CMSC 250: First Order Logic - Proofs

Justin Wyss-Gallifent

February 23, 2023

1 Proofs Involving Statements with Quantifiers

1.1 Proving Existential and Disproving Universal; Counterexamples

Suppose we wish to prove an existential statement, meaning one of the form:

$$\exists x, P(x)$$

To prove that such a statement is true, often we can simply find a specific example. Please note that $P(x)$ itself might be its own fairly complex expression.

Example 1.1. Consider the statement:

There is some integer $x \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ which is a perfect square

or more formally:

$$\exists x \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, \exists y \in \mathbb{Z}, x = y^2$$

To prove this statement is true, we simply identify such an integer. A proof could simply stating that $x = 4$ (or $x = 9$) is a perfect square.

■

Example 1.2. Consider the statement

$$\exists n \in \mathbb{Z}, n \text{ is even and } n \text{ is prime}$$

To prove this statement is true, we simply identify such an integer. A proof could simply be stating that $n = 2$ is even and is prime.

■

Suppose now we wish to disprove a universal statement $\forall x, P(x)$.

Definition 1.1.1. To *disprove* a statement means to prove its negation.

This means we are trying to prove:

$$\sim [\forall x, P(x)]$$

However this is equivalent to:

$$\exists x, \sim P(x)$$

This means that disproving a universal statement is the same as proving a related existential statement.

Example 1.3. To disprove:

$$\forall x \in \{\text{primes}\},\ x \text{ is odd.}$$

We instead prove the negation:

$$\sim [\forall x \in \{\text{primes}\},\ x \text{ is odd.}]$$

This is equivalent to:

$$\exists x \in \{\text{primes}\},\ x \text{ is not odd.}$$

As a proof we present the prime $x = 2$, which is not odd.

□

Definition 1.1.2. When we disprove a universal statement by presenting a specific example which proves the existential negation of that universal we say we have found a *counterexample* to the universal statement.

■

Example 1.4. A counterexample to:

$$\forall x \in \{\text{primes}\},\ x \text{ is odd.}$$

is $x = 2$, since x is a prime which is not odd.

□

Example 1.5. A counterexample to:

$$\forall a \in \mathbb{Z}, a \nmid (a+1)$$

Is $a = 1$, since a is an integer and $1 \mid (1+1)$.

□

Example 1.6. A counterexample to:

$$\forall a, b, c, m \in \mathbb{Z} \text{ with } m \geq 2, (ac \equiv bc \mod m) \to (a \equiv b \mod m)$$

Is $a = 1$, $b = 2$, $c = 2$, $m = 2$, since $1 \cdot 2 \equiv 2 \cdot 2 \mod 2$ but $2 \not\equiv 2 \mod 2$.

□

1.2 Proving Universal and Disproving Existential

Suppose we wish to prove a universal statement, meaning one of the form:

$$\forall x \in D, P(x)$$

Since we wish to prove it's always true we cannot show it's true for just one specific example. The approach here will be to start with a *general* x in D and

show that $P(x)$ is true. We will have a more organized way soon but for now, a simple example:

Example 1.7. To prove:

$$\forall x \in \mathbb{R}, \text{ if } x > 3 \text{ then } x^2 + 2x + 2 > 17$$

To prove this, we start with an unknown $x \in \mathbb{R}$. We take this x and then prove: If $x > 3$ then $x^2 + 2x + 2 > 17$. To do this we observe:

$$x^2 + 2x + 2 > (3)^2 + 2(3) + 2 = 9 + 6 + 2 = 17$$

Then we are done.

□

Suppose now we wish to disprove an existential statement $\exists x, P(x)$. To disprove an existential statement means to prove its negation. This means we're trying to prove:

$$\sim [\exists x, P(x)]$$

However this is equivalent to:

$$\forall x, \sim P(x)$$

This means that disproving an existential statement is equivalent to proving a related universal statement.

Example 1.8. To disprove:

$$\exists x \in \mathbb{R}, x^2 + 2x < -1$$

We instead prove the negation:

$$\sim \left[\exists x \in \mathbb{R}, x^2 + 2x < -1\right]$$

This is equivalent to:

$$\forall x \in \mathbb{R}, x^2 + 2x \geq -1$$

Since $x^2 + 2x + 1 = (x + 1)^2 \geq 0$ we know $x^2 + 2x \geq -1$.

□

Example 1.9. To disprove:

$$\exists a \in \mathbb{Z}, \ x \text{ is even and } a \text{ is odd}$$

We instead prove the negation:

$$\sim [\exists a \in \mathbb{Z}, \ a \text{ is even and } a \text{ is odd}]$$

This is equivalent to:

$$\forall a \in \mathbb{Z}, \text{ either } a \text{ is not even or } a \text{ is not odd}$$

We'll talk about how to do this later.

□

2 What's a Formal Proof?

Just to be honest and open, there is no "official" definition of a formal proof nor is there a hard line between "formal" and "informal". Rather there is a relatively large grey area and it's best to stay on the right side of this grey area.

To that note, here are some guidelines to help you know if your proofs are "formal enough". This is not comprehensive, it's just a list of things that can help guide you!

1. Your proof should flow when the reader reads it. This means sentences and connecting words like "therefore" and "from here we can see" and so on.
2. Equations should be contextualized, meaning there should be words to clarify their existence and the role they play in the greater context.
3. Variables should not be introduced without explanation as to why they are there.
4. Lead the reader into the process at the beginning by making sure they know where you're starting and why.
5. Make sure the reader knows why you have achieved the goal.
6. It's standard to use the third person when writing proofs. That is, "we" and "us" and so on. You don't have to but the entire mathematical community will think you're strange if you don't.

3 Basic Proof Type Overview

3.1 Direct Proofs

Suppose we are trying to prove an implication of the form $P \to Q$.

Definition 3.1.1. A *direct proof* of $P \to Q$ involves assuming P and finding a series of steps, each of which introduces new facts which follow logically from previous facts, until we obtain Q.

□

Direct proofs are exactly what we were doing when we proved the validity of arguments.

Example 3.1. Let's prove the statement:

$$\forall x \in \mathbb{Z}, \text{ if } x \text{ is even then } 3x + 7 \text{ is odd}$$

Because this is a $\forall$ statement we start with a general and unknown $x \in \mathbb{Z}$.

For a direct proof we assume that x is even. Since x is even, $x = 2k$ for some integer k. Then $3x + 7 = 3(2k) + 7 = 6k + 7 = 2(3k + 2) + 1$. Since we have written $3k + 7$ as $2(\text{integer}) + 1$ we have proven that $3k + 7$ is odd.

□

Let's pause for a second and reflect on the previous section regarding informality. Here is the exact same proof as above but devoid of any clarification:

Example 3.2. Proof: $x = 2k$, $3x + 7 = 2(3k + 2) + 1$, done.

Notice that the following questions arise for someone new to the problem:

- Q: Where did that $x = 2k$ come from?
- Q: What is k?
- Q: Where did the $3x + 7$ come from?
- Q: In what way are we done?

Answering these simple questions leads to a nice, readable proof:

- Q: Where did that $x = 2k$ come from?
  A: Since x is even.
- Q: What is k?
  A: It's an integer.
- Q: Where did the $3x + 7$ come from?
  A: It's the thing we want to prove is odd.
- Q: In what way are we done?
  A: Well $3x + 7$ now has the form of an odd number.

Filling this in:

Proof: Since x is even $x = 2k$ for some integer k. Then look at $3x+7$ and note that $3x+7 = 3(2k)+7 = 6k+7 = 2(3k+2)+1$. Since $3k+7 = 2(\text{integer})+1$ we know that $3k + 7$ is odd.

Much nicer!

□

Example 3.3. Let's prove the statement:

$$\forall x \in \mathbb{R}, \text{ if } x > 5 \text{ then } x^2 - x - 10 > 10.$$

Because this is a $\forall$ statement we start with a general and unknown $x \in \mathbb{R}$.

For a direct proof we assume that $x > 5$. Then observe that:

$$x^2 - x - 10 = x(x-1) - 10 > 5(5-1) - 10 = 10$$

□

Example 3.4. Let's prove the following statement. Notice that the nature of a, b, and c is implied.

$$\text{If } a|b \text{ and } b|c \text{ then } a|c.$$

Because this is a $\forall$ statement we start with general and unknown a, b, and c.

Proof: We assume that $a|b$ and $b|c$. Then $ak = b$ and $bl = c$ for integers k, l. Then $c = bl = (ak)l = (kl)a$ and since kl is an integer we have proved $a|c$.

□

We can often prove a direct proof by exhaustion.

Definition 3.1.2. A *direct proof by exhaustion* of a universal statement is a proof where we show that the statement is true for all possible values. This only works when there are finitely many values.

□

Example 3.5. Let's prove the statement:

$$\forall n \in 1, 2, 4, 6,\ n^2 + 1 \text{ is prime.}$$

Proof: Observe that $1^2 + 1 = 2$, $2^2 + 1 = 5$, $4^2 + 1 = 17$, and $6^2 + 1 = 37$ are all prime.

□

3.2 Proof by Contrapositive

Suppose we are trying to prove an implication of the form $P \to Q$. We know that a statement is logically equivalent to its contrapositive:

$$P \to Q \equiv \sim Q \to \sim P$$

We can thus instead prove $\sim Q \to \sim P$ directly.

Definition 3.2.1. A *proof by contrapositive* of $P \to Q$ involves assuming $\sim Q$ and finding a series of steps, each of which introduces new facts which follow logically from previous facts, until we obtain $\sim P$.

□

We might want to do this when assuming P gives us little to work with or when assuming $\sim Q$ gives us a lot to work with.

Note 3.2.1. Recall that the contrapositive of a statement wrapped in a quantifer is just the contrapositive of the statement. The quantifier doesn't change. So the contrapositive of $\forall x, (P(x) \to Q(x))$ is $\forall x, (\sim Q(x) \to \sim P(x))$.

□

Example 3.6. Let's prove the statement:

$$\forall a, b \in \mathbb{Z}, \text{ if } a \nmid (2b) \text{ then } a \nmid b$$

Because this is a $\forall$ statement we start with general and unknown $a, b \in \mathbb{Z}$.

If we were to approach this as a direct proof we would assume $a \nmid (2b)$ but this doesn't give us much to work with. After all, this just means that there *isn't* some $k \in \mathbb{Z}$ with $ak = 2b$, and what do we do with that?

For a proof by contrapositive we assume $\sim(a \nmid b)$, which is $a \mid b$, and we attempt to prove $\sim a \nmid (2b)$, which is $a \mid (2b)$. These are easier to work with.

Proof: If $a \mid b$ then there is some $k \in \mathbb{Z}$ with $ak = b$. From here we can put $a(2k) = 2b$ and since we have written $a(\text{integer}) = 2b$ we have proven that $a \mid (2b)$.

□

Example 3.7. Let's prove the statement:

If the square of an integer is even, then the integer is even.

Because this is a $\forall$ statement we start with general and unknown $x \in \mathbb{Z}$.

If we were to approach this as a direct proof we would assume that x^2 is even, meaning $x^2 = 2k$ for some integer k. But this doesn't give us much. We can say $x = \pm\sqrt{2k}$ but this isn't particularly helpful.

For a proof by contradiction we assume x is not even and attempt to prove x^2 is not even.

Proof: Assume x is odd and so $x = 2k + 1$ for some integer k. Then we have $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which tells us that x^2 is odd, and hence not even.

□

3.3 Proof by Contradiction

Suppose we are trying to prove an implication of the form P. This might be of the form $P \to Q$ but not necessarily.

Definition 3.3.1. A *proof by contradiction* of P involves assuming the negation $\sim P$ and finding a series of steps, each of which introduces new facts which follow logically from previous facts, until we obtain some (any) contradiction at all. This contradiction could be two facts with disagree with one another or something which is simply untrue.

□

Example 3.8. Let's prove:

$$\forall x \in \mathbb{R},\, x \neq x + 1$$

Proof: We assume the negation:

$$\sim [\forall x \in \mathbb{R},\, x \neq x + 1]$$

This is equivalent to:

$$\exists x \in \mathbb{R}\; x = x + 1$$

Since we are assuming such an x exists, we know $x = x + 1$ and then $0 = 1$.

Since this is impossible, we have our contradiction and our assumption is false and so our original assertion is true.

□

Example 3.9. Let's prove the statement:

There is no greatest integer.

Proof: We assume the negation, that there is a greatest integer. Let's call it N. But then notice that $N + 1$ is also an integer and $N + 1 > N$. This contradicts the assumption that N is greatest. Thus our original assertion is true.

□

Note 3.3.1. When the implication we wish to prove is of the form $P \to Q$ then assuming the negation $\sim(P \to Q)$ means assumign $P \wedge \sim Q$. This means we get to assume both P and $\sim Q$. This is very much the best of both worlds since we get more things to chew on in our hunt for a contradiction. This is why proofs by contradiction are extremely common and powerful.

□

Example 3.10. Let's prove that an even integer is not odd. This means we are proving:

$$\forall x \in \mathbb{Z}, \text{ if } x \text{ is even then } x \text{ is not odd}$$

Proof: We assume the negation:

$$\sim [\forall x \in \mathbb{Z}, \text{ if } x \text{ is even then } x \text{ is not odd}]$$

This is equivalent to:

$$\exists x \in \mathbb{Z}, \sim [\text{if } x \text{ is even then } x \text{ is not odd}]$$

And to:

$$\exists x \in \mathbb{Z}, \ x \text{ is even and } x \text{ is odd}$$

So we assume this is true. Since we are assuming such an x exists, we know $x = 2k$ and $x = 2l + 1$ for $k, l \in \mathbb{Z}$.

But then $2k = 2l+1$ and so $2(k-l) = 1$ and so $k-l = \frac{1}{2}$ which is impossible since $k, l \in \mathbb{Z}$.

This is our contradiction, and therefore our hypothesis is false and so our original assertion is true.

□

Generally we won't write so much detail:

Example 3.11. Let's prove the statement:

$$\forall a \in \mathbb{Z}, \text{ if } a \mod 6 = 3 \text{ then } a \mod 3 \neq 2.$$

Proof: We assume, by way of contradiction, that there is some $a \in \mathbb{Z}$ with $a \mod 6 = 3$ and $a \mod 3 = 2$.

The first tells us $a = 6q_1 + 3$ and the second tells us $a = 3q_2 + 2$, where q_1, q_2 are integers. Then we have:

$$\begin{aligned} 6q_1 + 3 &= 3q_2 + 2 \\ 6q_1 - 3q_2 &= -1 \\ 3(2q_1 - q_2) &= -1 \\ 2q_1 - q_2 &= -\frac{1}{2} \end{aligned}$$

Since $2q_1 - q_2$ is an integer, this is a contradiction and our original assertion is true.

□