides } n$$

Proof. Let $m = 1$. Then let n be an arbitrary integer. Well,

$$n = 1 \cdot n = m \cdot n$$

So 1 divides n. □

Example 2.

$$\forall n \in \mathbb{Z} \,.\, \forall m \in \mathbb{Z} \,.\, (n \text{ divides } m) \to (\forall z \in \mathbb{Z} \,.\, (z \text{ divides } n) \to (z \text{ divides } m))$$

Proof. Let n and m be arbitrary integers, where n divides m. Let z be an arbitrary integer where z divides n.

As n divides m, we can find an integer a such that $m = a \cdot n$. Similarly, we can find b such that $n = b \cdot z$ as z divides n.

Doing a substitution, we see $m = a \cdot (b \cdot z)$, or

$$m = (ab) \cdot z$$

So z divides m. □

Question 3. Write a formula $\varphi(x)$ such that for a given integer n, $\varphi(n)$ is true if and only if n is an even number.

Answer 3.

$$\varphi(x) := \exists m \in \mathbb{Z} \,.\, x = 2 \cdot m$$

Example 3.

$$\forall n \in \mathbb{Z} \,.\, n(n+1) \text{ is even}$$

Proof. Let n be an arbitrary natural number. We can do cases on whether n itself is even.

Case 1: n is even.

Then $n(n+1)$ is even, since an even times an odd is even. Or, just using the definition of even, since n is even we can find an m such that $n = 2m$. Thus, $n(n+1) = 2(m(n+1))$, which is clearly even.

Case 2: n is odd

Then $n+1$ is even, and so $n(n+1)$ is even since an even times an odd is even. Or, just using the definition, since $n+1$ is even we can find m such that $n+1 = 2m$. thus $n(n+1) = 2(mn)$, which is clearly even. □

1.1.2 Contradiction Examples

Question 4. How would you define $\varphi(x)$ to be such that for any real number y, if y is rational then $\varphi(y)$ holds.

Answer 4.

$$\exists m \in \mathbb{Z} \,.\, \exists n \in \mathbb{Z} \,.\, (m \neq 0) \wedge \left(\frac{n}{m} = x\right)$$

Example 4.

$$\exists y \in \mathbb{R} \,.\, \neg(y \text{ is rational})$$

Proof. More specifically, we will prove $\sqrt{2}$ is irrational.

For contradiction, suppose that $\sqrt{2}$ was rational. Then we can take witnesses m and n integers, $m \neq 0$ such that $\frac{n}{m} = \sqrt{2}$. Multiplying both sides by m and squaring both sides, we have:

$$n^2 = 2m^2$$

Without loss of generality, we can assume that m and n have no common factors, ie. we wrote $\sqrt{2}$ as a reduced fraction. Note that n^2 is even. By a homework problem, we know that n is also even. By the definition of even, we can find a n' such that $n = 2n'$. Therefore,

$$(2n')^2 = 2m^2$$

ie. $4(n')^2 = 2m^2$. Dividing both sides by 2, we have

$$2(n')^2 = m^2$$

But, then m is also divisible by 2. So, m and n are both divisble by 2, which contradicts $\frac{n}{m}$ being a fully reduced fraction. □

1.1.3 Contrapositive Examples

We have already seen two:

- $\forall x, y \in \mathbb{R} \,.\, (x \geq y) \rightarrow \left(\sqrt{x} \geq \sqrt{y}\right)$
- $\forall n \in \mathbb{Z} \,.\, n^2$ is even $\rightarrow n$ is even

Proofs by contrapositive are useful when the negation of the conclusion is “easier to work with” than the hypotheses themselves. For instance

Example 5.

$$\forall n, m \in \mathbb{N} \,.\, (n + 1 \neq m + 1) \rightarrow (n \neq m)$$

Proof. Notice, the assumption $n + 1 \neq m + 1$ is odd to work with, because we're not used to doing algebra on non-equalities.

First, we take n, m in the naturals arbitrary, and then we proceed by contraposition. As a clue to our reader, this is what I would say:

For sake of proving the contrapositive, assume $n = m$ and we aim to prove that $n + 1 = m + 1$.

This statement tells the reader your assumption, and your goal.

Now, when we have $n = m$, we can just add 1 to both sides and be done! □

1.1.4 Exhaustion Examples

A **proof by exhaustion** is a proof by cases. It's also called a **brute force** proof. The idea is: extra assumptions are good. The easiest way to get extra assumptions is the partition all possibilities into different cases which give us more specific information. We've already seen some proofs by cases.

Example 6. The Triangle Inequality:

$$\forall x, y \in \mathbb{R} \,.\, |x + y| \leq |x| + |y|$$

Proof. We did cases on where $x + y \geq 0$ and $x + y < 0$. □

Example 7.

$$\exists x \,.\, \exists y \,.\, \neg(x \text{ is rational}) \wedge \neg(y \text{ is rational}) \wedge (x^y \text{ is rational})$$

Proof. Here we do a proof by cases. First, note above we proved that $\sqrt{2}$ is irrational. Therefore, consider the following:

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational

Then we are done, as $x = y = \sqrt{2}$ satified all the above.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational

Then consider $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

As 2 is rational, we are done. □

2 Induction

Next we segway into another way to write a proof about natural numbers.

Consider a row of dominoes all upright. Let's postulate that if the ith domino falls it will cause the $i+1$th domino to fall. If you know the 1st domino falls, what can you say about the dominoes?

Definition 1 (Principle of Mathematical Induction)**.** Let $\varphi(x)$ be a formula. If $\varphi(0)$ is true, and $\varphi(n) \to \varphi(n+1)$ is true, then $\varphi(m)$ is true for any natural number m. In particular, $\forall m \in \mathbb{N} \mathbin{\centerdot} \varphi(m)$ is true.

Question 5. Think about the domino metaphor above. Do you think induction works for the integers, rationals, and reals.

Answer 5. No; the integers aren't like the dominoes because there is no first domino. The reals and the rationals also don't have a first, but even more disappointingly, they don't have the "one after another" property either, which is another hindrance to knowing they all get knocked down.

Remark 1. I am very particular about variables, as I said. This makes the form of an induction proof very important to me. Pay attention to my form, and try to emulate it.

Theorem 1.

$$\forall n \in \mathbb{N} \mathbin{\centerdot} \left(\sum_{i=0}^{n} 2^i\right) = 2^{n+1} - 1$$

Proof With Exposition. The first thing you want to do in an induction proof is notify the reader that they are about to read a proof by induction. Otherwise, it could be very confusing why you are doing what you are doing. It's also useful to say the variable you are inducting on.

We prove this by induction on $n \in \mathbb{N}$.

First, we want to show that that we can knock down the first domino. This is called our **base case**. Sometimes, we need to do more than one, depending what we are trying to prove. We will talk more about this tomorrow.

But, we need to show the above sum is true when $n = 0$. When $n = 0$, the summation is just 2^0, which is 1. The RHS is $2^1 - 1 = 1$. So the base case is true.

Now, we need to show $\forall n \in \mathbb{N} \mathbin{\centerdot} \varphi(n) \to \varphi(n+1)$. That is, if the nth domino falls, so will the $n+1$th. This is called out **inductive step**.

Let n be a natural number, and assume that $\sum_{i=0}^{n} 2^i$. This assumption is called the **inductive hypothesis**. There are a few important things to note:

- The induction hypothesis is "allowed" to be the base case. For example, to see domino number 1 falls, we need to know domino number 0 knocks down domino number 1. So it's very important, since our base case $n = 0$ is allowed to be the n assumed in the induction hypothesis.
- When you think about these proofs, think about them as an iterative procedure rather than a proof. Don't think about trying to prove $\forall n \in \mathbb{N} \mathbin{\centerdot} \varphi(n)$ think concretely that you are interested in $\varphi(70)$ or something. The way you prove this is to prove $\varphi(0)$, then prove $\varphi(0) \to \varphi(1)$, then $\varphi(1) \to \varphi(2)$, and so on. The principle of induction formalized this procedure.

At this point in the proof, it's useful to say your goal. We want to prove

$$\left(\sum_{i=0}^{n+1} 2^i\right) = 2^{n+2} - 1$$

Well, we know that

$$\left(\sum_{i=0}^{n} 2^i\right) = 2^{n+1} - 1$$

So, notice, if we ass 2^{n+1} to both sides, we get

$$2^{n+1} + \left(\sum_{i=0}^{n} 2^i\right) = 2^{n+1} + 2^{n+1} - 1$$

Which we can rewrite as

$$\left(\sum_{i=0}^{n+1} 2^i\right) = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

Which was what we wanted!

Now, you want to say a summary statement, concluding that we have accomplished our goal. So we might say, by induction, this statement is true for all n in the natural numbers. □

Proof as I'd write it. We proceed by induction on the natural number n

In our base case, $n = 0$. Note that

$$\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^1 - 1$$

Thus the statement is true when $n = 0$.

For our induction hypothesis, let n be a natural number, and assume that our statement is true at n; that is:

$$\text{(IH)} \qquad \left(\sum_{i=0}^{n} 2^i\right) = 2^{n+1} - 1$$

We would like to true that this statement is true at $n + 1$; that is

$$\left(\sum_{i=0}^{n+1} 2^i\right) = 2^{n+2} - 1$$

Well, by adding 2^{n+1} to both sides of my induction hypothesis, we see

$$2^{n+1} + \left(\sum_{i=0}^{n} 2^i\right) = 2^{n+1} + 2^{n+1} - 1$$

Simplifying,

$$\left(\sum_{i=0}^{n+1} 2^i\right) = 2^{n+2} - 1$$

Which was what we wanted.

Thus, by induction, we have proved the statement for all n in the natural numbers. □