# Mathematical Proofs
# A Transition to Advanced Mathematics

## Chapter 3
## Direct Proof and Proof by Contrapositive

Gary Chartrand  Albert D. Polimeni  Ping Zhang

# Direct Proof and Proof by Contrapositive

We are now prepared to begin discussing our main topic:

mathematical proofs.

Initially, we will be primarily concerned with one question:

For a given true mathematical statement, how can we show that it is true?

In this chapter you will be introduced to two important proof techniques.

# Direct Proof and Proof by Contrapositive

**Definition**

A true mathematical statement whose truth is accepted without proof is referred to as an **axiom**.

A true mathematical statement whose truth can be verified is often referred to as a **theorem**, although many mathematicians reserve the word "theorem" for such statements that are especially significant or interesting.

We will use the word "theorem" sparingly, however, primarily reserving it for true mathematical statements that will be used to verify other mathematical statements that we will encounter later. Otherwise, we will simply use the word "result."

# Direct Proof and Proof by Contrapositive

For the most part then, our results are examples used to illustrate proof techniques and our goal is to prove these results.

**Definition**

A **corollary** is a mathematical result that can be deduced from, and is thereby a consequence of, some earlier result.

A **lemma** is a mathematical result that is useful in establishing the truth of some other result.

Some people like to think of a lemma as a "helping result." Indeed, the German word for lemma is "hilfsatz," whose English translation is "helping theorem." Ordinarily then, a lemma is not of primary importance itself. Indeed, its very existence is due only to its usefulness in proving another (more interesting) result.

# Trivial and Vacuous Proofs

In nearly all of the implications $P \Rightarrow Q$ that we will encounter, $P$ and $Q$ are open sentences; that is, we will actually be considering $P(x) \Rightarrow Q(x)$ or $P(n) \Rightarrow Q(n)$ or some related implication, depending on which variable is being used. The variables $x$ or $n$ (or some other symbols) are used to represent elements of some set $S$ being discussed, that is, $S$ is the domain of the variable. As we have seen, for each value of a variable from its domain, a statement results.

# Trivial and Vacuous Proofs

Whether $P(x)$ (or $Q(x)$) is true ordinarily depends on which element $x \in S$ we are considering; that is, it is rarely the case that $P(x)$ is true for all $x \in S$ (or that $P(x)$ is false for all $x \in S$). For example, for

$$P(n) : 3n^2 - 4n + 1 \text{ is even}$$

where $n \in \mathbf{Z}$, $P(1)$ is a true statement while $P(2)$ is a false statement. Likewise, it is seldom the case that $Q(x)$ is true for all $x \in S$ or that $Q(x)$ is false for all $x \in S$.

# Trivial and Vacuous Proofs

When the quantified statement $\forall x \in S,\ P(x) \Rightarrow Q(x)$ is expressed as a result or theorem, we often write such a statement as

$$\text{For } x \in S, \text{ if } P(x) \text{ then } Q(x).$$

or as

$$\text{Let } x \in S. \text{ If } P(x), \text{ then } Q(x).$$

This implication is true if $P(x) \Rightarrow Q(x)$ is a true statement for each $x \in S$; while it is false if $P(x) \Rightarrow Q(x)$ is false for at least one element $x \in S$.

# Trivial and Vacuous Proofs

For a given element $x \in S$, let's recall (see the implication truth table in the figure below) the conditions under which $P(x) \Rightarrow Q(x)$ has a particular truth value for an element $x$ in its domain.

| $P(x)$ | $Q(x)$ | $P(x) \Rightarrow Q(x)$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

# Trivial and Vacuous Proofs

## Definition

Accordingly, if $Q(x)$ is true for all $x \in S$ or $P(x)$ is false for all $x \in S$, then determining the truth or falseness of

$$\text{Let } x \in S. \text{ If } P(x), \text{ then } Q(x)$$

becomes considerably easier.

If it can be shown that $Q(x)$ is true for all $x \in S$ (regardless of the truth value of $P(x)$), then, according to the truth table for the implication, it is true. This constitutes a proof and is called a **trivial proof**.

# Trivial and Vacuous Proofs

## Example 1

**Result** Let $x \in \mathbf{R}$. If $x < 0$, then $x^2 + 1 > 0$.

**Proof.** Since $x^2 \geq 0$ for each real number $x$, it follows that

$$x^2 + 1 > x^2 \geq 0.$$

Hence, $x^2 + 1 > 0$. □

# Trivial and Vacuous Proofs

The symbol □ that occurs at the end of the proof indicates that the proof is complete. There are definite advantages to using □ (or some other symbol) to indicate the conclusion of a proof. First, as you start reading a proof, you can look ahead for this symbol to determine the length of the proof. Also, without this symbol, you may continue to read past the end of the proof, still thinking that you're reading a proof of the result. When you reach this symbol, you are *supposed* to be convinced that the result is true. If you are, this is good! Everything happened as planned.

# Trivial and Vacuous Proofs

**Definition**

Let $P(x)$ and $Q(x)$ be open sentences over a domain $S$. Then $\forall x \in S, P(x) \Rightarrow Q(x)$ is a true statement if it can be shown that $P(x)$ is false for all $x \in S$ (regardless of the truth value of $Q(x)$), according to the truth table for implication. Such a proof is called a **vacuous proof** of $\forall x \in S, P(x) \Rightarrow Q(x)$.

## Example 2

**Result** Let $x \in \mathbf{R}$. If $x^2 - 2x + 2 \leq 0$, then $x^3 \geq 8$.

**Proof.** First observe that

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

Therefore,

$$x^2 - 2x + 2 = (x - 1)^2 + 1 \geq 1 > 0.$$

Thus, $x^2 - 2x + 2 \leq 0$ is false for all $x \in \mathbf{R}$ and the implication is true. □

# Trivial and Vacuous Proofs

## Definition

Whenever there is a vacuous proof of a result, we often say that the result follows **vacuously**. While a trivial proof is almost never encountered in mathematics, the same cannot be said of vacuous proofs.

## Example 3

**Result** Let $S = \{n \in \mathbf{Z} : \ n \geq 2\}$ and let $n \in S$.

$$\text{If } 2n + \frac{2}{n} < 5, \text{ then } 4n^2 + \frac{4}{n^2} < 25.$$

**Proof.** First, we observe that if $n = 2$, then $2n + \frac{2}{n} = 5$. Of course, $5 < 5$ is false. If $n \geq 3$, then $2n + \frac{2}{n} > 2n \geq 6$. So, when $n \geq 3$, $2n + \frac{2}{n} < 5$ is false as well. Thus, $2n + \frac{2}{n} < 5$ is false for all $n \in S$. Hence, the implication is true. □

# Direct Proofs

Let $P(x)$ and $Q(x)$ be open sentences over a domain $S$. Suppose that our goal is to show that $P(x) \Rightarrow Q(x)$ is true for every $x \in S$, that is, our goal is to show that the quantified statement $\forall x \in S, P(x) \Rightarrow Q(x)$ is true. If $P(x)$ is false for some $x \in S$, then $P(x) \Rightarrow Q(x)$ is true for this element $x$. Hence, we need only be concerned with showing that $P(x) \Rightarrow Q(x)$ is true for all $x \in S$ for which $P(x)$ is true.

## Definition

In a **direct proof** of $P(x) \Rightarrow Q(x)$ for all $x \in S$, we consider an arbitrary element $x \in S$ for which $P(x)$ is true and show that $Q(x)$ is true as well for this element $x$. To summarize then, to give a direct proof of $P(x) \Rightarrow Q(x)$ for all $x \in S$, we assume that $P(x)$ is true for an arbitrary element $x \in S$ and show that $Q(x)$ must be true for this element $x$.

# Direct Proofs

In order to illustrate this type of proof (and others as well), we need to deal with mathematical topics with which we're all familiar. Let's first consider the integers and some of their elementary properties. We assume that you are familiar with the integers and the following properties of integers:

1. The negative of every integer is an integer.
2. The sum (and difference) of every two integers is an integer.
3. The product of every two integers is an integer.

# Direct Proofs

We will agree that we can use any of these properties. No justification is required or expected. Initially, we will use even and odd integers to illustrate our proof techniques. In this case, however, any properties of even and odd integers must be verified before they can be used. For example, you probably know that the sum of every two even integers is even but this must first be proved to be used. We need to lay some groundwork before any examples of direct proofs are given.

# Direct Proofs

Since we will be working with even and odd integers, it is essential that we have precise definitions of these kinds of numbers.

**Definition**

An integer $n$ is defined to be **even** if $n = 2k$ for some integer $k$.

For example, 10 is even since $10 = 2 \cdot 5$ (where, of course, 5 is an integer). Also, $-14 = 2(-7)$ is even, as is $0 = 2 \cdot 0$. The integer 17 is not even since there is no *integer* $k$ for which $17 = 2k$.

We could define an integer $n$ to be odd if it's not even but it would be difficult to work with this definition.

**Definition**

Instead, we define an integer $n$ to be **odd** if $n = 2k + 1$ for some integer $k$.

Now 17 is odd since $17 = 2 \cdot 8 + 1$. Also, $-5$ is odd because $-5 = 2(-3) + 1$. On the other hand, 26 is not odd since there is no *integer* $k$ such that $26 = 2k + 1$.

# Direct Proofs

From time to time, we will find ourselves in a position where we have a result to prove and it may not be entirely clear how to proceed. In such a case, we need to consider our options and develop a plan, which we refer to as a **proof strategy**. The idea is to discuss a proof strategy for the result and, from it, construct a proof.

At other times, we may wish to reflect on a proof that we have just given in order to understand it better. Such a discussion will be referred to as a **proof analysis**.

As with examples, we conclude both a proof strategy and a proof analysis with the symbol ⧫. You will find many examples of proof strategies and proof analyses in the textbook.

## Example 4

**Result** If $n$ is an odd integer, then $3n + 7$ is an even integer.

**Proof.** Assume that $n$ is an odd integer. Since $n$ is odd, we can write $n = 2k + 1$ for some integer $k$. Now,

$$3n + 7 = 3(2k + 1) + 7 = 6k + 3 + 7 = 6k + 10 = 2(3k + 5).$$

Since $3k + 5$ is an integer, $3n + 7$ is even. □

## Example 5

**Result** If $n$ is an even integer, then $3n^5$ is an even integer.

**Proof.** Since $n$ is an even integer, $n = 2x$ for some integer $x$. Therefore,

$$3n^5 = 3(2x)^5 = 3(32x^5) = 96x^5 = 2(48x^5).$$

Since $48x^5 \in \mathbf{Z}$, the integer $3n^5$ is even. □

# Proof by Contrapositive

**Definition**

For statements $P$ and $Q$, the **contrapositive** of the implication $P \Rightarrow Q$ is the implication $(\sim Q) \Rightarrow (\sim P)$.

For example, for $P_1$ : 3 is odd and $P_2$: 57 is prime, the contrapositive of the implication

$$P_1 \Rightarrow P_2\text{: If 3 is odd, then 57 is prime.}$$

is the implication

$$(\sim P_2) \Rightarrow (\sim P_1)\text{: If 57 is not prime, then 3 is even.}$$

# Proof by Contrapositive

The most important feature of the contrapositive $(\sim Q) \Rightarrow (\sim P)$ is that it is logically equivalent to $P \Rightarrow Q$. This fact is stated formally as a theorem and is verified in the truth table shown in the figure below.

| $P$ | $Q$ | $P \Rightarrow Q$ | $\sim Q$ | $\sim P$ | $(\sim Q) \Rightarrow (\sim P)$ |
|---|---|---|---|---|---|
| T | T | **T** | F | F | **T** |
| T | F | **F** | T | F | **F** |
| F | T | **T** | F | T | **T** |
| F | F | **T** | T | T | **T** |

# Proof by Contrapositive

## Theorem

For every two statements $P$ and $Q$, the implication $P \Rightarrow Q$ and its contrapositive are logically equivalent; that is,

$$P \Rightarrow Q \equiv (\sim Q) \Rightarrow (\sim P).$$

| $P$ | $Q$ | $P \Rightarrow Q$ | $\sim Q$ | $\sim P$ | $(\sim Q) \Rightarrow (\sim P)$ |
|---|---|---|---|---|---|
| T | T | **T** | F | F | **T** |
| T | F | **F** | T | F | **F** |
| F | T | **T** | F | T | **T** |
| F | F | **T** | T | T | **T** |

# Proof by Contrapositive

Suppose that we wish to prove a result (or theorem) which is expressed as

$$\text{Let } x \in S. \text{ If } P(x), \text{ then } Q(x). \tag{1}$$

or as

$$\text{For all } x \in S, \text{ if } P(x), \text{ then } Q(x). \tag{2}$$

We have seen that a proof of such a result consists of establishing the truth of the implication $P(x) \Rightarrow Q(x)$ for all $x \in S$. If it can be shown that $(\sim Q(x)) \Rightarrow (\sim P(x))$ is true all $x \in S$, then $P(x) \Rightarrow Q(x)$ is true for all $x \in S$.

# Proof by Contrapositive

## Definition

A **proof by contrapositive** of the result

$$\text{Let } x \in S. \text{ If } P(x), \text{ then } Q(x).$$

is a direct proof of its contrapositive:

$$\text{Let } x \in S. \text{ If } \sim Q(x), \text{ then } \sim P(x).$$

or, a **proof by contrapositive** of the result

$$\text{For all } x \in S, \text{ if } P(x), \text{ then } Q(x).$$

is a direct proof of its contrapositive:

$$\text{For all } x \in S, \text{ if } \sim Q(x), \text{ then } \sim P(x).$$

# Proof by Contrapositive

Thus, to give a proof by contrapositive, we assume that $\sim Q(x)$ is true for an arbitrary element $x \in S$ and show that $\sim P(x)$ is true for this element $x$.

## Example 6

**Result** Let $x \in \mathbf{Z}$. If $5x - 7$ is even, then $x$ is odd.

**Proof.** Assume that $x$ is even. Then $x = 2a$ for some integer $a$. So

$$5x - 7 = 5(2a) - 7 = 10a - 7 = 10a - 8 + 1 = 2(5a - 4) + 1.$$

Since $5a - 4 \in \mathbf{Z}$, the integer $5x - 7$ is odd. □

## Example 7

**Result** Let $x \in \mathbf{Z}$. Then $11x - 7$ is even if and only if $x$ is odd.

**Proof.** There are two implications to prove here, namely,

(1) if $x$ is odd, then $11x - 7$ is even and

(2) if $11x - 7$ is even, then $x$ is odd.

We begin with (1). In this case, a direct proof is appropriate. Assume that $x$ is odd. Then $x = 2r + 1$, where $r \in \mathbf{Z}$. So

$$\begin{aligned} 11x - 7 &= 11(2r + 1) - 7 = 22r + 11 - 7 \\ &= 22r + 4 = 2(11r + 2). \end{aligned}$$

**Example 7 (continued)**

Since $11r + 2$ is an integer, $11x - 7$ is even.

We now prove (2), which is the converse of (1). We use a proof by contrapositive here. Assume that $x$ is even. Then $x = 2s$, where $s \in \mathbf{Z}$. Therefore,

$$\begin{aligned} 11x - 7 &= 11(2s) - 7 = 22s - 7 \\ &= 22s - 8 + 1 = 2(11s - 4) + 1. \end{aligned}$$

Since $11s - 4$ is an integer, $11x - 7$ is odd. □

# Proof by Contrapositive

The following example will be useful to us in the future; thus, we refer to it as a theorem.

**Theorem**

Let $x \in \mathbf{Z}$. Then $x^2$ is even if and only if $x$ is even.

**Proof.** Assume that $x$ is even. Then $x = 2a$ for some integer $a$. Therefore,

$$x^2 = (2a)^2 = 4a^2 = 2(2a^2).$$

Because $2a^2 \in \mathbf{Z}$, the integer $x^2$ is even.
For the converse, assume that $x$ is odd. So, $x = 2b + 1$, where $b \in \mathbf{Z}$. Then

$$x^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1.$$

Since $2b^2 + 2b$ is an integer, $x^2$ is odd. □

# Proof by Contrapositive

**Result to Prove:** Let $x \in \mathbf{Z}$. If $5x - 7$ is odd, then $9x + 2$ is even.

## Lemma

Let $x \in \mathbf{Z}$. If $5x - 7$ is odd, then $x$ is even

**Proof.** Assume that $x$ is odd. Then $x = 2y + 1$, where $y \in \mathbf{Z}$. Therefore,

$$5x - 7 = 5(2y + 1) - 7 = 10y - 2 = 2(5y - 1).$$

Since $5y - 1$ is an integer, $5x - 7$ is even. □

# Proof by Contrapositive

## Example 8

**Result** Let $x \in \mathbf{Z}$. If $5x - 7$ is odd, then $9x + 2$ is even.

**Proof.** Let $5x - 7$ be an odd integer. By the lemma, the integer $x$ is even. Since $x$ is even, $x = 2z$ for some integer $z$. Thus,

$$9x + 2 = 9(2z) + 2 = 18z + 2 = 2(9z + 1).$$

Because $9z + 1$ is an integer, $9x + 2$ is even. □

# Proof by Cases

## Definition

While attempting to give a proof of a mathematical statement concerning an element $x$ in some set $S$, it is sometimes useful to observe that $x$ possesses one of two or more properties. A common property which $x$ may possess is that of belonging to a particular subset of $S$. If we can verify the truth of the statement for each property that $x$ may have, then we have a proof of the statement. Such a proof is then divided into parts called **cases**, one case for each property that $x$ may possess or for each subset to which $x$ may belong. This method is called **proof by cases**. Indeed, it may be useful in a proof by cases to further divide a case into other cases, called **subcases**.

## Example 9

**Result** If $n \in \mathbf{Z}$, then $n^2 + 3n + 5$ is an odd integer.

**Proof.** We proceed by cases, according to whether $n$ is even or odd.

*Case* 1. *$n$ is even.* Then $n = 2x$ for some $x \in \mathbf{Z}$. So,

$$\begin{aligned} n^2 + 3n + 5 &= (2x)^2 + 3(2x) + 5 = 4x^2 + 6x + 5 \\ &= 2(2x^2 + 3x + 2) + 1. \end{aligned}$$

Since $2x^2 + 3x + 2 \in \mathbf{Z}$, the integer $n^2 + 3n + 5$ is odd.

**Example 9 (continued)**

*Case* 2. *n is odd.* Then $n = 2y + 1$, where $y \in \mathbf{Z}$. Thus,

$$\begin{aligned} n^2 + 3n + 5 &= (2y+1)^2 + 3(2y+1) + 5 = 4y^2 + 10y + 9 \\ &= 2(2y^2 + 5y + 4) + 1. \end{aligned}$$

Because $2y^2 + 5y + 4 \in \mathbf{Z}$, the integer $n^2 + 3n + 5$ is odd. □

# Proof by Cases

**Definition**

Two integers $x$ and $y$ are said to be **of the same parity** if $x$ and $y$ are both even or are both odd.

The integers $x$ and $y$ are **of opposite parity** if one of $x$ and $y$ is even and the other is odd.

For example, 5 and 13 are of the same parity, while 8 and 11 are of opposite parity.

Because the definition of two integers having the same (or opposite) parity requires the two integers to satisfy one of two properties, any result containing these terms is likely to be proved by cases. The following theorem presents a characterization of two integers that are of the same parity.

# Proof by Cases

## Theorem

Let $x, y \in \mathbf{Z}$. Then $x$ and $y$ are of the same parity if and only if $x + y$ is even.

**Proof.** First, assume that $x$ and $y$ are of the same parity. We consider two cases.

*Case* 1. *$x$ and $y$ are even.* Then $x = 2a$ and $y = 2b$ for some integers $a$ and $b$. So,

$$x + y = 2a + 2b = 2(a + b).$$

Since $a + b \in \mathbf{Z}$, the integer $x + y$ is even.

*Case* 2. *$x$ and $y$ are odd.* Then $x = 2a + 1$ and $y = 2b + 1$, where $a, b \in \mathbf{Z}$. Therefore,

$$x + y = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1).$$

Since $a + b + 1$ is an integer, $x + y$ is even.

## Proof (continued)

For the converse, assume that $x$ and $y$ are of opposite parity. Again, we consider two cases.

*Case* 1. *$x$ is even and $y$ is odd.* Then $x = 2a$ and $y = 2b + 1$, where $a, b \in \mathbf{Z}$. Then

$$x + y = 2a + (2b + 1) = 2(a + b) + 1.$$

Since $a + b \in \mathbf{Z}$, the integer $x + y$ is odd.

*Case* 2. *$x$ is odd and $y$ is even.* The proof is similar to the proof of the preceding case and is therefore omitted. □

# Proof by Cases

We use the phrase **without loss of generality** (some abbreviate this as *WOLOG* or *WLOG*) to indicate that the proofs of the two situations are similar, so the proof of only one of these is needed. Sometimes it is rather subjective to say that two situations are similar. We present one additional example to illustrate this.

# Proof by Cases

**Theorem**

Let $a$ and $b$ be integers. Then $ab$ is even if and only if $a$ is even or $b$ is even.

**Proof.** First, assume that $a$ is even or $b$ is even. Without loss of generality, let $a$ be even. Then $a = 2x$ for some integer $x$. Thus,

$$ab = (2x)b = 2(xb).$$

## Proof (continued)

Since $xb$ is an integer, $ab$ is even.

For the converse, assume that $a$ is odd and $b$ is odd. Then

$$a = 2x + 1 \text{ and } b = 2y + 1,$$

where $x, y \in \mathbf{Z}$. Hence,

$$\begin{aligned} ab &= (2x+1)(2y+1) = 4xy + 2x + 2y + 1 \\ &= 2(2xy + x + y) + 1. \end{aligned}$$

Since $2xy + x + y$ is an integer, $ab$ is odd. □

# Proof Evaluations

We have now stated several results and have given a proof of each result (sometimes preceding a proof by a proof strategy or following the proof with a proof analysis). Let's reverse this process by giving an example of a proof of a result but not stating the result being proved. We will follow the proof with several options for the statements of the result being proved.

# Proof Evaluations

## Example 10

Given below is a proof of a result.

**Proof.** Assume that $n$ is an odd integer. Then $n = 2k + 1$ for some integer $k$. Then

$$3n - 5 = 3(2k + 1) - 5 = 6k + 3 - 5 = 6k - 2 = 2(3k - 1).$$

Since $3k - 1$ is an integer, $3n - 5$ is even. □

Which of the following is proved above?

(1) $3n - 5$ is an even integer.
(2) If $n$ is an odd integer, then $3n - 5$ is an even integer.
(3) Let $n$ be an integer. If $3n - 5$ is an even integer, then $n$ is an odd integer.
(4) Let $n$ be an integer. If $3n - 5$ is an odd integer, then $n$ is an even integer.

# Proof Evaluations

**Problem** Evaluate the proposed proof of the following result.

## Example 11

**Result** If $x$ and $y$ are integers of the same parity, then $x - y$ is even.

**Proof.** Let $x$ and $y$ be two integers of the same parity. We consider two cases, according to whether $x$ and $y$ are both even or are both odd.

*Case* 1. *$x$ and $y$ are both even.* Let $x = 6$ and $y = 2$, which are both even. Then $x - y = 4$, which is even.

*Case* 2. *$x$ and $y$ are both odd.* Let $x = 7$ and $y = 1$, which are both odd. Then $x - y = 6$, which is even. □

**Problem** Evaluate the proposed proof of the following result.

## Example 12

**Result** If $m$ is an even integer and $n$ is an odd integer, then $3m + 5n$ is odd.

**Proof.** Let $m$ be an even integer and $n$ an odd integer. Then $m = 2k$ and $n = 2k + 1$, where $k \in \mathbf{Z}$. Therefore,

$$\begin{aligned} 3m + 5n &= 3(2k) + 5(2k + 1) = 6k + 10k + 5 \\ &= 16k + 5 = 2(8k + 2) + 1. \end{aligned}$$

Since $8k + 2$ is an integer, $3m + 5n$ is odd. □