Proving Non-Conditional Statements

MAT231

Transition to Higher Mathematics

Fall 2014

Outline

1. If-and-Only-If Proof

2. Equivalent Statements

3. Existence Proofs

4. Constructive Verses Non-Constructive Proofs

5. Examples

If-Then Proof

We've now spent some time proving *conditional statements* of the form

$$\text{if } P, \text{ then } Q.$$

Recall from the truth table for this implication, that it is only false if P is true and Q is false – so all we needed to show was that if P is true then we are sure that Q will also be true.

We've seen proofs that use each of the following approaches:

1. direct proof; assume P is true and show Q must be true,
2. contrapositive proof (also called an *indirect proof*); assume Q is false and show P must be false, and
3. proof by contradiction; assume $P \wedge \sim Q$ and show that a contradiction arises.

If-and-Only-If Proof

Sometimes we want to prove a *bi-conditional statement* in the form

$$P \text{ if and only if } Q$$

which is equivalent to the statement

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

Bi-conditional statements are strong in the sense that both a conditional statement and its converse are true.

Often we will need to work a little harder to prove a bi-conditional statement than we'd need to for a conditional statement. This is usually because we'll need to prove two conditional statements: $P \Rightarrow Q$ and $Q \Rightarrow P$.

Other than that, we'll proceed much as we have been.

If-and-Only-If Proof Example 1

We've already seen one bi-conditional statement proof, but stated it and proved it as two separate conditional statements. Back when we introduced the modulo operator we proved two propositions:

Proposition

Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If a mod $n = b$ mod n, then $a \equiv b \pmod{n}$.

Proposition

Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then a mod $n = b$ mod n.

Combining these two, we have the single statement

Proposition

Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then a mod $n = b$ mod n if and only if $a \equiv b \pmod{n}$.

The proof of this requires both proofs we carried out before.

If-and-Only-If Proof Example 2

Proposition

An integer a is odd if and only if a^3 is odd.

If-and-Only-If Proof Example 2

Proposition

An integer a is odd if and only if a^3 is odd.

Proof.

We begin by showing that if a is odd then a^3 is odd. Suppose a is odd so it can be written as $a = 2k + 1$ for some integer k. Then

$$a^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$$

which is odd by definition since $4k^3 + 6k^2 + 3k$ is an integer by the closure properties for integers.

(Continued next slide)

If-and-Only-If Proof Example 2

Proposition

An integer a is odd if and only if a^3 is odd.

Proof.

(Continued from previous slide) Conversely, we need to show that if a^3 is odd then a is odd. We'll do this using a contrapositive proof. Suppose a is not odd, i.e., a is even, so $a = 2k$ for some integer k. Then

$$a^3 = (2k)^3 = 8k^3 = 2(4k^3).$$

Since a^3 is an integer multiple of 2, we see that it is even by definition and therefore not odd. Thus, a^3 being odd implies a is odd. This completes the proof. □

Equivalent Statements

Sometimes we have what amounts to an "if-and-only-if" statement with more than two parts; three or more statements are all *logically equivalent*. If any one of them is true, then they all are true, and if any one of them is false, then they all are false.

Usually these statements have the form given by the template:

Proposition

Each of the following statements are equivalent:

- P
- Q
- R
- S

where P, Q, R, and S are statements.

Equivalent Statements

Proving a statement is usually done by showing how any one statement, implies another, and then repeating this to form a *chain* that ends up back at the original statement. Our template proposition could be proved by showing any of the following

$$
\begin{array}{ll}
P \Rightarrow Q \Rightarrow R \Rightarrow S \Rightarrow P, & \qquad P \Rightarrow Q \Rightarrow S \Rightarrow R \Rightarrow P, \\
P \Rightarrow S \Rightarrow Q \Rightarrow R \Rightarrow P, & \qquad P \Rightarrow S \Rightarrow R \Rightarrow Q \Rightarrow P, \\
P \Rightarrow R \Rightarrow Q \Rightarrow S \Rightarrow P, & \qquad P \Rightarrow R \Rightarrow S \Rightarrow Q \Rightarrow P, \\
Q \Rightarrow R \Rightarrow S \Rightarrow P \Rightarrow Q, & \qquad Q \Rightarrow R \Rightarrow P \Rightarrow S \Rightarrow Q, \\
Q \Rightarrow S \Rightarrow R \Rightarrow P \Rightarrow Q, & \qquad Q \Rightarrow S \Rightarrow P \Rightarrow R \Rightarrow Q, \\
Q \Rightarrow P \Rightarrow R \Rightarrow S \Rightarrow Q, & \qquad Q \Rightarrow P \Rightarrow S \Rightarrow R \Rightarrow Q, \\
R \Rightarrow S \Rightarrow P \Rightarrow Q \Rightarrow R, & \qquad R \Rightarrow S \Rightarrow Q \Rightarrow P \Rightarrow R, \\
R \Rightarrow P \Rightarrow S \Rightarrow Q \Rightarrow R, & \qquad R \Rightarrow P \Rightarrow Q \Rightarrow S \Rightarrow R, \\
R \Rightarrow Q \Rightarrow S \Rightarrow P \Rightarrow R, & \qquad R \Rightarrow Q \Rightarrow P \Rightarrow S \Rightarrow R, \\
S \Rightarrow P \Rightarrow Q \Rightarrow R \Rightarrow S, & \qquad S \Rightarrow P \Rightarrow R \Rightarrow Q \Rightarrow S, \\
S \Rightarrow Q \Rightarrow P \Rightarrow R \Rightarrow S, & \qquad S \Rightarrow Q \Rightarrow R \Rightarrow P \Rightarrow S, \\
S \Rightarrow R \Rightarrow P \Rightarrow Q \Rightarrow S, & \qquad S \Rightarrow R \Rightarrow Q \Rightarrow P \Rightarrow S.
\end{array}
$$

Existence Proof

How could we prove this proposition?

Proposition

There exists an integer n for which $8n + 5 = 61$.

Existence Proof

How could we prove this proposition?

Proposition

There exists an integer n for which $8n + 5 = 61$.

To prove this we need to show that there is an integer n for which $8n + 5 = 61$ is a true statement. Although it is not *necessary* to find the value of n, if we can find a value for n that works then we've completed the proof.

In this case $n = 7$ works since $8 \cdot 7 + 5 = 56 + 5 = 61$.

This is an example of an **existence proof**. In some cases the easiest way to prove the statement is to find a value that makes it true. Sometimes this is not possible.

Existence and Uniqueness Proof

Now consider the proposition

Proposition

There exists a unique integer n for which $8n + 5 = 61$.

Now we need to show two things:

1. an integer n that satisfies $8n + 5 = 61$ exists, and
2. it is the only integer that satisfies $8n + 5 = 61$.

Existence and Uniqueness Proof

Now consider the proposition

Proposition

There exists a unique integer n for which $8n + 5 = 61$.

Now we need to show two things:

1. an integer n that satisfies $8n + 5 = 61$ exists, and
2. it is the only integer that satisfies $8n + 5 = 61$.

How can we show $n = 7$ is the only such integer? Suppose that there is another integer, say m, that satisfies the equation. Then

$$\begin{aligned} 8m + 5 &= 61 \\ 8m &= 56 \\ m &= 56/8 = 7. \end{aligned}$$

Since $m = 7$, we conclude that the only number that satisfies $8n + 5 = 61$ is 7.

Constructive Verses Non-Constructive Proof

There are two ways to prove a statement about existence.

Constructive: A *constructive proof* demonstrates the existence of the quantity described in the statement **and** shows how to generate one or more of those values.

Non-Constructive: A *non-constructive proof* affirms the existence of the quantity, but does not provide any direction to help with finding the quantity.

Proving there is an integer n that satisfies $n^2 + 3 = 19$ by solving for n algebraically (or merely guessing-and-checking) is a constructive proof – part of the prove is finding a value that works.

The proof of of the Intermediate Value Theorem (from Calculus) is a non-constructive proof.

Practice

Proposition

An integer a is even if and only if a^2 is even.

Proposition

Suppose that $a \in \mathbb{Z}$. Prove that $14|a$ if and only if $7|a$ and $2|a$.

Proposition

Let A be any finite set. There exists a set X for which $A \in X$ and $A \subseteq X$.