Contents

CHAPTER 1
Preliminaries

1.1 Logic

Propositions

Definition 1.1. A *proposition* or *statement* is a declarative sentence which is true T or false F, but not both.

Example 1.1 Some propositions:

- Brussels is in Belgium: T
- $2 + 2 = 3$: F
- $x = 2$ is a solution of $x^2 = 4$: T

Many propositions are *composite*, that is, composed of *subpropositions* and various *connectives* discussed subsequently. Such composite propositions are called *compound propositions*. A proposition is said to be *primitive* if it cannot be broken down into simpler propositions.

The fundamental property of a compound proposition is that its truth value is completely determined by the truth values of its subpropositions together with the way in which they are connected to form the compound proposition.

Connectives

Any two propositions $\mathcal{P}$ and $\mathcal{Q}$ can be combined by the word "and" to form a compound proposition called the *conjunction* of $\mathcal{P}$ and $\mathcal{Q}$, denoted $\mathcal{P} \wedge \mathcal{Q}$ and read "$\mathcal{P}$ and $\mathcal{Q}$". If $\mathcal{P}$ and $\mathcal{Q}$ are true, then $\mathcal{P} \wedge \mathcal{Q}$ is true; otherwise $\mathcal{P} \wedge \mathcal{Q}$ is false. The truth value of $\mathcal{P} \wedge \mathcal{Q}$ may be defined equivalently by the following truth table:

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \wedge \mathcal{Q}$
T	T	T
T	F	F
F	T	F
F	F	F

Any two propositions $\mathcal{P}$ and $\mathcal{Q}$ can be combined by the word "or" to form a compound proposition called the *disjunction* of $\mathcal{P}$ and $\mathcal{Q}$, denoted $\mathcal{P} \vee \mathcal{Q}$ and read "$\mathcal{P}$ or $\mathcal{Q}$". If $\mathcal{P}$ and $\mathcal{Q}$ are false, then $\mathcal{P} \vee \mathcal{Q}$ is false; otherwise $\mathcal{P} \vee \mathcal{Q}$ is true. The truth value of $\mathcal{P} \vee \mathcal{Q}$ may be defined equivalently by the following truth table:

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \vee \mathcal{Q}$
T	T	T
T	F	T
F	T	T
F	F	F

Any proposition $\mathcal{P}$ can be preceded by the word "not" to form a new proposition called the *negation* of $\mathcal{P}$, denoted $\neg\mathcal{P}$ and read "not $\mathcal{P}$". If $\mathcal{P}$ is true, then $\neg\mathcal{P}$ is false; and if If $\mathcal{P}$ is false, then $\neg\mathcal{P}$ is true. The truth value of $\neg\mathcal{P}$ may be defined equivalently by the following truth table:

$\mathcal{P}$	$\neg\mathcal{P}$
T	F
F	T

A proposition containing only T in the last column of its truth table is called a *tautology* denoted $\top$, eg.

$\mathcal{P}$	$\neg\mathcal{P}$	$\mathcal{P} \vee \neg\mathcal{P}$
T	F	T
F	T	T

A proposition containing only F in the last column of its truth table is called a *contradiction* denoted $\bot$, eg.

$\mathcal{P}$	$\neg\mathcal{P}$	$\mathcal{P} \wedge \neg\mathcal{P}$
T	F	F
F	T	F

Logical Equivalence

The propositions $\mathcal{P}$ and $\mathcal{Q}$ are said to be *logically equivalent*, denoted by $\mathcal{P} \equiv \mathcal{Q}$ if they have identical truth tables.

Example 1.2 Show that $\neg(\mathcal{P} \wedge \mathcal{Q}) \equiv \neg\mathcal{P} \vee \neg\mathcal{Q}$

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \wedge \mathcal{Q}$	$\neg(\mathcal{P} \wedge \mathcal{Q})$	$\neg\mathcal{P}$	$\neg\mathcal{Q}$	$\neg\mathcal{P} \vee \neg\mathcal{Q}$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Theorem 1.1. *Let $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{R}$ be propositions.*

1. $\mathcal{P} \vee \mathcal{P} \equiv \mathcal{P}$ *and* $\mathcal{P} \wedge \mathcal{P} \equiv \mathcal{P}$ *(idempotent laws)*
2. $\mathcal{P} \vee \mathcal{Q} \equiv \mathcal{Q} \vee \mathcal{P}$ *and* $\mathcal{P} \wedge \mathcal{Q} \equiv \mathcal{Q} \wedge \mathcal{P}$ *(commutative laws)*
3. $\mathcal{P} \vee (\mathcal{Q} \vee \mathcal{R}) \equiv (\mathcal{P} \vee (\mathcal{Q}) \vee \mathcal{R} \equiv \mathcal{P} \vee \mathcal{Q} \vee \mathcal{R}$ *and* $\mathcal{P} \wedge (\mathcal{Q} \wedge \mathcal{R}) \equiv (\mathcal{P} \wedge (\mathcal{Q}) \wedge \mathcal{R} \equiv \mathcal{P} \wedge \mathcal{Q} \wedge \mathcal{R}$ *(associative laws)*
4. $\mathcal{P} \wedge (\mathcal{Q} \vee \mathcal{R}) \equiv (\mathcal{P} \wedge \mathcal{Q}) \vee (\mathcal{P} \wedge \mathcal{R})$ *and* $\mathcal{P} \vee (\mathcal{Q} \wedge \mathcal{R}) \equiv (\mathcal{P} \vee \mathcal{Q}) \wedge (\mathcal{P} \vee \mathcal{R})$ *(distributive laws)*
5. $\mathcal{P} \vee \bot \equiv \mathcal{P}$ *and* $\mathcal{P} \wedge \bot \equiv \bot$ *(identity laws)*
6. $\mathcal{P} \vee \top \equiv \top$ *and* $\mathcal{P} \wedge \top \equiv \mathcal{P}$ *(identity laws)*
7. $\mathcal{P} \vee \neg\mathcal{P} \equiv \top$ *and* $\mathcal{P} \wedge \neg\mathcal{P} \equiv \bot$ *(complement laws)*
8. $\neg\top \equiv \bot$ *and* $\neg\bot \equiv \top$ *(complement laws)*
9. $\neg(\neg\mathcal{P}) \equiv \mathcal{P}$ *(involution law)*
10. $\neg(\mathcal{P} \vee \mathcal{Q}) \equiv \neg\mathcal{P} \wedge \neg\mathcal{Q}$ *and* $\neg(\mathcal{P} \wedge \mathcal{Q}) \equiv \neg\mathcal{P} \vee \neg\mathcal{Q}$ *(DeMorgan's laws)*

Exercise 1.1 Use a truth table to show the logical equivalence of the propositions in the theorems.

Conditional Propositions

Many statements are of the form "If $\mathcal{P}$ then $\mathcal{Q}$". Such statements are called *conditional propositions*, and are denoted by $\mathcal{P} \Rightarrow \mathcal{Q}$. The conditional $\mathcal{P} \Rightarrow \mathcal{Q}$ is frequently read "$\mathcal{P}$ implies $\mathcal{Q}$ ", or "$\mathcal{P}$ only if $\mathcal{Q}$".

Another common statement is of the form "$\mathcal{P}$ if and only if $\mathcal{Q}$". Such statements are called *biconditional propositions*, and are denoted by $\mathcal{P} \Leftrightarrow \mathcal{Q}$.

Their truth values are defined by following truth tables:

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \Rightarrow \mathcal{Q}$	$\neg\mathcal{P}$	$\neg\mathcal{P} \vee \mathcal{Q}$	$\mathcal{P} \Leftrightarrow \mathcal{Q}$	$\mathcal{Q} \Rightarrow \mathcal{P}$	$(\mathcal{P} \Rightarrow \mathcal{Q}) \wedge (\mathcal{Q} \Rightarrow \mathcal{P})$
T	T	T	F	T	T	T	T
T	F	F	F	F	F	T	F
F	T	T	T	T	F	F	F
F	F	T	T	T	T	T	T

Observe that:

- The conditional $\mathcal{P} \Rightarrow \mathcal{Q}$ is false only when the first part $\mathcal{P}$ is true and the second part $\mathcal{Q}$ is false. Accordingly, when $\mathcal{P}$ is false, the conditonal $\mathcal{P} \Rightarrow \mathcal{Q}$ is false regardless of the truth value of $\mathcal{Q}$.
- $\mathcal{P} \Rightarrow \mathcal{Q}$ is logically equivalent to $\neg\mathcal{P} \vee \mathcal{Q}$.
- The biconditional $\mathcal{P} \Leftrightarrow \mathcal{Q}$ is true whenever $\mathcal{P}$ and $\mathcal{Q}$ have the same truth values and false otherwise.
- $\mathcal{P} \Leftrightarrow \mathcal{Q}$ is logically equivalent to $(\mathcal{P} \Rightarrow \mathcal{Q}) \wedge (\mathcal{Q} \Rightarrow \mathcal{P})$. $\mathcal{Q} \Rightarrow \mathcal{P}$ is called the *converse* of $\mathcal{P} \Rightarrow \mathcal{Q}$.

1.2 Sets and Functions

Sets

Definition 1.2. A *set* is a collection of objects called *elements* of the set.

In general, we denote a set by a capital letter and an element by a lower case letter. If an element a belongs to a set S we write $a \in S$. If a does not belong to S we write $a \notin S$.

A set can be described by listing its elements in braces separated by commas, eg. $\{a, e, i, o, u\}$, or by describing some property held by all elements, eg. $\{x \mid x \text{ is a vowel}\}$.

If each element of a set A belongs to a set B we call A a *subset* of B, written $A \subset B$. If $A \subset B$ and $B \subset A$ we call A and B *equal* and write $A = B$.

Often we restrict our discussion to subsets of a particular set called the *universe* or the *universal set* denoted by Ω, eg. the set of the letters of the roman alphabet.

It is useful to consider a set having no elements at all. This is called the *empty set* and is denoted by $\varnothing$. It is a subset on any set.

A universe Ω can be represented geometrically by the set of points inside a rectangle. In such case subsets of Ω such as A and B are represented by sets of points inside ellipses. Such diagrams, called *Venn diagrams*, often serve to provide geometric intuition regarding possible relationships between sets.

Theorem 1.2. *If $A \subset B$ and $B \subset C$, then $A \subset C$.*

Proof. SET THE CONTEXT: Let A, B and C be sets for which $A \subset B$ and $B \subset C$.

ASSERT THE HYPOTHESIS: Suppose $x \in A$.

LIST IMPLICATIONS:

1. Since $x \in A$, it is true that $x \in B$ by the definition of subset.
2. Since $x \in B$, it is true that $x \in C$ by the definition of subset.

STATE THE CONCLUSION: Therefore, by the definition of subset, $A \subset C$. □

Set Operations

The set of all elements which belong to A or B is called the *union* of A and B and is denoted by $A \cup B$.

The set of all elements which belong to A and B is called the *intersection* of A and B and is denoted by $A \cap B$. Two sets A and B such that $A \cap B = \varnothing$ are called *disjoint sets*.

The set consisting of all elements of A which do not belong to B is called the *difference* of A and B denoted by $A \setminus B$.

The set consisting of all elements of Ω which do not belong to A is called the *complement* of A denoted by $A^c = \Omega \setminus A$.

Theorem 1.3. *Let A, B and C be sets.*

1. $A \cup A = A$ *and* $A \cap A = A$ *(idempotent laws)*
2. $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$ *(commutative laws)*
3. $A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C$ *(associative laws)*
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributive laws)*
5. $A \cup \varnothing = A$ *and* $A \cap \varnothing = \varnothing$ *(identity laws)*
6. $A \cup \Omega = \Omega$ *and* $A \cap \Omega = A$ *(identity laws)*
7. $A \cup A^c = \Omega$ *and* $A \cap A^c = \varnothing$ *(complement laws)*
8. $\Omega^c = \varnothing$ *and* $\varnothing^c = \Omega$ *(complement laws)*
9. $(A^c)^c = A$ *(involution law)*
10. $(A \cup B)^c = A^c \cap B^c$ *and* $(A \cap B)^c = A^c \cup B^c$ *(DeMorgan's laws)*
11. $A \setminus B = A \cap B^c$
12. *If* $A \subset B$, *then* $B^c \subset A^c$
13. $A = (A \cap B) \cup (A \cap B^c)$

Example 1.3 Proof the first law of DeMorgan.

Proof. *SET THE CONTEXT:* Let A and B be any two sets.

PART 1: $(A \cup B)^c \subset A^c \cap B^c$

ASSERT THE HYPOTHESIS: Suppose $x \in (A \cup B)^c$.

LIST IMPLICATIONS:

1. By the definition of set complement, $x \notin A \cup B$.
2. If $x \in A$ or $x \in B$, then $x \in A \cup B$ which is false.
3. Thus, $x \notin A$ and $x \notin B$, so by the definition of set complement $x \in A^c$ and $x \in B^c$.
4. By the definition of set intersection $x \in A^c \cap B^c$.

CONCLUSION PART 1: Hence, from the definition of subset, it follows that $(A \cup B)^c \subset A^c \cap B^c$.

PART 2: $A^c \cap B^c \subset (A \cup B)^c$

ASSERT THE HYPOTHESIS: Suppose $x \in A^c \cap B^c$.

LIST IMPLICATIONS:

1. By the definition of set intersection, $x \in A^c$ and $x \in B^c$.
2. Thus by the definition of set complement, $x \notin A$ and $x \notin B$.
3. If $x \in A \cup B$, then by the definition of the union, it would follow that $x \in A$ or $x \in B$ which is false.
4. Thus, $x \notin A \cup B$, and by definition of set complement $x \in (A \cup B)^c$.

CONCLUSION PART 2: Hence, from the definition of subset, it follows that $A^c \cap B^c \subset (A \cup B)^c$.

STATE THE CONCLUSION: Therefore, because $(A \cup B)^c$ and $A^c \cap B^c$ are subsets of each other, by the definition of set equality $(A \cup B)^c = A^c \cap B^c$. □

Exercise 1.2 Proof the other theorems.

Cartesian Product

The set of all *ordered pairs* of elements (x, y) where $x \in A$ and $y \in B$ is called the *Cartesian product* or *product set* of A and B and is denoted by $A \times B$. In general, $A \times B \neq B \times A$.

The notion of Cartesian product can be generalized to ordered tuples of element $(x, y, z, \ldots)$.

Functions

Definition 1.3. A function f from a set X to a set Y, often written $f : X \to Y$, is a rule which assigns to each $x \in X$ a unique element $y \in Y$.

The element y is called the *image* of x under f and is denoted by $f(x)$. If $A \subset X$, then $f(A)$ is the set of all elements $f(x)$ where $x \in A$ and is called the *image* of A under f. Symbols x and y are called *variables*.

A function $f : X \to Y$ can also be defined as a subset of the Cartesian product $X \times Y$ such that if (x_1, y_1) and (x_2, y_2) are in this subset and $x_1 = x_2$, then $y_1 = y_2$.

The set X is called the *domain* of f and $f(X)$ is called the *range* of f. If $Y = f(X)$ we say that f is from X onto Y and refer to f as a *surjective* function.

If an element $a \in A \subset X$ maps into an element $b \in B \subset Y$, then a is called the *inverse image* of b under f and is denoted by $f^{-1}(b)$. The set of all $x \in X$ for which $f(x) \in B$ is called the *inverse image* of B under f and is denoted by $f^{-1}(B)$.

If $f(a_1) = f(a_2)$ only when $a_1 = a_2$, we say that f is an *injective* function.

If a function $f : X \to Y$ is both surjective and injective, we say there is a one to one correspondence between X and Y and call f a *bijective* function. Given any element $y \in Y$, there will be only one element $f^{-1}(y)$ in X. In such case f^{-1} will define a function from Y to X called the *inverse function*.

Cardinal Numbers

Two sets A and B are called *equivalent* and we write $A \sim B$ if there exists a one to one correspondence between A and B.

Theorem 1.4. *If $A \sim B$ and $B \sim C$, then $A \sim C$.*

Axiom 1.1. Following axioms define the natural numbers and are known as the axioms of Peano.

1. 0 is a natural number.
2. Every natural number has a successor which is also a natural number.
3. 0 is not the successor of any natural number.
4. If the successor of x equals the successor of y, then x equals y.
5. If a statement is true for 0, and if the truth of that statement for a natural number implies its truth for the successor of that natural number, then the statement is true

for every natural number. (*Axiom of induction*)

The set of natural number is denoted by $\mathbb{N}$.

A set which is equivalent to the set $\{1, 2, 3, \ldots, n\}$ for some $n \in \mathbb{N}$ is called *finite*; otherwise it is called *infinite*.

An infinite set which is equivalent to the set of natural numbers is called *denumerable*; otherwise it is called *non-denumerable*.

A set which is either empty, finite or denumerable is called *countable*; otherwise it is called *non-countable*.

The *cardinal number* of the set $\{1, 2, 3, \ldots, n\}$ as well as any set equivalent to it is defined to be n. The cardinal number of any denumerable set is defined as $\aleph_0$, *aleph null*. The cardinal number of the empty set $\varnothing$ is defined as 0.

The cardinal number of a set S is denoted by $\#S$.

Propositional Functions and Quantifiers

Let A be a given set. A *propositional function* defined on A is a function $A \to \{T, F\} : \mathcal{P}(x)$ which has the property that $\mathcal{P}(a)$ is true or false for each $a \in A$. That is, $\mathcal{P}(x)$ becomes a proposition (with a truth value) whenever any element $a \in A$ is substituted for the variable x. The set $T_{\mathcal{P}}$ of all elements of $a \in A$ for which $\mathcal{P}(a)$ is true is called the *truth set* of $\mathcal{P}(x)$.

Example 1.4 Find the truth set $T_{\mathcal{P}}$ of each propositional function $\mathcal{P}(x)$ defined on $\mathbb{N}$.

- Let $\mathcal{P}(x)$ be " $x + 2 > 7$ ". Then $T_{\mathcal{P}} = \{x \mid x \in \mathbb{N}, x + 2 > 7\} = \{6, 7, 8, \ldots\}$.
- Let $\mathcal{P}(x)$ be " $x + 5 < 3$ ". Then $T_{\mathcal{P}} = \{x \mid x \in \mathbb{N}, x + 5 < 3\} = \varnothing$. In other words, $\mathcal{P}(x)$ is false for any natural number.
- Let $\mathcal{P}(x)$ be " $x + 5 > 1$ ". Then $T_{\mathcal{P}} = \{x \mid x \in \mathbb{N}, x + 5 > 1\} = \mathbb{N}$. Thus $\mathcal{P}(x)$ is true for every natural number.

Let $\mathcal{P}(x)$ be a propositional function defined on a set A. Consider the expression " $\forall x \in A : \mathcal{P}(x)$ " which reads "For every x in A, $\mathcal{P}(x)$ is a true statement". The symbol $\forall$ which reads "for all" or "for every" is called the *universal quantifier*. The proposition $\forall x \in A : \mathcal{P}(x)$ expresses that the truth set of $\mathcal{P}(x)$ is the entire set A, or symbolically, $T_{\mathcal{P}} = \{x \mid x \in A, \mathcal{P}(x)\} = A$.

Example 1.5 Some propositions using the universal quantifier:

- The proposition $\forall n \in \mathbb{N} : n + 4 > 3$ is true since $\{n : n \in \mathbb{N}, n + 4 > 3\} = \mathbb{N}$.
- The proposition $\forall n \in \mathbb{N} : n + 2 > 8$ is false since $\{n : n \in \mathbb{N}, n + 2 > 8\} = \{7, 8, 9, \ldots\}$.
- The symbol $\forall$ can be used to define the intersection of an indexed collection $\{A_i : i \in I\}$ of sets A_i as follows: $\bigcap_{i \in I} A_i = \{x : \forall i \in I, x \in A_i\}$.

Let $\mathcal{P}(x)$ be a propositional function defined on a set A. Consider the expression " $\exists x \in A : \mathcal{P}(x)$ " which reads "There exists an x in A such that $\mathcal{P}(x)$ is a true statement". The symbol $\exists$ which reads "there exists" or "for some" or "for at least one" is called the *existential quantifier*. The proposition $\exists x \in A : \mathcal{P}(x)$ expresses that the truth set of $\mathcal{P}(x)$ is not the emptyset, or symbolically, $T_{\mathcal{P}} = \{x \mid x \in A, \mathcal{P}(x)\} \neq \varnothing$.

Example 1.6 Some propositions using the existential quantifier:

- The proposition $\exists n \in \mathbb{N} : n + 4 < 7$ is true since $\{n : n \in \mathbb{N}, n + 4 < 7\} = \{0, 1, 2\} \neq \varnothing$.
- The proposition $\forall n \in \mathbb{N} : n + 6 < 4$ is false since $\{n : n \in \mathbb{N}, n + 6 < 4\} = \varnothing$.
- The symbol $\exists$ can be used to define the intersection of an indexed collection $\{A_i : i \in I\}$ of sets A_i as follows: $\bigcap_{i \in I} A_i = \{x : \exists i \in I, x \in A_i\}$.

Consider the proposition: "All officers are engineers". Its negation is either of the following equivalent statements:

- "It is not the case that all officers are engineers".
- "There exists at least one officer who is not an engineer".

Symbolically, using M to denote the set of officers, the above can be written as

$$\neg(\forall x \in M : x \text{ is an engineer }) \equiv \exists x \in M : x \text{ is not an engineer},$$

or, when $\mathcal{P}(x)$ denotes " x is an engineer",

$$\neg(\forall x \in M : \mathcal{P}(x)) \equiv \exists x \in M : \neg\mathcal{P}(x).$$

The above is true for any proposition $\mathcal{P}(x)$.

Theorem 1.5. $\neg(\forall x \in A : \mathcal{P}(x)) \equiv \exists x \in A : \neg\mathcal{P}(x)$.

In other words, the following two statements are equivalent:

- It is not true that, for all $a \in A$, $\mathcal{P}(a)$ is true.
- There exists an $a \in A$ such that $\mathcal{P}(a)$ is false.

There is an analogous theorem for the negation of a proposition which contains the existential quantifier.

Theorem 1.6. $\neg(\exists x \in A : \mathcal{P}(x)) \equiv \forall x \in A : \neg\mathcal{P}(x)$.

That is, the following two statements are equivalent:

- It is not true that, for some $a \in A$, $\mathcal{P}(a)$ is true.
- For all $a \in A$, $\mathcal{P}(a)$ is false.

Previously, $\neg$ was used as an operation on propositions, here $\neg$ is used as an operation on propositional functions. The operations $\vee$ and $\wedge$ can also be applied to propositional functions. In terms of truth sets:

1. $\neg\mathcal{P}(x)$ is the complement of $T_{\mathcal{P}}$, that is $T_{\mathcal{P}}^c$.
2. $\mathcal{P}(x) \vee \mathcal{Q}(x)$ is the union of $T_{\mathcal{P}}$ and $T_{\mathcal{Q}}$, that is $T_{\mathcal{P}} \cup T_{\mathcal{Q}}$.
3. $\mathcal{P}(x) \wedge \mathcal{Q}(x)$ is the intersection of $T_{\mathcal{P}}$ and $T_{\mathcal{Q}}$, that is $T_{\mathcal{P}} \cap T_{\mathcal{Q}}$.

A propositional function of 2 variables defined over a product set $A = A_1 \times A_2$ is a function $A_1 \times A_2 \to \{T, F\} : \mathcal{P}(x_1, x_2)$ which has the property that $\mathcal{P}(a_1, a_2)$ is true or false for any pair (a_1, a_2) in A.

A propositional function can be generalized over a product set of more than 2 sets.

A propositional function preceded by a quantifier for each variable denotes a proposition and has a truth value.

Example 1.7 Let $B = \{1, 2, 3, \ldots, 9\}$ and let $\mathcal{P}(x, y)$ denotes " $x + y = 10$ ". Then $\mathcal{P}(x, y)$ is a propositional function on $A = B \times B$.

1. The following is a proposition since there is a quantifier for each variable: $\forall x \in B, \exists y \in B : \mathcal{P}(x, y)$ that is, "For every x in B, there exists a y in B such that $x + y = 10$ ". This statement is true.
2. The following is also a proposition: $\exists y \in B, \forall x \in B : \mathcal{P}(x, y)$ that is, "There exists a y in B such that, for every x in B, we have $x + y = 10$ ". No such y exists; hence the statement is false.

Observe that the only difference between both examples is the order of the quantifiers. Thus a different ordering of the quantifiers may yield a different statement!

Theorem 1.7. *For any propositional function* $\mathcal{P}(x, y)$ *:*

1. $\forall x \in A, \forall y \in B : \mathcal{P}(x, y) \Leftrightarrow \forall y \in B, \forall x \in A : \mathcal{P}(x, y)$.
2. $\exists x \in A, \exists y \in B : \mathcal{P}(x, y) \Leftrightarrow \exists y \in B, \exists x \in A : \mathcal{P}(x, y)$.
3. $\exists x \in A, \forall y \in B : \mathcal{P}(x, y) \Rightarrow \forall y \in B, \exists x \in A : \mathcal{P}(x, y)$.
4. $\forall x \in A, \exists y \in B : \mathcal{P}(x, y) \not\Rightarrow \exists y \in B, \forall x \in A : \mathcal{P}(x, y)$.

Quantified statements with more than one variable may be negated by successively applying the theorems of DeMorgan. Thus each $\forall$ is changed to $\exists$, and each $\exists$ is changed to $\forall$ as the negation symbol $\neg$ passes through the statement from left to right.

Example 1.8 Some examples of the negation of quantified statement with more than one variable:

- $\neg(\forall x \in A, \exists y \in B, \exists z \in C : \mathcal{P}(x, y, z)) \equiv \exists x \in A, \neg(\exists y \in B, \exists z \in C : \mathcal{P}(x, y, z)) \equiv \exists x \in A, \forall y \in B, \neg(\exists z \in C : \mathcal{P}(x, y, z)) \equiv \exists x \in A, \forall y \in B, \forall z \in C : \neg\mathcal{P}(x)$.
- Consider the proposition: "Every student has at least one course where the lecturer is an officer". Its negation is the statement: "There is a student such that in every course the lecturer is not an officer".

1.3 Proofs

Many proofs can be written by following a simple *template* that suggests guidelines to follow when writing the proof.

Direct Proof

To proof $\mathcal{P} \Rightarrow \mathcal{Q}$, we can proceed by looking at the truth table. The table shows that if $\mathcal{P}$ is false, the statement $\mathcal{P} \Rightarrow \mathcal{Q}$ is automatically true. This means that if we are concerned with showing $\mathcal{P} \Rightarrow \mathcal{Q}$ is true, we don't have to worry about the situations where $\mathcal{P}$ is false because the statement $\mathcal{P} \Rightarrow \mathcal{Q}$ will be automatically true in those cases. But we must be very careful about the situations where $\mathcal{P}$ is true. We must show that the condition of $\mathcal{P}$ being true forces $\mathcal{Q}$ to be true also.

SET THE CONTEXT
ASSERT THE HYPOTHESIS
LIST IMPLICATIONS
STATE THE CONCLUSION

Example 1.9 Proof the proposition "The sum of any two odd natural numbers is even".

Proof. *SET THE CONTEXT*: Let m and n be two natural numbers.
ASSERT THE HYPOTHESIS: Suppose m and n are odd.
LIST IMPLICATIONS:

1. From the definition of odd natural numbers, there is a natural number k_1 such that $m = 2k_1 + 1$ and a natural number k_2 such that $n = 2k_2 + 1$.
2. Then $m + n = (2k_1 + 1) + (2k_2 + 1) = 2(k_1 + k_2 + 1)$.
3. Since k_1 and k_2 are natural numbers, so is $k_1 + k_2 + 1$.
4. Thus, the sum $m + n$ is equal to twice a natural number, so by the definition of even natural numbers, $m + n$ is even.

STATE THE CONCLUSION: Therefore, the sum of any two odd natural number is always even. □

In proving a statement is true, we sometimes have to examine multiple cases before showing the statement is true in all possible scenarios.

SET THE CONTEXT
CASE 1: ASSERT THE HYPOTHESIS
CASE 1: LIST IMPLICATIONS
CASE 1: STATE THE CONCLUSION
CASE 2: ASSERT THE HYPOTHESIS
CASE 2: LIST IMPLICATIONS
CASE 2: STATE THE CONCLUSION
...
STATE THE CONCLUSION

Example 1.10 Proof the proposition "If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4".

Proof. Let n be a natural number.
CASE 1: Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{N}$, and $(-1)^n = 1$. Thus $1 + (-1)^n(2n - 1) = 1 + (1)(2 \cdot 2k - 1) = 4k$, which is a multiple of 4.
CASE 2: Suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{N}$, and $(-1)^n = -1$. Thus $1 + (-1)^n(2n - 1) = 1 - (2(2k + 1) - 1) = -4k$, which is a multiple of 4.
These cases show that $1 + (-1)^n(2n - 1)$ is always a multiple of 4. □

Proof by Contraposition

Sometimes a direct proof of $\mathcal{P} \Rightarrow \mathcal{Q}$ is very hard. The proposition $\neg\mathcal{Q} \Rightarrow \neg\mathcal{P}$ is logically equivalent to $\mathcal{P} \Rightarrow \mathcal{Q}$. This is called the *contraposition* of the initial proposition.

Exercise 1.3 Show $\neg\mathcal{Q} \Rightarrow \neg\mathcal{P} \equiv \mathcal{P} \Rightarrow \mathcal{Q}$ using a truth table.

SET THE CONTEXT
ASSERT THE HYPOTHESIS: $\neg\mathcal{Q}$ is true
LIST IMPLICATIONS
STATE THE CONCLUSION: $\neg\mathcal{P}$ is true

Example 1.11 Proof by contraposition the proposition "Let $x \in \mathbb{N}$. If $x^2 + 6x + 5$ is even, then x is odd".

A direct proof would be problematic. We will proof the logically equivalent proposition "If x is not odd, then $x^2 + 6x + 5$ is not even".

Proof. Let $x \in \mathbb{N}$.

Suppose x is not odd.

Then x is even and $x = 2k$ for some $k \in \mathbb{N}$. Thus $x^2 + 6x + 5 = (2k)^2 + 6 \cdot (2k) + 5 = 2(2k^2 + 6k + 2) + 1$. Since k is a natural number, $2k^2 + 6k + 2$ is also a natural number. Consequently, $x^2 + 6x + 5$ is odd.

Therefore, $x^2 + 6x + 5$ is not even. □

Proof by Contradiction

A proof by *contradiction* is not limited to proving just conditional statements—it can be used to prove any kind of statement whatsoever. The basic idea is to assume that the statement we want to prove is false, and then show that this assumption leads to nonsense. We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true.

Exercise 1.4 Show $\mathcal{P} \equiv \neg\mathcal{P} \Rightarrow \mathcal{C} \wedge \neg\mathcal{C}$ using a truth table.

SET THE CONTEXT
ASSERT THE HYPOTHESIS: $\mathcal{P}$ is false.
LIST IMPLICATIONS
STATE THE CONCLUSION: $\mathcal{C} \wedge \neg\mathcal{C}$.

A slightly unsettling feature of this method is that we may not know at the beginning of the proof what the statement $\mathcal{C}$ is going to be.

Example 1.12 Proof by contradiction the proposition "If $a, b \in \mathbb{N}$, then $a^2 - 4b \neq 2$".

Proof. Let $a, b \in \mathbb{N}$.

Suppose there exist a and b for which $a^2 - 4b = 2$. From this equation we get $a^2 = 4b + 2 = 2(2b + 1)$, so a^2 is even.

Because a^2 is even, it follows that a is even, so $a = 2c$ for some natural number c. Now plug $a = 2c$ back into the boxed equation to get $(2c)^2 - 4b = 2$, so $4c^2 - 4b = 2$. Dividing by 2, we get $2c^2 - 2b = 1$.

Therefore, $1 = 2(c^2 - b)$, and because $c^2 - b \in \mathbb{N}$, it follows that 1 is even.

We know 1 is **not** even, so something went wrong. But all the logic after the first line of the proof is correct, so it must be that the first line was incorrect. In other words, we were wrong to assume the proposition was false. Thus the proposition is true. □

The previous two proof methods dealt exclusively with proving conditional statements, we now formalize the procedure in which contradiction is used to prove a conditional statement. Thus we need to prove that $\mathcal{P} \Rightarrow \mathcal{Q}$ is true. Proof by contradiction begins with the assumption that $\neg(\mathcal{P} \Rightarrow Q)$ is true, that is, that $\mathcal{P} \Rightarrow \mathcal{Q}$ is false. But we know that $\mathcal{P} \Rightarrow \mathcal{Q}$ being false means that it is possible that $\mathcal{P}$ can be true while $\mathcal{Q}$ is false. Thus the first step in the proof is to assume $\mathcal{P}$ and $\neg\mathcal{Q}$.

SET THE CONTEXT
ASSERT THE HYPOTHESIS: $\mathcal{P}$ and $\neg\mathcal{Q}$ are true.
LIST IMPLICATIONS
STATE THE CONCLUSION: $\mathcal{C} \wedge \neg\mathcal{C}$.

Example 1.13 Proof by contradiction the proposition "Let $a \in \mathbb{N}$. If a^2 is even, then a is even".

Proof. Let $a \in \mathbb{N}$.

Suppose a^2 is even and a is not even.

Since a is odd, there exists a natural number c for which $a = 2c + 1$. Then $a^2 = (2c + 1)^2 = 4c2 + 4c + 1 = 2(2c^2 + 2c) + 1$, so a^2 is odd.

Thus a^2 is even and a^2 is not even, a contradiction. □

If-and-only-if Proof

Some propositions have the form $\mathcal{P} \Leftrightarrow \mathcal{Q}$. We know that this is logically equivalent to $(\mathcal{P} \Rightarrow \mathcal{Q}) \wedge (\mathcal{Q} \Rightarrow \mathcal{P})$. So to prove "$\mathcal{P}$ if and only if $\mathcal{Q}$" we must prove **two** conditional statements. Recall that $\mathcal{Q} \Rightarrow \mathcal{P}$ is called the *converse* of $\mathcal{P} \Rightarrow \mathcal{Q}$. Thus we need to prove both $\mathcal{P} \Rightarrow \mathcal{Q}$ and its converse. These are both conditional statements, so we may prove them with either direct, contrapositive or contradiction proof.

Example 1.14 Proof the proposition "The natural number n is odd if and only if n^2 is odd".

Proof. Let $n \in \mathbb{N}$.

First we show that n being odd implies that n^2 is odd.

Suppose n is odd.

Then, by definition of an odd number, $n = 2a + 1$ for some natural number. Thus $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. This expresses n^2 as twice a natural number, plus 1.

Therefore, n^2 is odd.

Conversely, we need to prove that n^2 being odd implies that n is odd. We use contraposition and proof the proposition "n not odd implies that n^2 is not odd".

Suppose n is not odd.

Then n is even, so $n = 2a$ for some natural number a by definition of an even number. Thus $n^2 = (2a)^2 = 2(2a^2)$, so n^2 is even because it's twice a natural number.

Therefore, n^2 is not odd. □

Existence Proof

Up until this point, we have dealt with proving conditional statements or with statements that can be expressed with two or more conditional statements. Generally, these conditional statements have form $\mathcal{P}(x) \Rightarrow \mathcal{Q}(x)$. (Possibly with more than one variable.) We saw that this can be interpreted as a universally quantified statement $\forall x : \mathcal{P}(x) \Rightarrow \mathcal{Q}(x)$.

But how would we prove an *existentially* quantified statement? What technique would we employ to prove a theorem of the form $\exists x : \mathcal{P}(x)$. This statement asserts that there exists some specific object x for which $\mathcal{P}(x)$ is true. To prove $\exists x : \mathcal{P}(x)$ is true, all we would have to do is find and display an *example* of a specific x that makes $\mathcal{P}(x)$ true.

Example 1.15 There exists anatural number that can be expressed as the sum of two perfect cubes in two different ways.

Proof. Consider the number 1729.
Note that $1^3 + 12^3 = 1729$ and $9^3 + 10^3 = 1729$.
Therefore, the number 1729 can be expressed as the sum of two perfect cubes in two different ways. □

Counterexamples

How to disprove a universally quantified statement such as $\forall x : \mathcal{P}(x)$? To disprove this statement, we must prove its negation. Its negation is $\neg\forall x : \mathcal{P}(x) \Rightarrow \mathcal{Q}(x) \equiv \exists x : \neg(\mathcal{P}(x) \Rightarrow \mathcal{Q}(x))$. The negation is an existence statement. To prove the negation is true, we just need to produce an example of an x that makes $\mathcal{P}(x)$ false.

Example 1.16 Disproof the proposition "For every $n \in \mathbb{N}$, the natural number $f(n) = n^2 - n + 11$ is prime".

Proof. The statement "For every $n \in \mathbb{N}$, the natural number $f(n) = n^2 - n + 11$ is prime," is false. For a counterexample, note that for $n = 11$, the natural number $f(11) = 121 = 11 \cdot 11$ is not prime. □

Proof by Induction

Suppose the variable n represents any natural number, and there is a propositional function $\mathcal{P}(n)$ that includes this variable as an argument. *Mathematical induction* is a proof technique that uses the axiom of induction to show that $\mathcal{P}(n)$ is true for all n greater than or equal to some base value $b \in \mathbb{N}$.

SET THE CONTEXT: The statement will be proved by mathematical induction on n for all $n \geq b$.
PROVE $\mathcal{P}(b)$: Prove that the statement is true when the variable n is equal to the base value, b.
STATE THE INDUCTION HYPOTHESIS: Assume that $\mathcal{P}(n)$ is true for some natural number $n = k \geq b$.
PERFORM THE INDUCTION STEP: Using the fact that $\mathcal{P}(k)$ is true, prove that $\mathcal{P}(k + 1)$ is true.
STATE THE CONCLUSION: Therefore, by mathematical induction, $\mathcal{P}(n)$ is true for all natural numbers $n \geq b$.

Example 1.17 Proof by induction the proposition "If $n \in \mathbb{N} \setminus \{0\}$, then $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$ ".

Proof. Let $n \in \mathbb{N} \setminus \{0\}$.
Observe that if $n = 1$, this statement is $1 = 1^2$, which is obviously true.
Suppose that $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ for some natural number $k \geq 1$.
Then, $1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = k^2 + 2k + 1 = (k + 1)^2$.
Therefore, by mathematical induction, $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$ for all natural numbers $n \geq 1$. □