Mathematical Proofs

Duncan Bandojo

November 26, 2020

Logic and Proofs
Ideas of axiomatic systems and proof within mathematics; the need for proof; the role of counter-examples in mathematics. Elementary logic; implication and negation; examples of negation of compound statements. Proof techniques... [6]

Contents

0 Introduction

These Mathematical Proofs notes are base on the book Mathematical Proofs: A Transition to Advanced Mathematics by G. Chartrand et al.

1 Logic

1.1 Statements

Definition (Statement)**.** A *statement* is a declarative sentence or assertion that has a truth value, namely *true* or *false*.

Example. The following are statements:

(i) The integer 3 is odd.

(ii) The integer 57 is prime.

Definition (Open Sentence)**.** An *open sentence* is a declarative sentence that contains one or more variables, each variable representing a value in some prescribed set, called the *domain* of the variable.

Example. The following are open sentences with variable x in some domain S.

1. $3x = 4$
2. $x^2 + 4x + 3 = 0$

An open sentence that contains a variable x is typically represented by $P(x)$, $Q(x)$ or $R(x)$. If $P(x)$ is an open sentence, where the domain of x is S, then we say $P(x)$ is an open sentence over the domain S.

1.2 Negations

Definition (Negation)**.** The *negation* of a statement P, denoted by $\sim P$ is the statement

not P

The truth table for $\sim P$ is

P	$\sim P$
T	**F**
T	**F**
F	**T**
F	**T**

Example. The negation of the statement

$$P_1 : \text{The integer 3 is odd.}$$

is

$$\sim P_1 : \text{The integer 3 is even.}$$

Example. The negation of the statement

$$P_2 : \text{The real number } r \text{ is at most } \sqrt{2}$$

is

$$\sim P_2 : \text{The real number } r \text{ is greater than } \sqrt{2}$$

1.3 Disjunctions and Conjunctions

Definition (Disjunction)**.** The *disjunction* of the statements P and Q is the statement

$$P \textbf{ or } Q$$

denoted by $P \vee Q$.

Definition. The *conjunction* of the statements P and Q is the statement

$$P \textbf{ and } Q$$

denoted by $P \wedge Q$

The truth table for $P \vee Q$ and $P \wedge Q$ is

P	Q	$P \vee Q$	$P \wedge Q$
T	T	**T**	**T**
T	F	**T**	**F**
F	T	**T**	**F**
F	F	**F**	**F**

1.4 Implications

Definition (Implication)**.** For statements P and Q, the *implication* (or *conditional*) is the statement

$$\textbf{If } P, \textbf{ then } Q.$$

denoted by $P \Rightarrow Q$. Which can also be expressed as

$$P \textbf{ implies } Q.$$

The truth table for $P \Rightarrow Q$ is

P	Q	$P \Rightarrow Q$
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

In summary, $P \Rightarrow Q$ is false when P is True and Q is false.

The following have the same truth value

- $\sim (P \Rightarrow Q)$ and P $\wedge \sim Q$
- $P \Rightarrow Q$ and $\sim P \vee Q$

The following are equivalent statements

- If P, then Q
- Q if P
- P implies Q
- P only if Q

- P is sufficient for Q
- Q is necessary for P

Example. A triangle is *equilateral* if the lengths of its three sides are the same, while *isosceles* if any two of its three sides are the same.

For a triangle $T \in S$, let

$$P(T)\text{: } T \text{ is equilateral} \qquad \text{and} \qquad Q(T)\text{: } T \text{ is isosceles}$$

Consider the implication $P(T) \Rightarrow Q(T)$

(i) For an equilateral triangle T_1, both $P(T_1)$ and $Q(T_1)$ are true and so $P(T_1) \Rightarrow Q(T_1)$ is also true.

(ii) If T_2 is not an equilateral triangle, then $P(T_2)$ is a false statement and so $P(T_2) \Rightarrow Q(T_2)$ is true regardless of the truth of $Q(T_2)$.

We now state $P(T) \Rightarrow Q(T)$ in a variety of ways:

- If T is an equilateral triangle, then T is isosceles.
- A triangle T is an isosceles if T is equilateral.
- A triangle T is equilateral only if T is isosceles.
- For a triangle T to be isosceles, it is sufficient that T be equilateral.
- For a triangle T to be equilateral, it is necessary that T be isosceles.

1.5 Biconditionals

Definition (Converse)**.** For statements (or open sentences) P and Q, the implication $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$.

Example. For the statements

$$P_1\text{: 3 is an odd integer} \qquad \text{and} \qquad P_2\text{: 57 is prime.}$$

the converse of the implication

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

is the implication

$$P \Rightarrow Q\text{: If 57 is prime, then 3 is an odd integer.}$$

Definition (Biconditional)**.** For statements (or open sentences) P and Q, the conjunction

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

of the implication $P \Rightarrow Q$ and its converse is called the *biconditional* of P and Q, denoted by $P \Leftrightarrow Q$.

Truth table of $P \Leftrightarrow Q$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
T	T	T	T	T	**T**
T	F	F	T	F	**F**
F	T	T	F	F	**F**
F	F	T	T	T	**T**

The biconditional $P \Leftarrow Q$ is often stated as

P **is equivalent to** Q.

or

P **if and only if** Q.

or as

P **is necessary and sufficient for** Q.

For statements P and Q, it then follows that the biconditional *"P if and only if Q"* is true only when P and Q have the same truth values.

Example. For the open sentences

$$P(T)\text{: } T \text{ is equilateral} \qquad \text{and} \qquad Q(T)\text{: } T \text{ is isosceles.}$$

over the domain S of all triangles, the converse of the implication

$$P(T) \Rightarrow Q(T)\text{: If } T \text{ is equilateral, then } T \text{ is isosceles.}$$

is the implication

$$Q(T) \Rightarrow P(T)\text{: If } T \text{ is isosceles, then } T \text{ is equilateral.}$$

We noted that $P(T) \Rightarrow Q(T$ is a true statement for all triangles T, while $Q(T) \Rightarrow P(T)$ is a false statement when T is an isosceles triangle that is not equilateral. On the other hand, the second implication becomes a true statement for all other triangles T. Therefore, the biconditional

$$P(T) \Leftrightarrow Q(T)\text{: } T \text{ is equilateral if and only if } T \text{ is isosceles.}$$

is false for all triangles that are isosceles and not equilateral, while it is true for all other triangles T.

1.6 Tautologies and Contradictions

Definition (Logical Connectives)**.** A *logical connective* is a symbol or word used to connect two or more sentences n a grammatically valid way, such that the value of the compound sentence produced depends only on that of the original sentences and on the meaning of the connective.

$$\sim,\ \wedge,\ \vee,\ \Rightarrow,\ \Leftrightarrow$$

Definition (Compound statement)**.** a *compound statement*is a statement composedof one or more given statements (called *component statements* in this context) and at least one logical connective.

Example. For a given statement P, its negation $\sim P$ is a compound statement.

Definition (Tautology)**.** A compound statement S is called a *tautology* if it is true for all possible combinations of truth values of the component statements

Example. The compound statement $P \vee \sim P$ is a tautology

P	$\sim P$	$P \vee \sim P$
T	F	**T**
T	F	**T**
F	T	**T**
F	T	**T**

Example. For statements P and Q, the compound statement $(\sim Q) \vee (P \Rightarrow Q)$ is a tautology, as is verified in the truth table.

P	Q	$\sim Q$	$P \Rightarrow Q$	$(\sim Q) \vee (P \Rightarrow Q)$
T	T	F	T	**T**
T	F	T	F	**T**
F	T	F	T	**T**
F	F	T	T	**T**

Definition (Contradiction)**.** A compound statement S is called a *contradiction* if it is false for all possible combinations of truth values of the component statements.

Example. The compound statement $P \wedge \sim P$ is a contradiction.

P	$\sim P$	$P \wedge \sim P$
T	F	**F**
T	F	**F**
F	T	**F**
F	T	**F**

Example. For statements P and Q, the compound statement $(P \wedge Q) \wedge (Q \Rightarrow (\sim P))$ is a contradiction, as is verified in the truth table.

P	Q	$\sim P$	$P \wedge Q$	$Q \Rightarrow (\sim P)$	$(P \wedge Q) \wedge (Q \Rightarrow (\sim P))$
T	T	F	T	F	**F**
T	F	F	F	T	**F**
F	T	T	F	T	**F**
F	F	T	F	T	**F**

Definition (Modus Ponens)**.** For statements P and Q, $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ is a tautology. (This logical argument form is called *modus ponens*)

If P is true and $P \Rightarrow Q$ is true, then Q is true.

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$(P \wedge (P \Rightarrow Q) \Rightarrow Q)$
T	T	T	T	**T**
T	F	F	F	**T**
F	T	T	F	**T**
F	F	T	F	**T**

Definition (Syllogism)**.** For statements P, Q, and R show that $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow R)$ is a tautology. (This logical argument form is called *syllogism*)

If $P \Rightarrow Q$ and $Q \Rightarrow R$, then $P \Rightarrow R$

1.7 Logical Equivalence

Definition (Logical Equivalence)**.** Let R and S be two compound statements involving the same component statements P and Q. Then R and S are called *logically equivalent* if R and S have the same truth values for all combinations of truth values of their component statements denoted by

$$R \equiv S$$

Example. The statements $P \implies Q$ and $(\sim P) \vee Q$ are logically equivalent,in other words $P \implies Q \equiv (\sim P) \vee Q$.

P	Q	$\sim P$	$P \Rightarrow Q$	$(\sim P) \vee Q$
T	T	F	**T**	**T**
T	F	F	**F**	**F**
F	T	T	**T**	**T**
F	F	T	**T**	**T**

Logical equivalence guarantess the truth of the other statement. If we can establish the truth of the statement $(\sim P) \vee Q$, then the logical equivalence of $P \Rightarrow Q$ and $(\sim P) \vee Q$ guarantees $P \Rightarrow Q$ is also true.

Example. For the following statement

If you earn an A on the final exam, then you will receive an A for the final grade.

We need only know that the student did not receive an A on he final exam or the student received an A as a final grade to see that the instructor kept her promise.

Theorem. Let P and Q be two statements. Then

$$P \Rightarrow Q \text{ and } (\sim P) \vee Q$$

are logically equivalent.

For the following statements

$$Q \Rightarrow P \text{ is written as ”}P \text{ if } Q\text{”}$$

$$P \Rightarrow Q \text{ is written as ”}P \text{ only if } Q\text{”}.$$

their conjunction can be written as ”P if Q and P only if Q”, or more simply

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

1.8 Fundamental Properties of Logical Equivalence

Theorem. For statements P, Q, and R.

1. *Commutative Laws*
   - $P \vee Q \equiv Q \vee P$
   - $P \wedge Q \equiv Q \wedge P$
2. *Associative Laws*

- $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$
- $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

3. *Distributive laws*
    - $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
    - $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
4. *De Morgan's Laws*
    - $\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$
    - $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$

Theorem. For statements P and Q

- $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q)$
- $\sim (P \Rightarrow Q) \equiv (P \wedge (\sim Q)) \vee (Q \wedge (\sim P))$

Proof. We make use of the De Morgan's Laws

$$\begin{aligned}(P \Rightarrow Q) &\equiv \sim ((\sim P) \vee Q)\\ &\equiv (\sim (\sim P)) \wedge (\sim Q)\\ &\equiv P \wedge \sim Q\end{aligned}$$

□

Proof. We make use of the De Morgan's Laws

$$\begin{aligned}\sim (P \Leftarrow Q) &\equiv \sim ((P \Rightarrow Q) \wedge (Q \Rightarrow P))\\ &\equiv (\sim (P \Rightarrow Q)) \vee (\sim (Q \Rightarrow P))\\ &\equiv (P \wedge (\sim Q)) \vee (Q \wedge (\sim P))\end{aligned}$$

□

1.9 Quantified Statements

If $P(x)$ is an open sentence over a domain S, then $P(x)$ is a statement for each $x \in S$. *Quantification* is a method to convert open sentences to a *quantified statement.*

Definition (Universal Quantifier)**.** Adding the phrase *"For every"* $x \in S$ to $P(x)$, where *"for every"* is referred as universal quantifier denoted by $\forall$

$$\forall x \in S,\ P(x).$$

in words

For every $x \in S$, $P(x)$

The quantified statement is true if $P(x)$ is true for every $x \in S$; while false if for at least one element $x \in S$, $P(x)$ is false.

Definition (Existential Quantifier)**.** Each of the phrases *"there exists"*, *"there is"*, *"for some"*, and *"for at least one"* is referred to as an *existential quantifier* and is denoted by the symbol $\exists$. The quantified statement

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

can be expressed in words by

$$\text{There exists } x \in S \text{ such that } P(x).$$

The quantified statement is true if $P(x)$ is true for at least one element $x \in S$; while false if $P(x)$ is false for all $x \in S$.

Example. The quantified statement $\forall x \in S,\ P(x)$ can be expressed

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

Example. Consider $P(x):\ x^2 \geq 0$ over $\mathbb{R}$. Then

$$\forall x \in \mathbb{R},\ x^2 \geq 0$$

or equivalently

$$\text{For every real number } x,\ x^2 \geq 0.$$

or

$$\text{If } x \text{ is a real number, then } x^2 \geq 0$$

The statement $\forall x \in \mathbb{R},\ x^2 \geq 0$ is true

Example. Consider the open sentence $Q(x):\ x^2 \leq 0$.

The statement $\forall x \in \mathbb{R},\ Q(x)$ is false, since $Q(1)$ is false. If it were not the case, then there must exist x such that $x^2 > 0$. This negation

$$\text{There exists a real number } x \text{ such that } x^2 > 0$$

can be written

$$\exists x \in \mathbb{R},\ x^2 > 0 \text{ or } \exists x \in \mathbb{R},\ \sim Q(x).$$

More generally, if we are considering an open sentence $P(x)$ over a domain S, then

$$\sim (\forall x \in S, P(x)) \equiv \exists x \in S, \sim P(x).$$

Example. Consider $A = \{1, 2, 3\}$ and $\mathcal{P}(A)$, the power set of A.

$$\text{For every set } B \in \mathcal{P}(A),\ A - B \neq \emptyset$$

is false since for the subset $B = A = \{1, 2, 3\}$, $A - B = \emptyset$.

It can be written as

$$\text{If } B \subseteq A, \text{ then } A - B \neq \emptyset$$

The negation is

$$\text{There exists } B \in \mathcal{P}(A) \text{ such that } A - B = \emptyset$$

and can be expressed as

There exist some subset B of A such that $A - B = \emptyset$

Generally, if we are considering an open sentence $Q(x)$ over domain S.

$$\sim (\exists x \in S,\ Q(x)) \ \equiv\ \forall x \in S,\ \sim Q(x)$$

For an open sentence containing two variables, the domains of the variables need not be the same.

$$\sim (\forall s \in S,\ \forall t \in T,\ Q(s,t)) \equiv \exists s \in S,\ \exists t \in T,\ \sim Q(s,t)$$

1.10 Characterizations

Definition (Characterization)**.** Suppose that some concept (or object) is expressed in an open sentence $P(x)$ over a domain S and $Q(x)$ is another open sentence over the domain S concerning the concept. We say that this concept is *characterized* by $Q(x)$, if $\forall x \in S,\ P(x) \Leftrightarrow Q(x)$ is a true statement. The statement $\forall x \in S,\ P(x) \Leftrightarrow Q(x)$ is then called a *characterization* of this concept.

Example. Irrational numbers are defined as real numbers that are not rational and are characterized as real numbers whose decimal expansions are nonrepeating.

This provides a characterization of irrational numbers:

A real number r is irrational if and only if r has a nonrepeating decimal expansion.

Example. We saw that equilateral triangles are defined as triangles whose sides are equal. They are characterized, however, as triangles whose angles are equal.

Therefore, we have the characterization:

A triangle T is equilateral if and only if T has three equal angles.

You might think that equilateral triangles are also characterized as those triangles having three equal sides but the associated biconditional:

A triangle T is equilateral if and only if T has three equal sides

is not a characterization of equilateral triangles. Indeed, this is the definition we gave of equilateral triangles.

Example. Define an integer n to be odd if n is not even. Then a characterization of odd integers is

An integer n is odd if and only if n^2 is odd

2 Direct Proof and Proof by Contrapostive

We will now start the main gist of the notes. For a given true mathematical statement, how can we show that it is true?

Definition (Axiom)**.** A true mathematical statement whose truth is accepted without proof.

Definition (Theorem)**.** A true mathematical statement whose truth can be verified

Definition (Corrolary)**.** A mathematical result that can be deduced from, and is thereby a consequence of, some earlier result

Definition (Lemma)**.** A mathematical result that is useful in establishing the truth of some other result

Most theorems (or results) are stated as implications. We now begin our study of proofs of such mathematical statements.

2.1 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.

Definition (Trivial Proof)**.** 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 $Q(x)$ is true for all $x \in S$ (regardless of the truth value of $P(x)$, according to the truth table for implication.

Example. Let $x \in \mathbb{R}$. 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, $x^2 + 1 > 0$. □

Since we verified the truth of $Q(x)$ for every $x \in \mathbb{R}$, it follows that $P(x) \Rightarrow Q(x)$ is true for all $x \in \mathbb{R}$. The proof did not depend on $P(x)$, in fact we could have replaced it by any hypothesis and the result would still be true.

Definition (Vacuous Proof)**.** 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.

Example. Let $x \in \mathbb{R}$. If $x^2 - 2x + 2 \leq 0$, then $x^2 \geq 8$.

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 $x \in \mathbb{R}$ and the implication is true. □

Even though the trivial and vacuous proofs are rarely encountered in mathematics, they are important reminders of the truth table for implication.

2.2 Direct Proofs

Typically, when we are discussing an implication $P(x) \Rightarrow Q(x)$ over a domain S, there is some connection between $P(x)$ and $Q(x)$. That is, the truth value of $Q(x)$ for a particular $x \in S$ often depends on the truth value of $P(x)$ for that same element x, or the truth value of $P(x)$ depends on the truth value of $Q(x)$.

Definition (Direct Proof)**.** Let $P(x)$ and $Q(x)$ be open sentences over a domain S. 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.

If $P(x)$ is true, then $P(x) \Rightarrow Q(x)$ follows vacuously. 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.

We define the set of all even integers as

$$E = \{2k : k \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

and the set if all odd integers as

$$O = \{2k + 1 : k \in \mathbb{Z}\} = \{\ldots, -5, -3, -1, 1, 3, 5 \ldots\}.$$

Example. If n is an even integer, then $-5n - 3$ is an odd integer.

Proof. Let n be an even integer. Then $n = 2x$, where x is an integer. Therefore,

$$-5n - 3 = -5(2x) - 3 = -10x - 3 = -10x - 4 + 1 = 2(-5x - 2) + 1.$$

Since $-5x - 2$ is an integer, $-5n - 3$ is an odd integer. □

Example. If n is an odd integer, then $4n^3 + 2n - 1$ is odd.

Proof. Assume that n is odd. Then $n = 2y + 1$ for some integer y. Therefore,

$$\begin{aligned} 4n^3 + 2n - 1 &= 4(2y + 1)^3 + 2(2y + 1) - 1 \\ &= 4(8y^3 + 12y^2 + 6y + 1) + 4y + 2 - 1 \\ &= 32y^3 + 48y^2 + 28y + 5 \\ &= 2(16y^3 + 24y^2 + 14y + 2) + 1. \end{aligned}$$

Since $16y^3 + 24y^2 + 14y + 2$ is an integer, $4n^3 + 2n - 1$ is odd. □

Although the direct proof that we gave is correct, this is not the *desired* proof. Indeed, had we observed that

$$4n^3 + 2n - 1 = 2(2n^3 + n - 1) + 1$$

and that $2n^3 + n - 1 \in \mathbb{Z}$, we could have concluded immediately that $4n^3 + 2n - 1$ is odd for every integer n. Hence, a trivial proof could be given and, in fact, preferred.

2.3 Proof by Contrapositive

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

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**

Example. Let $x \in \mathbb{Z}$. 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 $5a - 4 \in \mathbb{Z}$, the integer $5x - 7$ is odd. □

Theorem. Let $x \in \mathbb{Z}$. 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 $2a^2 \in \mathbb{Z}$, the integer x^2 is even.

For the converse, assume that x is odd. So, $x = 2b + 1$, where $b \in \mathbb{Z}$. Then

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

Since $2b^2 + 2b \in \mathbb{Z}$, x^2 is odd. □

Suppose that we have been successful in proving $P(x) \Rightarrow Q(x)$ for all x in some domain S (by whatever method). We therefore know that for every $x \in S$ for which the statement $P(x)$ is true, the statement $Q(x)$ is true. Also, for any $x \in S$ for which the statement $Q(x)$ is false, the statement $P(x)$ is false.

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

Lemma. Let $x \in \mathbb{Z}$. If $5x - 7$ is odd, then x 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. □

Alternative Proof. Assume that $5x - 7$ is odd. Then $5x - 7 = 2n + 1$ for some integer n. Observe that

$$9x + 2 = (5x - 7) + (4x + 9) = 2n + 1 + 4x + 9$$

$$= 2n + 4x + 10 = 2(n + 2x + 5).$$

Because $n + 2x + 5$ is an integer, $9x + 2$ is even. □

2.4 Proof by Cases

Definition. For a mathematical statement concerning an element $x \in S$, 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

For example, in a proof of $\forall n \in \mathbb{Z}, R(n)$, it might be convenient to use a proof by cases whose proof is divided into the two cases

- Case 1: *n is even*
- Case 2: *n is odd*

or in the case of $\forall x \in \mathbb{R}, P(x)$

- Case 1: $x = 0$
- Case 2: $x < 0$
- Case 3: $x > 0$

we also might attempt to prove $\forall n \in \mathbb{N}, P(n)$ using the cases

- Case 1: $n = 1$
- Case 2: $n \geq 2$

Furthermore, for $S = \mathbb{Z} - \{0\}$, we might try to prove $\forall x, y \in S, P(x, y)$ by using the cases.

- Case 1: $xy > 0$
- Case 2: $xy < 0$

Case 1 could, in fact, be divided into two subcases

$$\textit{Subcase } 1.1 : x > 0 \text{ and } y > 0. \text{ and } \textit{Subcase } 1.2 : x < 0 \text{ and } y < 0.$$

while Case 2 could be divided into two subcases

$$\textit{Subcase } 2.1 : x > 0 \text{ and } y < 0. \text{ and } \textit{Subcase } 2.2 : x < 0 \text{ and } y > 0.$$

Definition (Same Parity)**.** Two integers x and y are said to be *of the same parity* if x and y are both even or are both odd

Definition (Opposite Parity)**.** The integers x and y are *of opposite parity* if one of x and y is even and the other is odd.

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

Proof. ($\Rightarrow$) 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 $a + b \in Z$, the integer $x + y$ is even.
- Case 2: x and y are odd. Then $x = 2a + 1$ and$y = 2b + 1$, where $a, b \in Z$. 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

($\Leftarrow$) 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 $a, b \in Z$. Then
$$x + y = 2a + (2b + 1) = 2(a + b) + 1$$
Since $a + b \in \mathbb{Z}$, 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.

□

Remark. Although there is always some concern when omitting steps or proofs, it should be clear that it is truly a waste of effort to give a proof of the case when x is odd and y. However, there is an alternative when the converse is considered.

For the converse, assume that x and y are of opposite parity. *Without loss of generality*, assume that x is even and y is odd. Then $x = 2a$ and $y = 2b + 1$, where $a, b \in Z$. Then
$$x + y = 2a + (2b + 1) = 2(a + b) + 1$$
Since $a + b \in \mathbb{Z}$, the integer $x + y$ is odd.

We used the phrase ***without loss of generality*** to indicate that the proofs of the two situations are similar, so the proof of only one of these is needed.

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

Proof. ($\Leftarrow$) 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, $ab = (2x)b = 2(xb)$. Since xb is an integer, ab is even.

($\Rightarrow$) For the converse, assume that a is odd and b is odd. Then $a = 2x + 1$ and $b = 2y + 1$, where $x, y \in Z$. Hence,
$$ab = (2x + 1)(2y + 1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1.$$
Since $2xy + x + y$ is an integer, ab is odd. □

Result. Let $\mathcal{P} = \{A, B, C\}$ be a partition of the set $\mathbb{Z}$ of integers, where
$$A = \{n : n = 2a \text{ where } a \text{ is an odd integer}\}$$
$$B = \{n : n = 2b \text{ where } b \text{ is an even integer}\}$$
$$C = \{n : n \text{ is an odd integer}\}$$
If x and y are integers belonging to distinct elements of $\mathcal{P}$, then $x + y \in A \cup C$

Proof. (Consider three cases) □

2.5 Proof Evaluations

We now reverse the process, where we give the proof of some result, and we need to find the result.

Example. Evaluate the proposed proof of the following 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 $k \in \mathbb{Z}$. 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. □

Proof Evaluation. There is a mistake in the second sentence of the proposed proof, where it is written that $m = 2k$ and $n = 2k + 1$, where $k \in \mathbb{Z}$.

Since the same symbol k is used for both m and n, we have inadvertently added the assumption that $n = m + 1$. This is incorrect, as it was never stated that n and m must be consecutive integers.

In other words, we should write $m = 2k$ and $n = 2\ell + 1$, where $k, \ell \in \mathbb{Z}$. □

3 More on Direct Proof and Proof by Contrapositive

3.1 Proofs on Divisibility of Integers

Definition. In general, for integers a and b with $a \neq 0$, we say that a divides b, written as

$$a \mid b$$

if there is an integer c such that $b = ac$.

Hence, if n is an even integer, then $2 \mid n$; moreover, if 2 divides some integer n, then n is even. That is, an integer n is even if and only if $2 \mid n$.

Therefore, the *Theorem*,

For integers a and b, ab is even, if and only if a or b is even.

can be rewritten as

For integers a and b, $2 \mid ab$ if and only if $2 \mid a$ or $2 \mid b$.

If $a \mid b$, then we also say that b is a *multiple* of a and that a is a *divisor* of b. Thus, every even integer is a multiple of 2. If a does not divide b, then we write $a \nmid b$.

For example, $4 \mid 48$, since $4 \cdot 12 = 48$ and $-3 \mid 57$ since $57 = (-3) \cdot (19)$. On the other hand, $4 \nmid 66$ as there is no integer c such that $66 = 4c$.

3.2 Proofs of Congruence of Integers

Definition. For integers a, b and $n \geq 2$, we say that a is **congruent** to b **modulo** n, written

$$a \equiv b \pmod{n}, \text{ if } n \mid (a - b)$$

3.3 Proofs on Real Numbers

3.4 Proofs on Sets

3.5 Fundamental Properties of Set Operations

3.6 Proofs on Cartesian Products of Sets