Introduction to Proofs - Proof Strategies: Contradiction

Prof Mike Pawliuk

UTM

May 21, 2020

Slides available at: mikepawliuk.ca

Learning Objectives (for this video)

By the end of this video, participants should be able to:

1. Explain the logic of a proof by contradiction.
2. Produce a proof by contradiction.
3. Decide which proof technique (Direct, contrapositive, contradiction) is most appropriate.

Story about Avacados and Guacamole

This image is used with permission from Pixabay. https://pixabay.com/photos/avocado-salad-fresh-food-829092/

Proof by contradiction

Proof Technique ($P \implies Q$) - Contradiction

To prove $P \implies Q$, by contradiction: Assume P. Assume $\neg Q$. Derive a contradiction. (Conclude Q.)

We will look at three examples: one mild, one mild, one spicy.

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even and x is odd .

□

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even "Assume P." and x is odd .

□

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even $\boxed{\text{“Assume } P\text{.”}}$ and x is odd $\boxed{\text{“Assume } \neg Q\text{.”}}$.

□

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even "Assume P." and x is odd "Assume $\neg Q$.".
Since x is even, there is an integer k such that $x = 2k$. Since x is odd, there is an integer m such that $x = 2m + 1$.

□

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even "Assume P." and x is odd "Assume $\neg Q$.".
Since x is even, there is an integer k such that $x = 2k$. Since x is odd, there is an integer m such that $x = 2m + 1$.
So $2k = 2m + 1$, and also $2k - 2m = 1$ and $k - m = \frac{1}{2}$.

□

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even "Assume P." and x is odd "Assume $\neg Q$.".

Since x is even, there is an integer k such that $x = 2k$. Since x is odd, there is an integer m such that $x = 2m + 1$.

So $2k = 2m + 1$, and also $2k - 2m = 1$ and $k - m = \frac{1}{2}$. However, $k - m$ is an integer, and $\frac{1}{2}$ is not. $\Rightarrow\Leftarrow$ $\square$

Example 1

Definitions:

- An integer x is <u>even</u> if and only if $(\exists k \in \mathbb{Z})[x = 2k]$.
- An integer x is <u>odd</u> if and only if $(\exists m \in \mathbb{Z})[x = 2m + 1]$.

Theorem

If x is even, then x is not odd.

Proof.

Assume for the sake of contradiction, that x is even ["Assume P."] and x is odd ["Assume $\neg Q$."].
Since x is even, there is an integer k such that $x = 2k$. Since x is odd, there is an integer m such that $x = 2m + 1$.
So $2k = 2m + 1$, and also $2k - 2m = 1$ and $k - m = \frac{1}{2}$. However, $k - m$ is an integer, and $\frac{1}{2}$ is not. $\Rightarrow\Leftarrow$ [Indicates a contradiction] $\square$

Example 2

Exercise. Prove the following using a proof by contradiciton.

Theorem

There are no natural numbers x, y with $x^2 - y^2 = 1$.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p | n$.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Proof.

Suppose not.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Proof.

Suppose not. Let $p_1, p_2, \ldots, p_n$ be the list of all prime numbers.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Proof.

Suppose not. Let $p_1, p_2, \ldots, p_n$ be the list of all prime numbers.
Let $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Proof.

Suppose not. Let $p_1, p_2, \ldots, p_n$ be the list of <u>all</u> prime numbers.
Let $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$. By the lemma, there is a p_i so that $p_i|N$.

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Proof.

Suppose not. Let $p_1, p_2, \ldots, p_n$ be the list of <u>all</u> prime numbers.
Let $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$. By the lemma, there is a p_i so that $p_i|N$.
However, this is impossible, since dividing N by p_i will have a remainder of 1. $\Rightarrow\Leftarrow$. $\square$

Example 3

Lemma. If $n \in \mathbb{N}$ and $n > 1$, then there is a prime number p such that $p|n$.

Theorem (Proof due to Euclid)

There are infinitely many prime numbers.

Proof.

Suppose not. Let $p_1, p_2, \ldots, p_n$ be the list of <u>all</u> prime numbers.
Let $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$. By the lemma, there is a p_i so that $p_i|N$. However, this is impossible, since dividing N by p_i will have a remainder of 1. $\Rightarrow\Leftarrow$. □

Note the N in this proof is not necessarily prime. E.g.
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = (59)(509)$.

Pros and Cons of proof by contradiction

Pros:

1. It gives you two things to work with (P and $\neg Q$)
2. Often the proofs are short.

Pros and Cons of proof by contradiction

Pros:

1. It gives you two things to work with (P and $\neg Q$)
2. Often the proofs are short.

Cons:

1. The proofs are not constructive. (e.g. Euclid's proof does not tell you how to make large prime numbers.)
2. It's not always clear what contradiction to aim for.
3. It can make messy/confusing proofs.

What technique should I use?

1. **Direct**. Is good for "definition unwinding" proofs.
2. **Contrapositive**. Very similar to direct, but when $\neg Q$ and $\neg P$ are easier to work with. (e.g. $x + y = 0$ is easier to work with than $x + y \neq 0$.)
3. **Contradiction**. Good for statements of the form "no weird things exist". (If the things are sufficiently weird, then assuming it exists should produce a contradiction.)

What technique should I use?

1. **Direct**. Is good for "definition unwinding" proofs.
2. **Contrapositive**. Very similar to direct, but when $\neg Q$ and $\neg P$ are easier to work with. (e.g. $x + y = 0$ is easier to work with than $x + y \neq 0$.)
3. **Contradiction**. Good for statements of the form "no weird things exist". (If the things are sufficiently weird, then assuming it exists should produce a contradiction.)

Exercise What technique should you use to prove these statements?

1. $\sqrt{2}$ is irrational.
2. $(\forall x \in \mathbb{R})[x > 0 \implies x^2 > 0]$.
3. $(\forall x \in \mathbb{R})[x^2 > 0 \implies x \neq 0]$.

What technique should I use?

1. **Direct**. Is good for "definition unwinding" proofs.
2. **Contrapositive**. Very similar to direct, but when $\neg Q$ and $\neg P$ are easier to work with. (e.g. $x + y = 0$ is easier to work with than $x + y \neq 0$.)
3. **Contradiction**. Good for statements of the form "no weird things exist". (If the things are sufficiently weird, then assuming it exists should produce a contradiction.)

Exercise What technique should you use to prove these statements?

1. $\sqrt{2}$ is irrational. **Contradiction**
2. $(\forall x \in \mathbb{R})[x > 0 \implies x^2 > 0]$.
3. $(\forall x \in \mathbb{R})[x^2 > 0 \implies x \neq 0]$.

What technique should I use?

1. **Direct**. Is good for "definition unwinding" proofs.
2. **Contrapositive**. Very similar to direct, but when $\neg Q$ and $\neg P$ are easier to work with. (e.g. $x + y = 0$ is easier to work with than $x + y \neq 0$.)
3. **Contradiction**. Good for statements of the form "no weird things exist". (If the things are sufficiently weird, then assuming it exists should produce a contradiction.)

Exercise What technique should you use to prove these statements?

1. $\sqrt{2}$ is irrational. **Contradiction**
2. $(\forall x \in \mathbb{R})[x > 0 \implies x^2 > 0]$. **Direct**
3. $(\forall x \in \mathbb{R})[x^2 > 0 \implies x \neq 0]$.

What technique should I use?

1. **Direct**. Is good for "definition unwinding" proofs.
2. **Contrapositive**. Very similar to direct, but when $\neg Q$ and $\neg P$ are easier to work with. (e.g. $x + y = 0$ is easier to work with than $x + y \neq 0$.)
3. **Contradiction**. Good for statements of the form "no weird things exist". (If the things are sufficiently weird, then assuming it exists should produce a contradiction.)

Exercise What technique should you use to prove these statements?

1. $\sqrt{2}$ is irrational. **Contradiction**
2. $(\forall x \in \mathbb{R})[x > 0 \implies x^2 > 0]$. **Direct**
3. $(\forall x \in \mathbb{R})[x^2 > 0 \implies x \neq 0]$. **Contrapositive**

Reflection

- What types of proofs are constructive, and which are non-constructive?
- What are the advantages and disadvantages of both?
- What are some reasons why you might want to use proof by contradiciton?