The Foundations: Logic and Proofs

Mongi BLEL

King Saud University

August 30, 2019

Table of contents

The Foundations: Logic and Proofs

Logic is the hygiene the mathematician practices to keep his ideas healthy and strong

Hermann Weyl

Our discussion begins with an introduction to the basic building blocks of logic propositions.

Definition

A proposition (تقرير) is a declarative sentence (اَلجملة اَلخبرية) (that is, a sentence that declares a fact). The only statements that are considered are propositions, which contain no variables. Propositions are either true or false, but not both.

Example 1 :
All the following declarative sentences are propositions.

1. Any integer is odd or even.
2. $1 + 1 = 2$.
3. $2 + 2 = 3$.

Examples of non-propositions:

Example 2 :

1. What time is it?
2. $x + 1 = 2$, (may be true, may not be true, it depends on the value of x.)
3. $x.0 = 0$, (always true, but it's still not a proposition because of the variable.)
4. $x.0 = 1$, (always false, but not a proposition because of the variable.)

The truth value of a proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition. The area of logic that deals with propositions is called the propositional calculus or propositional logic.
We will use letters such as $p, q, r, s, \ldots$ or $A, B, C, D, \ldots$ to represent propositions. The letters are called logical variables.

Propositions can be constructed from other propositions using logical connectives

1. Negation: $\neg$ (not alternatively $-$),
2. Conjunction $\wedge$ (and),
3. Disjunction $\vee$ (or),
4. Implication $\rightarrow$
5. Biconditional $\leftrightarrow$

The Negation of a Proposition

Definition

Let p be a proposition. The negation of p, denoted by $\neg p$ (also denoted by $\bar{p}$), is the statement "It is not the case that p." The proposition $\neg p$ is read "not p." The truth value of the negation of p, $\neg p$, is the opposite of the truth value of p.

Example 3 :
The negation of the proposition “Badr’s PC runs Linux “
The negation is:
“It is not the case that Badr’s PC runs Linux.” This negation can be more simply expressed as “Badr’s PC does not run Linux.”

The Truth Table for the Negation of a Proposition.

p	$\neg p$
T	F
F	T

The conjunction of Propositions

Definition

Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, is the proposition "p and q." The conjunction $p \wedge q$ is true when both p and q are true and is false otherwise.

The truth table for the conjunction of two propositions.

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

In this case, we will say that the compound propositions $p \wedge q$ and $q \wedge p$ are equivalent propositions. We also say that the operator $\wedge$ is commutative.

The disjunction of Propositions

Definition

Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, is the proposition "p or q." The disjunction $p \vee q$ is false when both p and q are false and is true otherwise.

The truth table for the disjunction of two propositions.

p	q	$p \vee q$	$q \vee p$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

In this case, we will say that the compound propositions $p \vee q$ and $q \vee p$ are equivalent propositions. We also say that the operator $\vee$ is commutative.

The exclusive or of Propositions

Definition

Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

The truth table for the exclusive "or"

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

The conditional statement

Definition

Let p and q be propositions. The conditional statement $p \to q$ is the proposition "if p, then q." The conditional statement $p \to q$ is false when p is true and q is false, and is true otherwise.

In the conditional statement $p \to q$, p is called the hypothesis (or antecedent or premise) and q is called the conclusion (or consequence).
The statement $p \to q$ is called a conditional statement because $p \to q$ asserts that q is true on the condition that p holds. A conditional statement is also called an implication.
When $p \to q$, p is called a sufficient condition for q , q is a necessary condition for p.

The statement $p \to q$ is true when both p and q are true and when p is false (no matter what truth value q has). Conditional statements play such an essential role in mathematical reasoning.

Terminology is used to express $p \to q$.

"if p, then q"	" p implies q"
"if p, q"	"p only if q"
"p is sufficient for q"	"a sufficient condition for q is p"
"q if p"	"q whenever p"
"q when p"	"q is necessary for p"
"a necessary condition for p is q"	"q follows from p"
"q unless $\neg p$"	

The truth table for the conditional statement $p \to q$ of two propositions.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Converse, Contrapositive and Inverse

We can form some new conditional statements starting with a conditional statement $p \to q$. In particular, there are three related conditional statements that occur so often that they have special names.

1. The proposition $q \to p$ is called the **converse** of $p \to q$.
2. The proposition $\neg q \to \neg p$ is called the **contrapositive** of $p \to q$.
3. The proposition $\neg p \to \neg q$ is called the **inverse** of $p \to q$.

We will see that of these three conditional statements formed from $p \to q$, only the contrapositive always has the same truth value as $p \to q$.

Exercise

What are the contrapositive, the converse, and the inverse of the conditional statement
"The home team wins whenever it is raining".

Solution: Because "q whenever p" is one of the ways to express the conditional statement $p \to q$, the original statement can be rewritten as:
If it is raining, then the home team wins. Consequently, the **contrapositive** is:
If the home team does not win, then it is not raining.
The **converse** is : If the home team wins, then it is raining.
The **inverse** is : If it is not raining, then the home team does not win.
Only the contrapositive is equivalent to the original statement.

Biconditional Statements

Definition

Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition "p if and only if q". The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called bi-implications.

The biconditional $p \leftrightarrow q$ is true when the conditional statements $p \rightarrow q$ and $q \rightarrow p$ are true, and is false otherwise.
That is why we use the words "if and only if" to express this logical connective and why it is symbolically written by combining the symbols $\rightarrow$ and $\leftarrow$.
The last way of expressing the biconditional statement $p \leftrightarrow q$ uses the abbreviation "iff" for "if and only if."
There are some other common ways to express $p \leftrightarrow q$:
"p is necessary and sufficient for q"
"if p then q", and conversely if "q then p".

The Truth Table for the Biconditional $p \leftrightarrow q$ of Two Propositions..

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Truth Tables of Compound Propositions

We have now introduced four important logical connectives: **conjunctions**, **disjunctions**, **conditional statements**, and **biconditional statements** as well as negations. We can use these connectives to build up complicated compound propositions involving any number of propositional variables. We can use truth tables to determine the truth values of these compound propositions.

Example 4 :
Construction of the truth table of the compound proposition $(p \vee \neg q) \to (p \wedge q)$.

Truth Table of $(p \vee \neg q) \to (p \wedge q)$					
p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \to (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Definition

1. A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a tautology. You can think of a **tautology** as a rule of logic.
2. A compound proposition that is always false is called a **contradiction**. In other words, a contradiction is false for every assignment of truth values to its simple components.
3. A compound proposition that is neither a tautology nor a contradiction is called a **contingency**.

We will use T to denote any tautology and F to denote any contradiction.

Logical Equivalences

Compound propositions that have the same truth values in all possible cases are called logically equivalent. We can also define this notion as follows.

Definition

The compound propositions p and q are called logically equivalent and denoted $p \equiv q$ if $p \leftrightarrow q$ is a tautology.

Example 5 :
We can construct examples of tautologies and contradictions using just one propositional variable.
$p \vee \neg p$ is always true, it is a tautology and $p \wedge \neg p$ is always false, it is a contradiction.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

Theorem [De Morgan's Laws]

$\neg(p \wedge q) \equiv \neg p \vee \neg q$
$\neg(p \vee q) \equiv \neg p \wedge \neg q.$

Truth Table of $\neg(p \wedge q) \equiv \neg p \vee \neg q$ and $\neg(p \vee q) \equiv \neg p \wedge \neg q$									
p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
T	T	F	F	T	F	F	T	F	F
T	F	F	T	T	F	F	F	T	T
F	T	T	F	T	F	F	F	T	T
F	F	T	T	F	T	T	F	T	T

Exercise 1 :
Prove that $p \to q$ and $\neg p \vee q$ are logically equivalent.

Solution

Truth Table of $p \to q \equiv \neg p \vee q$				
p	q	$\neg p$	$p \to q$	$\neg p \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Exercise 2 :
Prove that $p \to q$ and $\neg q \to \neg p$ are logically equivalent.

Solution

Truth Table of $p \to q \equiv \neg q \to \neg p$					
p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Exercise 3 :
Prove that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent. (This is the distributive law of disjunction over conjunction.)

Solution

Truth Table of $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$							
p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Exercise 4 :
Prove that $p \wedge (q \vee r)$ and $(p \wedge q) \vee (p \wedge r)$ are logically equivalent. (This is the distributive law of conjunction over disjunction.)

Solution

Truth Table of $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$							
p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Equivalence	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws

Logical equivalences involving conditional statements

1. $p \to q \equiv \neg p \vee q$
2. $p \to q \equiv \neg q \to \neg p$
3. $p \to (q \vee r) \equiv (p \wedge \neg q) \to r \equiv (p \wedge \neg r) \to q.$
4. $(p \vee q) \to r \equiv (p \to r) \wedge (q \to r).$
5. $p \to (q \to r) \equiv (p \wedge q) \to r.$

Logical equivalences involving biconditional statements

1. $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$,
2. $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$,
3. $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$.

Exercise

Prove that $(p \wedge q) \rightarrow (p \vee q)$ *is a tautology.*

Solution

p	q	$p \wedge q$	$p \vee q$	$(p \wedge q) \rightarrow (p \vee q)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

Proof without truth table:

$$\begin{aligned}(p \wedge q) \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q)\\ &\equiv \neg p \vee \neg q \vee p \vee q\\ &\equiv T.\end{aligned}$$

Exercise

Prove that $(p \wedge q) \wedge (\neg p \vee \neg q)$ *is a contradiction.*

Solution

p	q	$p \wedge q$	$\neg p \vee \neg q$	$(p \wedge q) \wedge (\neg p \vee \neg q)$
T	T	T	F	F
T	F	F	T	F
F	T	F	T	F
F	F	F	T	F

Proof without truth table:

$$\begin{aligned}(p \wedge q) \wedge (\neg p \vee \neg q) &\equiv (p \wedge q \wedge \neg p) \vee (p \wedge q \wedge \neg q)\\ &\equiv F.\end{aligned}$$

Exercise

Proof without truth table that

1. $\neg(p \to q)$ and $p \wedge \neg q$ are logically equivalent,
2. $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$,

Solution

1. $$\begin{aligned}\neg(p \to q) &\equiv \neg(\neg p \vee q)\\ &\equiv \neg(\neg p) \wedge \neg q\\ &\equiv p \wedge \neg q\end{aligned}$$

2. $$\begin{aligned}\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q)\\ &\equiv \neg p \wedge [\neg(\neg p) \vee \neg q]\\ &\equiv \neg p \wedge (p \vee \neg q)\\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)\\ &\equiv F \vee (\neg p \wedge \neg q) \equiv \neg p \wedge \neg q\end{aligned}$$

Predicates

Definition

A predicate (مسند)is a statement that contains variables (predicate variables), and they may be true or false depending on the values of these variables.

Example 6 :
If $P(x) =$ "x^2 is greater than x" is a predicate. It contains one predicate variable x. If we choose $x \in]0, 1]$, $P(x)$ is a proposition always false.
If we choose $x \in]1, +\infty[$, $P(x)$ is a proposition always true.

Definition

1. The domain of a predicate variable is the collection of all possible values that the variable may take.
2. The truth domain of a predicate variable is the set of the variable that takes the predicate true.

The Universal Quantifier

Definition

The universal quantification of $P(x)$ is the statement "$P(x)$ for all values of x in the domain."
The notation $\forall x;\ P(x)$ denotes the universal quantification of $P(x)$.
The symbol $\forall$ is called the **universal quantifier**.
An element for which $P(x)$ is false is called a **counterexample** of $\forall x;\ P(x)$.

Example 7 :
This is a formal way to say that for all values that a predicate variable x can take in a domain D, the predicate is true:

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

for all x belonging to the real numbers $x^2 \geq 0$.

Example 8 :
Let $p(x)$ be the predicate "$x > 0$".
If $D = \mathbb{N}$ the proposition "$\forall\ x : x > 0$" is true.
If $D = \mathbb{Z}$ the proposition "$\forall\ x : x > 0$" is false.
So, the universal set is important.

The Existential Quantifier

Definition

The existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$".
We use the notation $\exists x;\ P(x)$ for the existential quantification of $P(x)$.
The symbol $\exists$ is called the existential quantifier.

Example 9 :

$$\exists x \in \mathbb{R}, \quad x^2 > x.$$

Truth value of quantified statements

1. $\forall x \in D,\ P(x)$ i.e. $P(x)$ is true for every $x \in D$.
   It is false whenever there is at least one x in D for which $P(x)$ is false.
   $\neg(\forall x \in D,\ P(x)) \equiv \exists x \in D,\ \neg(P(x))$ i.e. There is one $x \in D$ for which $P(x)$ is false.

   Example 10 :
   If $D = \{x_1, \ldots, x_n\}$, we have the following equivalence:

   $$(\forall x \in D,\ P(x)) \equiv (P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)).$$

   $$\neg(\forall x \in D,\ P(x)) \equiv \exists j \in \{1, \ldots, n\},\ \neg P(x_j).$$

2. $\exists x \in D,\ P(x)$. It is true when $P(x)$ is true for at least one x in D. It is false when $P(x)$ is false for all x in D.
   $\neg(\exists x \in D,\ P(x)) \equiv \forall x \in D,\ \neg(P(x))$ i.e. for all $x \in D$, $P(x)$ is false.

   Example 11 :
   If $D = \{x_1, \ldots, x_n\}$, we have the following equivalence:

$$(\exists x \in D,\ P(x)) \equiv (P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)).$$

$$\neg(\exists x \in D,\ P(x)) \equiv \forall j \in \{1, \ldots, n\},\ \neg P(x_j).$$

3. We can similarly assign truth values to combinations of predicates, or negation of combinations of predicates. The equivalence

$$\neg(\forall x \in D,\ P(x) \wedge Q(x)) \equiv \exists x \in D,\ \neg(P(x) \wedge Q(x)),$$

or

$$\neg(\forall x \in D,\ P(x) \wedge Q(x)) \equiv \exists x \in D,\ \neg P(x) \vee \neg Q(x).$$

How To Determine Truth Value

1. **Method of exhaustion**
   Suppose that the domain D is finite and we want to show that $\forall x \in D,\ P(x)$ is true. Try all cases.
   For example, if $D = \{-1, 2, 3\}$, and $P(x) =$ "$x^2 - x - 1 \geq 0$", then just compute $x^2 - x + 1$ for all the values of $x \in D$ to conclude that this true or false.
2. **Method of case**
   Suppose you want to show that $(\exists x \in D,\ P(x))$ is true. For this, we just need to find an $x \in D$ for which $P(x)$ is true.

Example 12 :
To show that "$\exists x \in [-1, 1],\ x^3 = 2x$" is true, take $x = 0$. Similarly, if to show that $\forall\ x \in [1, +\infty[, x^3 > 2x$ is false, it is enough to find one counterexample. Take $x = 1$.

3. **Method of logic derivation** This method consists of using logical steps to transform one logical expression into another.

Example 13 :
If $D = \{x_1, \dots x_n\}$ and we want to know the truth value of $\exists x \in D,\ (P(x) \vee Q(x))$. This is equivalent to the following:

$$\begin{aligned}\exists x \in D,\ (P(x) \vee Q(x)) &\equiv \exists j \in \{1, \dots, n\},\ P(x_j) \vee Q(x_j)\\ &\equiv (P(x_1) \vee Q(x_1)) \vee \dots \vee (P(x_n) \vee Q(x_n))\\ &\equiv (\exists x \in D,\ (P(x)) \vee (\exists x \in D,\ Q(x)).\end{aligned}$$

Examples

1. Let $P(x)$ be the statement "$x^2 - x + 1 > 0.$" What is the truth value of the quantification $\forall x\ P(x)$, where the domain consists of all real numbers?
   $P(x)$ is true for every real number x, because,
   $P(x) = (x - \frac{1}{2})^2 + \frac{3}{4}$.
2. Let $Q(x)$ be the statement "$x^2 - 3x + 1 > 0.$" What is the truth value of the quantification $\forall x;\ P(x)$, where the domain consists of all real numbers?
   $Q(x)$ is not true for every real number x, for instance, $Q(1)$ is false. That is, $x = 1$ is a counterexample for the statement $\forall x;\ Q(x)$. Thus $\forall x;\ Q(x)$ is false.

Examples

Find the negations of the following statements

1. $\forall x;\ (\sin x \leq x)$,
2. $\exists x;\ (\sin x = x)$.

Solution

1. The negation of $\forall x;\ (\sin x \leq x)$ is the statement $\exists x;\ (\sin x > x)$.
2. The negation of $\exists x;\ (\sin x = x)$ is the statement $\forall x;\ (\sin x \neq x)$.

Proof Techniques

Definition

1. A proof is a chain of deductions that establishes the truth of a statement.
2. A theorem is a statement obtained by a correct deduction or a sequence of correct deductions (that is, using explicitly the allowed rules of inference) from logical axioms and, possibly, other results of the same type already established.
3. A lemma is a "helping theorem" or a result which is needed to prove a theorem.

Definition

4. A corollary is a result which follows directly from a theorem.
5. Less important theorems are sometimes called propositions.

Remarks

1. Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
2. Many theorems have the form: $\forall x \in D;\ (P(x) \rightarrow Q(x))$ is true. To prove, we show that for all arbitrary element c of the domain, $P(c) \rightarrow Q(c)$ is true. So, we must prove something of the form: $p \rightarrow q$ is true.
   We have two trivial cases
   • Trivial Proof: If we know that q is true, then $p \rightarrow q$ is true as well.
   • Vacuous Proof: If we know that p is false then $p \rightarrow q$ is true.

In which follows we will see how to apply the logic rules to justify different proof techniques. We will discuss four proof techniques: **Direct proof, proof by induction, proof by contradiction and proof by contradiction.**

Direct Proof

A **direct proof** of a conditional statement $p \to q$ is constructed when the first step is the assumption that p is true, subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.
A direct proof shows that a conditional statement $p \to q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs. In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Example 14 :
Give a direct proof of "If n is an odd integer, then n^2 is odd."
Solution
Note that the statement is $\forall n;\ (P(n) \to Q(n))$, where $P(n)$ is "n is an odd integer" and $Q(n)$ is "n^2 is odd."
We assume that the hypothesis of this conditional statement is true, namely, we assume that $n = 2k + 1$ for some $k \in \mathbb{N}$.
$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is also odd.

Example 15 :
Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.
(An integer a is a perfect square if there is an integer b such that $a = b^2$.)

Solution
We assume that the hypothesis of this conditional statement is true, namely, we assume that $m = p^2$ and $n = q^2$. Hence, $mn = p^2q^2 = (pq)^2$, then mn is also a perfect square.

Proof by Contraposition

We need other methods of proving statements of the form $\forall x\,(P(x) \to Q(x))$. The method now is to do not start with the premises and end with the conclusion. This method is called **a indirect proof**.

A useful type of indirect proof is known as **proof by contraposition**. This method consists to use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$. We take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, to show that $\neg p$ is true.

Example 16 :

1. Prove $3n + 2$ is odd, then n is odd.
2. Prove that if $n = pq$, then $p \leq \sqrt{n}$ or $q \leq \sqrt{n}$. $(n, p, q \in \mathbb{N})$.

Solutions

1. If $n = 2k$ for some integer k, then
   $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$ is even.
2. We assume that the statement $(p \leq \sqrt{n}) \vee (q \leq \sqrt{n})$ is false, which means that both $p > \sqrt{n}$ and $q > \sqrt{n}$ are false. Then $n = pq > \sqrt{n}\sqrt{n} = n$ which is false.

Proof by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. We conclude that $\neg p$ is false, which means that p is true.

Example 17 :
$\sqrt{2}$ is irrational.
Assume that $\sqrt{2}$ is rational. There exist integers p and q with $\sqrt{2} = \frac{p}{q}$, where $q \neq 0$ and p and q have no common factors. When both sides of this equation are squared, it follows that $2q^2 = p^2$. Hence p^2 is even, let $p = 2r$ for some integer r. Thus, $2q^2 = 4r^2$ and $q^2 = 2r^2$ and q is even, which is impossible. Then $\sqrt{2}$ is irrational.

Example 18 :
Prove by contradiction that "if $3n+2$ is odd, then n is odd."
Let p be "$3n+2$ is odd" and q be "n is odd." To construct a proof by contradiction, assume that both p and $\neg q$ are true. That is, assume that $3n+2$ is odd and n is even. Then there is $k \in \mathbb{N}$ such that $n = 2k$. This implies that
$3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$. We have a contradiction. This completes the proof by contradiction.

Example 19 :

Prove that there is no largest prime number.

Assume that there is a largest prime number. Hence, we can list all the primes $p_1, \ldots, p_n$. Let

$$m = p_1.p_2 \ldots .p_n - 1.$$

None of the prime numbers on the list divides m. Therefore, either m is prime or there is a smaller prime that divides m. This contradicts the assumption that there is a largest prime.

Therefore, there is no largest prime.

Proof of Equivalence

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity of this approach is based on the tautology $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$.

Example 20 :
Prove that n is odd if and only if n^2 is odd."
Let p is "n is odd" and q is "n^2 is odd." To prove this result, we need to show that $p \to q$ and $q \to p$ are true.
We have already shown that $p \to q$ is true.
We prove that $q \to p$ by contraposition.
If n is odd, then $n = 2k - 1$ for some integer k.
$n^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$, which proves that q is false.

Proof by cases

A proof by cases of a mathematical statement should include the following:

1. Determine all possible cases which must be considered in order to prove the mathematical statement,
2. write the proof for each case.

Example 21 :
Prove that 3 does not divide the numbers $n^2 + 2n - 1$ for all $n \in \mathbb{N}$.
Case 1: Assume that $n = 3k$, then $n^2 + 2n - 1 = 3(3k^2 + 2k) - 1$ and 3 does not divide $n^2 + 2n - 1$.
Case 2: Assume that $n = 3k + 1$, then $n^2 + 2n - 1 = 3(3k^2 + 4k) + 2$ and 3 does not divide $n^2 + 2n - 1$.
Case 3: Assume that $n = 3k + 2$, then $n^2 + 2n - 1 = 3(3k^2 + 6k + 2) + 1$ and 3 does not divide $n^2 + 2n - 1$.

Example 22 :
Prove that $x + |x-1| \geq 1$ for all real numbers x.
Case1: Assume that $x \geq 1$. Then $x-1 \geq 0$ and $|x-1| = x-1$, so that $x + |x-1| = x + (x-1) = 2x - 1 \geq 2 - 1 = 1$, i.e., $x + |x-1| \geq 1$.
Case2: Assume that $x < 1$. Then $x - 1 < 0$ and $|x-1| = -(x-1) = 1 - x$, so that $x + |x-1| = x + (1-x) = 1$, i.e., $x + |x-1| \geq 1$.
Thus, for all possible cases, it has been proven that $x + |x-1| \geq 1$.

Exercise

1. *If x is a real number, then $|x+3| - x > 2$.*
2. *If x is a real number, then $|x-1| + |x+5| \geq 6$.*
3. *The expression $2m^2 - 1$ is odd for all integers m .*
4. *If n is an even integer, then $n = 4k$ or $n = 4k - 2$ for some integer k .*
5. *If a and b are real numbers, then $|\,|a| - |b|\,| \leq |a - b|$.*

Proof by working backward

A proof by working backward of a mathematical statement should include the following.

1. Begin with the final result, which must be proven true,
2. work backward step-by-step, writing equivalent statements, until a connection with the assumptions of the problem.

Example 23 :
Prove that $x^2 + y^2 \geq 2xy$ for all real numbers x and y.
$x^2 + y^2 \geq 2xy$ is true if and only if $x^2 + y^2 - 2xy \geq 0$ is true if and only if $(x - y)^2 \geq 0$ which is true. Since the last statement is true, all of the equivalent statements are true. In particular, $x^2 + y^2 \geq 2xy$.

Exercise

Prove the following:

1. *The expression* $x + \dfrac{9}{x} \geq 6$ *for all real numbers* $x > 0$ *.*
2. *If* $n^3 + 5n + 6$ *is divisible by* 3 *for some integer* n*, then* $(n+1)^3 + 5(n+1) + 6$ *is divisible by* 3*.*
3. *The expression* $\dfrac{x^4}{4} + (x+1)^3 > \dfrac{(x+1)^4}{4}$ *for all real numbers* $x \geq -1$ *.*
4. *There is a fixed positive integer* N *for which* $\dfrac{3}{n} < \dfrac{n-4}{n+10}$ *for all integers* $n \geq N$*.*

Mathematical Induction

This proof technique is to prove statements of the form $\forall n \in \mathbb{N}, P(n)$. We have two steps to do the proof:

1. We show that $P(1)$ is true. (Basis step)
2. Assume that $P(n)$ is true for some $n \geq 1$ (induction hypothesis) and prove that $P(n+1)$ is then true. (Inductive step)

Example 24 :

$$S_n = \sum_{k=1}^{n} (2k-1)^2 = \frac{n(4n^2-1)}{3}.$$

$S_1 = 1$ and assume that $S_n = \dfrac{n(4n^2-1)}{3}$ for some $n \in \mathbb{N}$.

$$\begin{aligned} S_{n+1} &= S_n + (2n+1)^2 = \frac{n(4n^2-1)}{3} + (2n+1)^2 \\ &= (2n+1)\frac{n(2n-1)+3(2n+1)}{3} \\ &= \frac{(n+1)(4(n+1)^2-1)}{3}. \end{aligned}$$

Example 25 :

$$\sum_{k=1}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

$S_1 = 1$ and assume that $S_n = \dfrac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$ for some $n \in \mathbb{N}$.

$$\begin{aligned} S_{n+1} &= S_n + (n+1)^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} + (n+1)^4 \\ &= (n+1)\frac{n(2n+1)(3n^2+3n-1) + 30(n+1)^3}{30} \\ &= \frac{(n+1)(n+2)(2n+3)(3(n+1)^2+3(n+1)-1)}{30}. \end{aligned}$$

Example 26 :

$$S_n = \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

$S_1 = \frac{1}{2}$ and assume that $S_n = \dfrac{n}{n+1}$ for some $n \in \mathbb{N}$.

$$\begin{aligned} S_{n+1} &= S_n + \frac{1}{(n+1)(n+2)} \\ &= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\ &= \frac{1}{n+1}(n + \frac{1}{n+2}) = \frac{n+1}{n+2}. \end{aligned}$$

Example 27 :
Let $(a_n)_n$ be a sequence defined by $a_0 \in (0,1]$, and for all $n \geq 0$, $a_{n+1} = \frac{2a_n + a_n^2}{4}$.
Prove that $\forall n \geq 0$, $a_n \in (0,1]$ and $a_n \leq a_{n+1}$.
Base step: $a_0 \in (0,1]$.
Inductive step:
Assume that $a_n \in (0,1]$. Then $0 < a_{n+1} = \frac{2a_n + a_n^2}{4} \leq \frac{3}{4} \leq 1$.
Then $a_n \in (0,1]$ for all $n \geq 0$.
Base step: $a_1 = \frac{2a_0 + a_0^2}{4} \leq = \frac{2a_0 + a_0}{4} = \frac{3}{4}a_0 \leq a_0$.
Inductive step:
Assume that $a_n \leq a_{n-1}$. Then $a_{n+1} = \frac{2a_n + a_n^2}{4} \leq \frac{3}{4}a_n \leq a_n$.
Then $a_{n+1} \leq a_n$ for all $n \geq 0$.

Strong Induction

We want to prove $\forall n \in \mathbb{N}$, $(P(n))$ is true.
Basis step: show $P(1)$ is true.
Inductive step: show $(P(1) \wedge \ldots \wedge P(n)) \rightarrow P(n+1)$ for all $n \in \mathbb{N}$.
(Assume n is arbitrary and $P(1), \ldots, P(n)$ are true. Show $P(n+1)$ is true.)

Example 28 :
Let $(a_n)_n$ be a sequence defined by $a_1 = 2$, $a_2 = 4$ and for all $n \geq 3$, $a_n = a_{n-1} + 2a_{n-2}$.
Prove that $\forall n \geq 1$, $a_n = 2^n$.
Base step: $a_1 = 2 = 2^1$, $a_2 = 4 = 2^2$.
Inductive step:
Assume for $n \geq 3$ fixed but random that: $a_{n-1} = 2^{n-1}$ and $a_{n-2} = 2^{n-2}$.
Then $a_n = a_{n-1} + 2a_{n-2} = 2^{n-1} + 2^{n-1} = 2^n$.