Academic year 2025-2026

Mathematical Logic

(Course and exercises with solutions)

Written by

LEMITA Samir

People’s Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research

Echahid Cheikh Larbi Tebessi University
Faculty of Exact, Natural and Life Sciences
Department of Mathematics

جامعة العربي التبسي - تبسة
Université Larbi Tébessi - Tébessa

Mathematical Logic
Course and exercises with solutions

Written by

LEMITA Samir

Intended to

Second-year BSc in Mathematics

Academic year 2025-2026

وزارة التعليم العالي والبحث العلمي
جـامعـة الشهيد الشيخ العربي التبسي -تبسة
كلية العلوم الدقيقة و علوم الطبيعة و الحياة

رقم: 2025/07/02 مكرر

تبسة في : 26/01/2026

مستخرج من محضر اجتماع المجلس العلمي المنعقد بتاريخ 03نوفمبر 2025

في اليوم الثالث من شهر نوفمبر لسنة 2025 و على الساعة العاشرة صباحا اجتمع المجلس العلمي لكلية العلوم الدقيقة و علوم الطبيعة و الحياة في دورة عادية برئاسة الاستاذ الدكتور بن خذير محمد لطفي حيث:

تمت دراسة و قبول طلب عرض مطبوعة دروس للخبرة

المؤلف : لميطة سمير

العنوان: Mathematical Logic Course and exercises with solutions

اللغة: انجليزية

موجهة لطلبة سنة ثانية ليسانس رياضيات

و تم قبول اقتراح الخبيرين:

الاسم واللقب	البريد الالكتروني	الجامعة
نابتي عبد الرزاق	abderrazak.nabti@univ-tebessa.dz	جامعة الشهيد الشيخ العربي التبسي – تبسة-
خلاف عمار	amarlasix@gmail.com	المدرسة الوطنية متعددة التقنيات قسنطينة

و بعد أن عاين السيد رئيس المجلس أن التقريرين إيجابيين تم اعتماد المطبوعة.

محمد لطفي بن خذير
رئيس المجلس العلمي للكلية


الحمد لله الذي بنعمته تتم الصالحات

Contents

Introduction

In early history, we can see that theory of logic is developed in many cultures such as: China, India, Greece, Roman and the Islamic world. Particularly, the term logic has been used firstly by ***Aristotle*** as found in the Organon. Moreover, Greek scientists are the ones who built the foundation art of reasoning and mathematical, which have known wide application in science disciplines for millennia.

Since the end of the 16^{th} century, there were a valuable contributions for philosophical logic and mathematical developments. We list the most of them as follows: ***Gottfried Leibniz, Jean-Henri Lambert*** introduced much of modern mathematical notation, such as logical quantifiers and the integration symbol. ***George Boole, Auguste De Morgan*** who introduced the truth calculus, logical combinations such as conjunction, disjunction and implication, symbolic logic and Boolean algebra. ***Gottlob Frege*** laid the groundwork of propositional and predicate logic. ***Georg Cantor*** created a large part in the creation of set theory, who defined infinite and well-ordered sets, and proved a fundamental concepts in real numbers. ***Giuseppe Peano, Gerhard Gentzen*** introduced axiomatization of arithmetic and defined the arithmetical properties. ***David Hilbert*** proposed a list of 23 important problems which inspired much work in mathematics and logic such as: the development of axiom systems for arithmetic, and used the reasoning language in proofs. ***Bertrand Russell*** made great contributions to fundamental theory in mathematics such as: contemporary formal logic, theory of types, popularizing of the first-order predicate calculus, discovery of Russell's paradox. ***Ernst Zermelo, Thoralf Skolem, Abraham Fraenkel*** made very significant contribution on axiomatic set theory. ***Kurt Gödel*** made important contributions in completeness of first-order logic and compactness, compatibility of the choice's axioms and the continuum hypothesis, incompleteness theorems of arithmetic. ***Stephen Kleene, Emil Post*** defined the concept of computability theory and complexity theory of algorithms.

Furthermore, mathematical logic also developed significantly due to its close association with informatics. In 1936, ***Alan Turing*** described an abstract machine to support the notions of algorithm and computation, which is recognized as an abstract model of the computer. In 1951, ***John von Neumann*** described a computer model, this model is characterized by a central processing unit which executes the instructions sequentially, and a single memory for data. ***Alonzo Church*** introduced what is called the lambda calculus, this made major contributions to the foundations of theoretical computer science. ***Haskell Curry, William Howard*** discovered what they called the Curry–Howard correspondence which represents the direct relationship between computer programs and mathematical proofs. ***Joachim Lambek*** developed a formal system, known as Lambek calculus, which has highly influence in computational linguistics and formal language theory. However, there are many others researchers had contributions in this field, each according to their point of view and needs.

Consequently, logic is the first formalization of mathematical language and reasoning. It has been developed from the end of the 19^{th} century, little by little, by a cohort of brilliant mathematicians and philosophers. Currently, in conjunction with the tremendous development in computer science, mathematical logic continues to be an active area of research, and made significant contributions in various fields such as: algorithm design, programming language theory, databases, knowledge bases, pre-post conditions of a procedure, artificial intelligence, logic gates, digital circuits, derive predictions, philosophy, linguistics, legal reasoning, etc.

The aim of this course is to study in detail the foundations of mathematical logic. To give students sufficient training, the course is divided into 5 chapters as follows: In chapter 1, we begin by explaining the different concepts of mathematical language. In chapter 2, we study the different types of mathematical proofs, and provide illustrative examples of each one. In chapter 3, we present a comprehensive study of set theory, which is a fundamental focus for every mathematician. Chapter 4 and 5, is dedicated to propositional calculus and predicate calculus, respectively. Which are represent a fundamental systems in mathematical logic.

1

Elements of mathematical language

In mathematics, terms: theorem, definition, axiom, lemma, corollary, proposition, and statement refer to different concepts, each one with its role in the structure of mathematical reasoning. In this chapter, we will going to discuss the breakdown of essential of these terms.

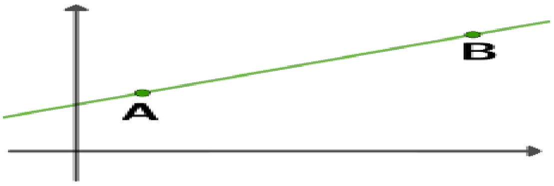
1.1 Axiom

Definition 1.1

Is a fundamental principles assumed to be true without proof. They serve as the starting point for further reasoning and arguments.

Example 1.1

In Euclidean geometry, one axiom is that through any two points, there is exactly one straight line.



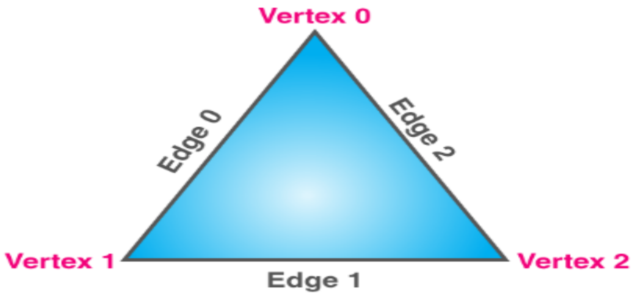
1.2 Definition

Definition 1.2

Represents a precise explanations of the meaning of a term or concept. Definitions establish the language and framework for discussion within a mathematical context.

Example 1.2

A triangle is defined as a polygon with three edges and three vertices.



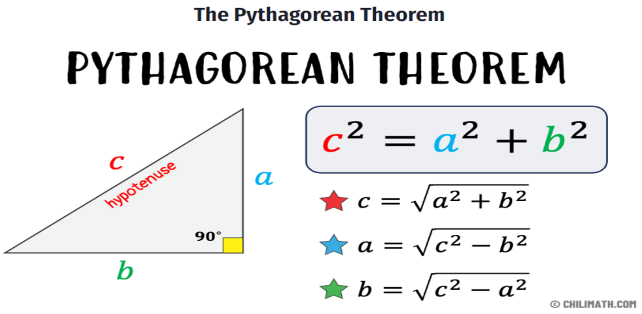
1.3 Theorem

Definition 1.3

Is statements that have been proven to be true based on axioms, definitions, and previously established theorems. Theorems often require substantial proof and are central to mathematical discourse.

Example 1.3

In any right triangle, Pythagorean theorem says that: Square of the hypotenuse's length equals to sum of squares of other two sides' lengths.



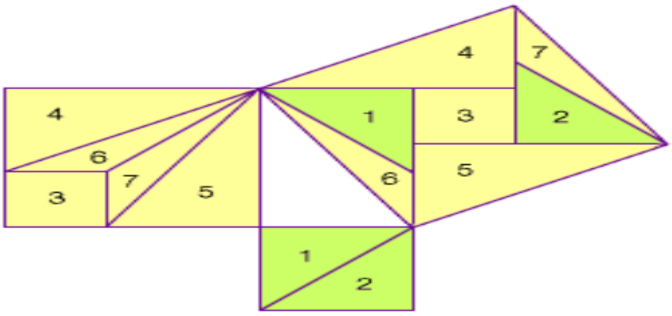
1.4 Lemma

Definition 1.4

Preliminary propositions or statements that are proven and used as stepping stones to prove larger theorems. Lemmas are often considered useful but not necessarily significant on their own.

Example 1.4

In proving the Pythagorean theorem, one might first prove a lemma about the properties of similar triangles.



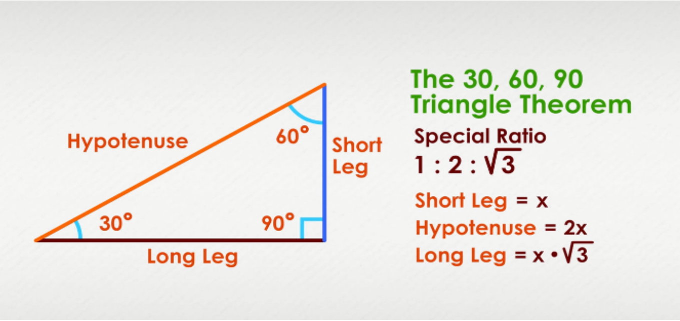
1.5 Corollary

Definition 1.5

Statements that follow readily from a previously proven theorem. Corollaries are often seen as direct consequences of theorems.

Example 1.5

A corollary of the Pythagorean theorem is that in a $30^\circ - 60^\circ - 90^\circ$ *triangle, then lengths of the sides are* 1, $\sqrt{3}$, 2, *respectively.*



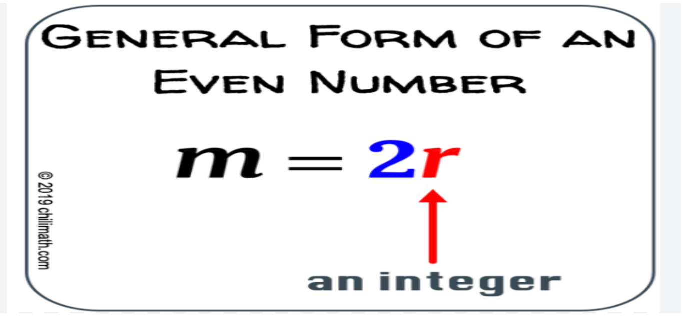
1.6 Proposition

Definition 1.6

Is statements that are asserted to be true or false, which can be proven or disproven. Propositions are often less significant than theorems but still important in the structure of proofs.

Example 1.6

A proposition might state that the sum of any two even integers is even.



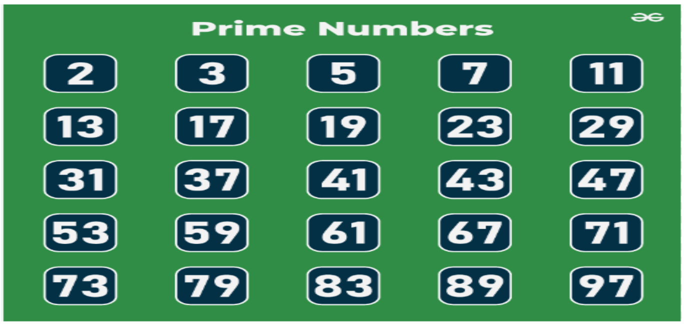
1.7 Statement

Definition 1.7

Is general assertions that may be true or false. In mathematics, statements can refer to any declarative sentence that has a truth value.

Example 1.7

All primes are odd: *is a statement that can be evaluated as true or false.*


Prime Numbers

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Remark 1.1

We can summarize the previous concepts in the following simplification:

1. *Axioms: are foundational truths.*
2. *Definitions: clarify terms and concepts.*
3. *Theorems: are significant proven statements.*
4. *Lemmas: are helpful intermediary results.*
5. *Corollaries: are direct consequences of theorems.*
6. *Propositions: are assertions that can be proven or disproven.*

7. *Statements: are general declarations that possess a truth value.*

Remark 1.2

We can see that there are other different types of statements can be used to convey information about mathematical concepts, such as: note, example, remark, indication, application, problem,... and others.

1.8 Paradoxes

Definition 1.8

Paradoxes in mathematics arise from statements which at first appear logical and consistent, but after careful examination reveal a contradiction or impossibility. These paradoxes play a key role in the development of mathematics, they exigent the mathematicians to enhance their definitions and clarify their reasoning. Among the famous mathematical paradoxes, we are satisfied with presenting just a discerption of: Russell's paradox, Liar paradox and Cantor's paradox.

1.8.1 Russell's paradox

Definition 1.9

Paradox of Russell is also known by Russell's antinomy. It was discovered by ***Bertrand Russell*** in 1903. Which represents a very simple paradox of set theory. The paradox can be written if we ask:

does the set of sets not belonging to themselves belong to itself?

Or can be formulated as follows:

$$W = \{\omega \,|\, \omega \notin \omega\}.$$

Thus,

$$W \in W \Leftrightarrow W \notin W.$$

So, possibilities: $W \in W$ and $W \notin W$ lead to a contradiction.
This paradox has an influence in the development of axiomatic set theory and other formal systems.

1.8.2 Liar's paradox

Definition 1.10

The liar paradoxes are self-referential logical paradox deriving from statement, sentence, proposition or any truth bearer that says that it is false. In 1956 ***Alfred Tarski*** is the ones who started work on the liar paradox. To understand the liar paradox, we consider the statement:

$$T: \textit{\textbf{This judgment is false.}}$$

We have two cases:
Case 1: If statement T is true, then what he says is true which means it must be false.
Case 2: If statement T is false, then what he says is false which means it must be true.
So, the statement T seems to be both true and false simultaneously. This creates a contradiction which represents the core of the liar paradox.
This paradox has a significant implications for mathematics, philosophy and the foundations of meaning and truth.

1.8.3 Cantor's paradox

Before describing the paradox, we point out to the **Cantor's Theorem**.

Theorem 1.1: (Cantor's Theorem)

The theorem proves that for any set S, the cardinality of power set $P(S)$ is greater than the cardinality of the set S. The proof of this theorem is clear for a finite sets. Because when S contains m elements, then the set $P(S)$ contains 2^m subsets. Thus, cardinality of $P(S)$ is greater than of S. But, in case for infinite sets the proof becomes noteworthy, this is what was proven by Cantor.

Definition 1.11: (Cantor's paradox)

Paradox of Cantor was discovered by ***Georg Cantor*** in 1890. This paradox states that:

If a set of all cardinalities existed, it would include the cardinality of every other set including its power set.

In other word, if we assume that: ***set of all sets*** exists and denoted by S, then its power set $P(S)$ also exists and be a subset of S. However, the Cantor's theorem described above gives us that cardinality of $P(S)$ must be larger than cardinality of S. This creates the paradox, because S is assumed as ***set of all sets***, which means that contains all sets including its power set $P(S)$.
This paradox led to new reasoning about set theory. In axiomatic set theory, there are some collections are too vast to be considered as sets. These collection are known by proper classes.

1.9 Exercises

Exercise 1.1

Consider the following statements:

1. Whole is greater than part.
2. Green's Theorem.
3. Dimension of a vector space V is the number of vectors in any basis B of this space
4. Pythagorean theorem.
5. $(3+4)^2 = 3^2 + 4^2$.
6. Find and prove all primes p that divide $N = 2^{100}3^{23}$.
7. Measure of the inscribed angle is half measure of the central angle.
8. If equals be added to equals, the wholes are equal.
9. Sets in mathematics, are simply a collection of distinct objects.
10. There's no right triangle whose sides measure 3cm, 4cm, and 6cm.
11. We have $x+2 = 2x$ when $x = -2$.
12. The angle in the Semicircle Theorem.
13. If α is a prime divides the integer $\beta\gamma$, then α divides β or α divides γ.
14. Fatou's Lemma in theory of measure and integration.

Give and explain the type of each of statements.

Exercise 1.2

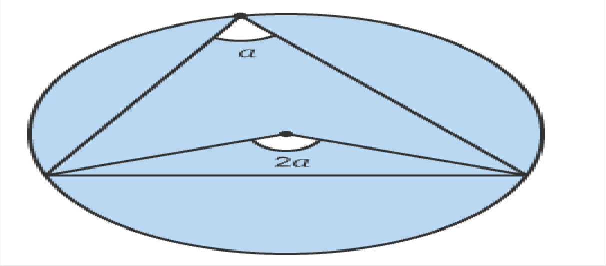
Theorem: For any linear transformation f between two vector spaces E and F, we have:

$$f(O_E) = O_F.$$

Based on definition of the linear transformation, prove the previous theorem and conclude the form of linear functions in Euclidean space $\mathbb{R}$.

Exercise 1.3

Theorem: Measure of the inscribed angle ($\alpha°$) is the half measure of the central angle ($2\alpha°$).



Prove this theorem, then conclude that the hypotenuse of a right triangle inscribed in a circle is the diameter of this circle.

Exercise 1.4

The Hölder's inequality is given by: Let $n \in \mathbb{N}$, x_k, $y_k \in \mathbb{R}$, and for $p, q \geq 1$, with $\frac{1}{p} + \frac{1}{q} = 1$, then:

$$\sum_{k=1}^{n} |x_k y_k| \leq \left(\sum_{k=1}^{n} |x_k|^p \right)^{\frac{1}{p}} \left(\sum_{k=1}^{n} |y_k|^q \right)^{\frac{1}{q}}.$$

This inequality interprets the general form of Cauchy Schwarz inequality. To prove the Hölder's inequality, we apply the definition of the concave function on: $f(t) = ln(t)$, $t > 0$ to get the following Young's inequality:

$$|v w| \leq \frac{|v|^p}{p} + \frac{|w|^q}{q},$$

then we use the new variable

$$v = x_k \left(\sum_{l=1}^{n} |x_l|^p \right)^{\frac{-1}{p}}, \quad w = y_k \left(\sum_{l=1}^{n} |y_l|^q \right)^{\frac{-1}{q}}$$

to get the required result.
Give a detailed explanation of the proof of this inequality, by using an appropriate steps which include the necessary definition, lemma, theorem and corollary.

1.10 Solutions

Solution of exercise 1.1:

The types of the given statements:

Expression $n^o 1$: Axiom.
Expression $n^o 2$: Theorem.
Expression $n^o 3$: Definition.
Expression $n^o 4$: Theorem.
Expression $n^o 5$: Statement.
Expression $n^o 6$: Corollary.
Expression $n^o 7$: Theorem.
Expression $n^o 8$: Axiom.
Expression $n^o 9$: Definition.
Expression $n^o 10$: Corollary.
Expression $n^o 11$: Statement.
Expression $n^o 12$: Theorem.
Expression $n^o 13$: Theorem.
Expression $n^o 14$: Lemma.

Solution of exercise 1.2:

In this part, we have **Definition**, **Theorem** and **Corollary**. We provide them one by one:

Definition: (Linear Transformation)

A linear transformation f (or linear map) is a function defined between two vector spaces E and F, that fulfills the following conditions:

1. $f(x_1+x_2)=f(x_1)+f(x_2)$, $\forall x_1, x_2 \in E$,
2. $f(\alpha x)=\alpha f(x)$, $\forall x \in E, \forall \alpha \in \mathbb{K}$.

Theorem:

For any linear transformation f between two vector spaces E and F, we have:

$$f(O_E)=O_F.$$

Proof: We can see easily that:

$$\begin{aligned}
f(O_E) &= f(x-x), \quad x \in E, \\
&= f(x+(-x)), \\
&= f(x)+f(-x), \quad (\textit{first condition}), \\
&= f(x)+(-1)f(x), \quad (\textit{second condition, with } \lambda=-1), \\
&= f(x)-f(x), \\
&= O_F, \quad f(x) \in F.
\end{aligned}$$

Corollary:

Based on the previous theorem, all linear functions in Euclidean space $\mathbb{R}$, must satisfy $f(0)=0$. Thus the form of these functions can be taken as:

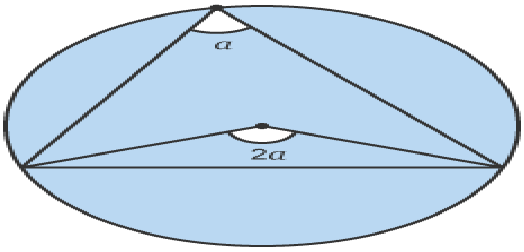
$$f(x)=\alpha x, \quad where \quad \alpha \in \mathbb{R}.$$

Solution of exercise 1.3:

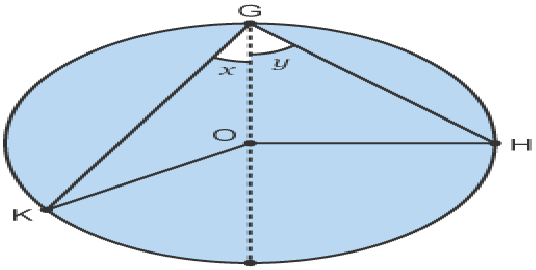
In this exercise, we have the following **Theorem** and **Corollary**:

Theorem: (Inscribed angle theorem)

Measure of the inscribed angle ($\alpha°$) equals to half measure of the central angle ($2\alpha°$).



Proof: In the shown figure, let $x,\ y$ be measures of angles $\widehat{OGK}$ and $\widehat{OGH}$, respectively.



As $OK = OG$, then the triangle GOK is an isosceles, it follows that:

$$\widehat{OGK} = \widehat{OKG} = x.$$

In the same way, we find:

$$\widehat{OGH} = \widehat{OHG} = y.$$

Furthermore, sum of measures of any triangle's angles equals to 180°, thus:

$$\begin{aligned} & \widehat{OGK} + \widehat{OKG} + \widehat{KOG} = 180°, \\ \Rightarrow\quad & x + x + \widehat{KOG} = 180°, \\ \Rightarrow\quad & \widehat{KOG} = 180° - 2x. \end{aligned}$$

Also,

$$\begin{aligned} & \widehat{OGH} + \widehat{OHG} + \widehat{HOG} = 180°, \\ \Rightarrow\quad & y + y + \widehat{HOG} = 180°, \\ \Rightarrow\quad & \widehat{HOG} = 180° - 2y. \end{aligned}$$

Finally, we have:

$$\widehat{KGH} = \widehat{OGK} + \widehat{OGH} = x + y,$$

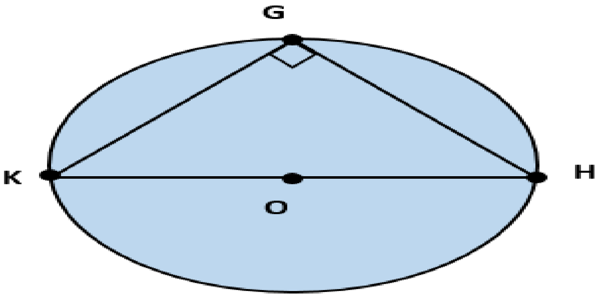
and

$$\begin{aligned} \widehat{KOH} &= 360^\circ - (\widehat{KOG} + \widehat{HOG}), \\ &= 360^\circ - (180^\circ - 2x + 180^\circ - 2y), \\ &= 360^\circ - 180^\circ + 2x - 180^\circ + 2y, \\ &= 2x + 2y, \\ &= 2(x + y), \\ &= 2\widehat{KGH}. \end{aligned}$$

Consequently, measure of inscribed angle $\widehat{KGH}$ is half measure of central angle $\widehat{KOH}$.

Corollary:

We take the measure of inscribed angle $\widehat{KGH} = a^\circ = 90^\circ$, to obtain a right triangle KHG inscribed in the circle. Moreover, based on the previous theorem, we have the measure of central angle $\widehat{KOH} = 2a^\circ = 180^\circ$, which means that hypotenuse of triangle KHG will be the diameter of this circle.



Solution of exercise 1.4:

In this part, we have **Definition**, **Lemma**, **Theorem** and **Corollary**. We explain them one by one in detail:

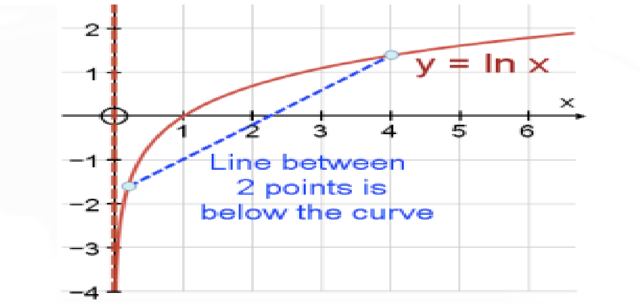
Definition: (Concave function)

We say that function g is concave on interval $[a, b]$, when verifies:

$$\forall x,\ y \in [a, b],\ \forall \theta \in [0, 1],\ g(\theta x + (1-\theta)y) \geq \theta g(x) + (1-\theta)g(y).$$

Graphically, we say that g is concave, when we draw a line segment $[x, y]$ between any two points x and y on the curve of g, then line segment $[x, y]$ will be always lie below the graph of this function.

Example: We can see that the natural logarithm function $g(x)=\ln(x)$, is considered as common example of concave functions. It is concave on interval $x \in]0,+\infty]$ as shown in its curve below.



Lemma: (Young's inequality)

Let $v,\ w \in \mathbb{R}$ and for every $p,q \geq 1$ with $\frac{1}{p}+\frac{1}{q}=1$, then:

$$|v\,w| \leq \frac{|v|^p}{p}+\frac{|w|^q}{q}.$$

Proof: The claim is certainly true when $v=w=0$, so assume that $v \neq 0$ and $w \neq 0$. Because the natural logarithm function $g(x)=\ln(x)$ is concave, we get: for all $x,\ y \in]0,+\infty]$, for all $\theta \in [0,1]$,

$$\ln(\theta x+(1-\theta)y) \geq \theta \ln(x)+(1-\theta)\ln(y).$$

We choose $\theta=\frac{1}{p}$, so $1-\theta=1-\frac{1}{p}=\frac{1}{q}$. Thus,

$$\ln\left(\frac{x}{p}+\frac{y}{q}\right) \geq \frac{\ln(x)}{p}+\frac{\ln(y)}{q}.$$

Employing of new variables: $x=|v|^p$, $y=|w|^q$ for $v,\ w \in \mathbb{R}$, we obtain:

$$\begin{aligned}
& \ln\left(\frac{x}{p}+\frac{y}{q}\right) \geq \frac{\ln(x)}{p}+\frac{\ln(y)}{q}, \\
\Rightarrow\ & \ln\left(\frac{|v|^p}{p}+\frac{|w|^q}{q}\right) \geq \frac{\ln(|v|^p)}{p}+\frac{\ln(|w|^q)}{q}, \quad (\textit{new variables}), \\
\Rightarrow\ & \ln\left(\frac{|v|^p}{p}+\frac{|w|^q}{q}\right) \geq \frac{p\ln(|v|)}{p}+\frac{q\ln(|w|)}{q}, \quad (\textit{logarithm properties}), \\
\Rightarrow\ & \ln\left(\frac{|v|^p}{p}+\frac{|w|^q}{q}\right) \geq \ln(|v|)+\ln(|w|), \\
\Rightarrow\ & \ln\left(\frac{|v|^p}{p}+\frac{|w|^q}{q}\right) \geq \ln(|v\,w|), \quad (\textit{logarithm properties}), \\
\Rightarrow\ & e^{\ln\left(\frac{|v|^p}{p}+\frac{|w|^q}{q}\right)} \geq e^{\ln(|v\,w|)}, \quad (\textit{exponential is increasing}), \\
\Rightarrow\ & \frac{|v|^p}{p}+\frac{|w|^q}{q} \geq |v\,w|.
\end{aligned}$$

Theorem: (Hölder's inequality)

Let $n \in \mathbb{N}$, $x_k,\ y_k \in \mathbb{R}$ and for every $p, q \geq 1$, with $\frac{1}{p} + \frac{1}{q} = 1$, then:

$$\sum_{k=1}^{n} |x_k y_k| \leq \left(\sum_{k=1}^{n} |x_k|^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^{n} |y_k|^q\right)^{\frac{1}{q}}.$$

Proof: The previous Lemma of Young's inequality gives us:

$$|v\, w| \leq \frac{|v|^p}{p} + \frac{|w|^q}{q}.$$

Consider the following new variables:

$$v = x_k \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}}, \quad w = y_k \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}},$$

then Young's inequality becomes:

$$\left| x_k y_k \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}} \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}} \right| \leq \frac{1}{p} \left| x_k \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}} \right|^p + \frac{1}{q} \left| y_k \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}} \right|^q,$$

$$\Rightarrow \quad \left|x_k y_k\right| \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}} \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}} \leq \frac{|x_k|^p}{p} \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-p}{p}} + \frac{\left|y_k\right|^q}{q} \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-q}{q}}.$$

Now, determine the sum with respect indic k, for $i = 1, ..., n$:

$$\left(\sum_{k=1}^{n} \left|x_k y_k\right|\right) \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}} \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}} \leq \frac{1}{p} \left(\sum_{k=1}^{n} |x_k|^p\right) \left(\sum_{l=1}^{n} |x_l|^p\right)^{-1} + \frac{1}{q} \left(\sum_{k=1}^{n} \left|y_k\right|^q\right) \left(\sum_{l=1}^{n} |y_l|^q\right)^{-1},$$

$$\Rightarrow \quad \left(\sum_{k=1}^{n} \left|x_k y_k\right|\right) \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}} \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}} \leq \frac{1}{p} + \frac{1}{q},$$

$$\Rightarrow \quad \left(\sum_{k=1}^{n} \left|x_k y_k\right|\right) \left(\sum_{l=1}^{n} |x_l|^p\right)^{\frac{-1}{p}} \left(\sum_{l=1}^{n} |y_l|^q\right)^{\frac{-1}{q}} \leq 1,$$

which means that:

$$\sum_{k=1}^{n} |x_k y_k| \leq \left(\sum_{k=1}^{n} |x_k|^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^{n} |y_k|^q\right)^{\frac{1}{q}}.$$

Corollary: (Cauchy Schwartz inequality)

If we take $p = q = 2$ in the Hölder's inequality, we obtain directly the following Cauchy Schwartz inequality:

$$\sum_{k=1}^{n} |x_k y_k| \leq \left(\sum_{k=1}^{n} |x_k|^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^{n} |y_k|^q\right)^{\frac{1}{q}},$$

$$\Rightarrow \quad \sum_{k=1}^{n} |x_k y_k| \leq \left(\sum_{k=1}^{n} |x_k|^2\right)^{\frac{1}{2}} \left(\sum_{k=1}^{n} |y_k|^2\right)^{\frac{1}{2}}, \quad (p = q = 2).$$

So,

$$\sum_{k=1}^{n} |x_k y_k| \leq \sqrt{\left(\sum_{k=1}^{n} |x_k|^2\right)}\sqrt{\left(\sum_{k=1}^{n} |y_k|^2\right)}.$$

Or,

$$\left(\sum_{k=1}^{n} |x_k y_k|\right)^2 \leq \left(\sum_{k=1}^{n} |x_k|^2\right)\left(\sum_{k=1}^{n} |y_k|^2\right).$$

2

Mathematical proofs

2.1 Mathematical proof

2.1.1 What means proof in mathematics?

Mathematical proof is the logical way or steps in which mathematicians demonstrate that a statement is true. In general, and as we have shown in the previous chapter, the statements are needed to prove are theorems and lemmas. A theorem is a declaration that must demonstrated to be true using some mathematical operations and arguments. On the other hand, a lemma is a smaller theorem, which is needed to prove firstly, then we use it for the demonstration of a greater theorem.

2.1.2 Why are proofs important in mathematics?

1. Proofs are helpful us to understand why a mathematical statement is true or false.
2. Proofs are what lets mathematics work.
3. Without proofs, every mathematical would be purely speculative.
4. Proofs are considered as backbone of mathematics.
5. Proofs lead the mathematicians to build other broader theories.

2.2 Types of mathematical proofs

There are 3 principal types of mathematical proofs:

1. Direct proof, (proof by construction).

2. Proof by Contradiction.
3. Proof by Induction.

Going to explain the procedure of each one and give some illustrative examples.

2.2.1 Direct proof

Definition 2.1

The direct proof is the most common form of proof in mathematics. It starts with given information, rules, definitions, inferences, math logic and moves in the direction of the hypothesis that is to be proven.

Example 2.1

Prove that the sum of two odd numbers is even.

Proof: *Let* m *and* n *be two odd numbers, by using the definition of the odd number, we write* $m = 2k_1 + 1$ *and* $n = 2k_2 + 1$*, where* $k_1, k_2 \in \mathbb{Z}$*. Then,*

$$\begin{aligned} m+n &= (2k_1+1)+(2k_2+1), \\ &= 2k_1+2k_2+2, \\ &= 2(k_1+k_2+1), \\ &= 2k_3, \end{aligned}$$

where, $k_3 = k_1 + k_2 + 1 \in \mathbb{Z}$*. So, we can conclude that sum of two odd numbers is even.*

Example 2.2

Prove that: if α *is odd, then* α^2 *is odd.*

Proof: *Suppose that* α *is odd. Hence,* $\alpha = 2k + 1$*,* $k \in \mathbb{Z}$*, then:*

$$\begin{aligned} \alpha^2 &= (2k+1)^2, \\ &= 4k^2+4k+1, \\ &= 2(2k^2+2k)+1, \\ &= 2k'+1, \end{aligned}$$

where, $k' = 2k^2 + 2k \in \mathbb{Z}$*. Therefore* α^2 *is odd.*

2.2.2 Proof by Contradiction

Definition 2.2

Sometimes, it's hard or impossible to prove that a surmise is true using direct methods. For this reason, we introduce the proof by contradiction. The core idea of this proof is: Assume that statement needed to prove is false, then show that this assumption leads us to baloney. So, we were wrong by assuming that statement was false. Thus, we conclude that this statement must be true.

Remark 2.1

We mention that this type of proof is not used just to prove conditional statements, but also to prove many kind of statement whatsoever.

Example 2.3

Prove that $\sqrt{2}$ is irrational.

Proof: *Suppose that $\sqrt{2}$ is rational, so by using the definition of rational numbers, we write:*

$$\sqrt{2} = \frac{a}{b},$$

where, a, b are co-prime integers and $b \neq 0$. Thus:

$$\begin{aligned} \sqrt{2} &= \frac{a}{b}, \\ \Rightarrow \quad 2 &= \frac{a^2}{b^2}, \\ \Rightarrow \quad 2b^2 &= a^2, \end{aligned}$$

which means that b^2 divides a^2, then b divides a, this is a contradiction because a, b are co-prime. So, we can conclude that $\sqrt{2}$ is an irrational number.

Example 2.4

Prove that: if β^2 is even, then β is even.

Proof: *Suppose that β^2 is even and β is odd.*

Since β is odd, there exists $c \in \mathbb{Z}$ for which $\beta = 2c + 1$. Then:

$$\begin{aligned} \beta^2 &= (2c+1)^2, \\ &= 4c^2 + 4c + 1, \\ &= 2(2c^2 + 2c) + 1, \\ &= 2d + 1, \end{aligned}$$

where, $d = 2c^2 + 2c \in \mathbb{Z}$*, so* β^2 *is odd. This is leads us to a contradiction. Then, our supposition that* β^2 *is even and* β *is odd was not be correct. Finally, we conclude that if* β^2 *is even, then* β *is even.*

2.2.3 Proof by Induction

Definition 2.3

Proof by induction is a way of proving that a certain statement is true for every positive integer n. Proof by induction has three steps:

1. Prove the base case: this means to prove that this statement is true for the initial value $n = 0$. (Or for initial value n_0).
2. Assume that statement is true for $n = k$. This step is known by inductive hypothesis.
3. Prove that statement is true for $n = k + 1$. This step is known by inductive step.

Remark 2.2

Proof by induction is an incredibly useful tool to prove a wide variety of things, including problems about divisibility, matrices and series.

Example 2.5

Prove by induction that: $n^2 > 2n$ *for any* $n \in \mathbb{N}$, $n > 2$.

Proof: *Let* $P_1(n)$ *be the statement:* $n^2 > 2n$.

Base case: *If* $n = 3$*, we get:*

$$3^2 = 9 > 6 = 2 \times 3.$$

So $P_1(3)$ *is true.*

Induction hypothesis: *We suppose that* $P_1(k)$ *is true for* $k \in \mathbb{N}$, $k > 2$*. That meaning* $k^2 > 2k$.

Induction step: *We prove that* $P_1(k+1)$ *is true. That meaning* $(k+1)^2 > 2(k+1)$.

We have:

$$\begin{aligned} (k+1)^2 &= k^2 + 2k + 1, \\ &> 2k + 2k + 1, \quad \textit{by the induction hypothesis,} \\ &> 2k + 2, \qquad \textit{clearly,} \\ &= 2(k+1). \end{aligned}$$

So $(k+1)^2 > 2(k+1)$*, this means that* $P_1(k+1)$ *is true.*

Example 2.6

Prove by induction that: for any $n \in \mathbb{N}$:

$$1+2+3+...+n = \frac{n(n+1)}{2}.$$

Proof: *Let $P_2(n)$ be the mathematical statement:*

$$P_2(n):\ 1+2+3+...+n = \frac{n(n+1)}{2}.$$

Base case: *If $n = 1$, we get:*

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1.$$

So $P_2(1)$ is true.

Induction hypothesis: *We suppose that $P_2(k)$ is true for $k \in \mathbb{N}$. That meaning:*

$$P_2(k):\ 1+2+3+...+k = \frac{k(k+1)}{2}.$$

Induction step: *We prove that $P_2(k+1)$ is true. That meaning:*

$$P_2(k+1):\ 1+2+3+...+k+k+1 = \frac{(k+1)(k+2)}{2}.$$

We have:

$$\begin{aligned} 1+2+3+...+k+k+1 &= \frac{k(k+1)}{2}+k+1, \\ &= \frac{k(k+1)+2(k+1)}{2}, \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

So, we conclude that $P_2(k+1)$ is true.

2.3 Other types of proofs

There are many other types of proof. We focus only on the following common types:

1. Proof by Cases.
2. Proof by Counterexample.
3. Proof by Contraposition.

2.3.1 Proof by Cases

Definition 2.4

Sometimes, it's not possible (or very difficult) to prove the whole theorem at once. So, by using the proof by cases, we divide up all possibilities into different cases, and then prove our claim for each one separately.

Example 2.7

For any integer y, the integer $y(y+1)$ is even.

Proof: *If y is even, then $y = 2k$, $k \in \mathbb{Z}$. So, we obtain:*

$$\begin{aligned} y(y+1) &= 2k(2k+1), \\ &= 2(2k^2+k), \\ &= 2k', \end{aligned}$$

where, $k' = 2k^2+k$, $d \in \mathbb{Z}$. Thus $y(y+1)$ is even.

If y is odd, then $y = 2k+1$, $k \in \mathbb{Z}$. So, we obtain:

$$\begin{aligned} y(y+1) &= (2k+1)(2k+1+1), \\ &= (2k+1)(2k+2), \\ &= 2(2k+1)(k+1), \\ &= 2(2k^2+3k+1), \\ &= 2k', \end{aligned}$$

where, $k' = 2k^2+3k+1$, $d \in \mathbb{Z}$. Thus $y(y+1)$ is even.

So, in both cases we proved that $y(y+1)$ is even.

2.3.2 Proof by Counterexample

Definition 2.5

A mathematical statement can be disproved by finding one counterexample. A counterexample is an example for which the given statement will be not true.

Example 2.8

For every positive integer n, we have: $n! \leq n^2$.

Proof: *The number 4 is a positive integer. But $4! = 24$ is not less or equal to $4^2 = 16$. Therefore, given conjecture is false.*

2.3.3 Proof by Contraposition

Definition 2.6

The core idea of this proof is: The truth of any proposition is equivalent to the truth of its contrapositive. Thus, we prove the contrapositive instead.

Example 2.9

Prove that: for any $\gamma \in \mathbb{Z}$, *if* $7\gamma + 9$ *is even, then* γ *is odd.*

Proof: *Proof by contraposition allow us to prove that:*

$$\text{for any } \gamma \in \mathbb{Z}, \text{ if } \gamma \text{ is even, then } 7\gamma + 9 \text{ is odd.}$$

Thus γ *is even, so* $\gamma = 2k$, $k \in \mathbb{Z}$. *Then:*

$$\begin{aligned} 7\gamma + 9 &= 7(2k) + 9, \\ &= 14k + 9, \\ &= 14k + 8 + 1, \\ &= 2(7k + 4) + 1, \\ &= 2k' + 1, \end{aligned}$$

where, $k' = 7k + 4$, $d \in \mathbb{Z}$, *Consequently* $7\gamma + 9$ *is odd.*

2.4 Other types of induction’s proof

In mathematical, the proof by induction is a technique used to prove statements which are related about natural numbers. In the previous section, we have shown the most common type. This type is called *simple induction proof,* it assumes the statement is true for k and proves it for $k+1$. However, there are other different types of proof by induction. Here, we will take care of the following two types:

1. Double induction proof.
2. Strong induction proof.

2.4.1 Double induction proof

Definition 2.7

Double induction proof is a way of proving that a certain statement $P(n)$ is true according to the following steps:

1. **Base case:** Prove that $P(0)$ and $P(1)$ are true. (Or other base cases $P(n_0), P(n_0+1)$).
2. **Inductive hypothesis:** For any $k \in \mathbb{N}$, assume that $P(k-1)$ and $P(k)$ are true.
3. **Inductive step:** Prove that $P(k+1)$ is true.

Example 2.10

Prove that $\alpha_n = 2^n$, $n \in \mathbb{N}$ *is a solution to the recurrence relation*

$$\begin{cases} \alpha_n = 5\alpha_{n-1} - 6\alpha_{n-2}, \\ \alpha_0 = 1, \alpha_1 = 2, \end{cases}$$

Proof: *Let* $P(n)$ *be the statement:*

$$\alpha_n = 2^n,\ n \in \mathbb{N} \quad \textit{is a solution of} \quad \alpha_n = 5\alpha_{n-1} - 6\alpha_{n-2}, \quad \textit{with} \quad \alpha_0 = 1,\ \alpha_1 = 2.$$

Base case: *We have:*

$$\alpha_0 = 2^0 = 1, \quad \alpha_1 = 2^1 = 1,$$

both agree with the initial conditions. So, $P(0)$ *and* $P(1)$ *are true.*

Induction hypothesis: *We suppose that* $P(k-1)$ *and* $P(k)$ *are true. This meaning:*

$$\alpha_{k-1} = 2^{k-1}, \quad \alpha_k = 2^k.$$

Induction step: *We prove that* $P(k+1)$ *is true. This meaning:*

$$\alpha_{k+1} = 2^{k+1}, \quad \textit{is a solution of} \quad \alpha_{k+1} = 5\alpha_k - 6\alpha_{k-1}.$$

We have

$$\begin{aligned} \alpha_{k+1} &= 5\alpha_k - 6\alpha_{k-1}, \\ &= 5 \times 2^k - 6 \times 2^{k-1}, \quad \textit{(induction hypothesis)}, \\ &= 10 \times 2^{k-1} - 6 \times 2^{k-1}, \\ &= 4 \times 2^{k-1}, \\ &= 2^{k+1}. \end{aligned}$$

So, we conclude that $P(k+1)$ *is true.*

2.4.2 Strong induction proof

Definition 2.8

Strong induction proof is a way of proving that a certain statement $P(n)$ is true according to the following steps:

1. **Base case:** Prove that $P(0)$ is true. (Or other base case $P(n_0)$).
2. **Inductive hypothesis:** Assume that $P(m)$ is true for all $m \leq k$.
3. **Inductive step:** Prove that $P(k+1)$ is true.

Example 2.11

Prove that: For any natural number $n \geq 2$, is either prime or can be written as product of primes.

Proof: *Let $P(n)$ be the statement:*

$$P(n): \text{ For } n \geq 2, n \text{ is either prime or is the product of primes.}$$

Base case: *Clearly that $P(2)$ is true, because 2 is prime.*

Induction hypothesis: *We suppose that $P(m)$ is true for all $2 \leq m \leq k$. Meaning that m is either prime or is a product of primes.*

Induction step: *We prove that $P(k+1)$ is true. Meaning that $k+1$ is either prime or is a product of primes.*

Here, we have two cases:

Case 1: *If $k+1$ is prime, hence $P(k+1)$ is true.*

Case 2: *If $k+1$ is not prime, then $k+1$ has more than 2 divisors, so we can write:*

$$k+1 = pq, \quad \text{where}, \quad p, q \in [[2, k]].$$

By the inductive hypothesis p and q are each either primes or are product of primes. Thus, also $k+1$ can be written as product of primes. So, we conclude that $P(k+1)$ is true.

2.5 Exercises

Exercise 2.1

Use the direct proof method to prove the following statements:

1. The equation $h(x) = e^x - 2x$, has no roots.
2. For any angle θ, we have: $\cos^2(\theta) + \sin^2(\theta) = 1$.
3. The inverse of the matrix $A = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix}$ is the matrix $B = \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix}$.

Exercise 2.2

Use the proof by contradiction to prove the following statements:

1. There are no integers a and b for which $5a + 10b = 1$.
2. If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.
3. For all $x, y \in \mathbb{R}$, if $x \neq y$, $x > 0$, $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

Exercise 2.3

Use the proof by induction to prove the following statements:

1. For all $n \in \mathbb{N}$, $n \geq 3$, we have: $2^n > n + 4$.
2. For any positive integer n, we have: $1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$.
3. For all $n \in \mathbb{N}$, then $3^{2n+2} + 8n - 9$ is divisible by 8.

Exercise 2.4

Prove the following statements using the appropriate method.

1. The sum of two square numbers is always a square number.
2. If $x^2 - 6x + 5$ is even, then x is odd.
3. If n is an integer, then $3n^2 + n + 10$ is even.

Exercise 2.5

By the double induction proof, prove that:

$$\textit{For all} \quad n \in \mathbb{N}, \quad (1+\sqrt{2})^n + (1-\sqrt{2})^n \in \mathbb{N}.$$

Exercise 2.6

By the strong induction proof, prove that:

$$\forall n \in \mathbb{N}^*, \exists (p,q) \in \mathbb{N}^2, \quad \textit{such that} \quad n = 2^p(2q+1).$$

2.6 Solutions

Solution of exercise 2.1:

By using the direct proof method, we will prove the statements 1, 2 and 3, respectively.

1. To prove that equation $h(x) = e^x - 2x$ has no roots, we need just to study its variation table. Clearly that $D_h = \mathbb{R}$, so:

$$\lim_{x\to-\infty} h(x) = \lim_{x\to-\infty} (e^x - 2x) = +\infty,$$

and,

$$\lim_{x\to+\infty} h(x) = \lim_{x\to+\infty} (e^x - 2x) = \lim_{x\to+\infty} x\left(\frac{e^x}{x} - 2\right) = +\infty.$$

Also, we have $h'(x) = e^x - 2$, thus:

$$h'(x) = 0 \Rightarrow e^x - 2 = 0 \Rightarrow x = \ln(2),$$

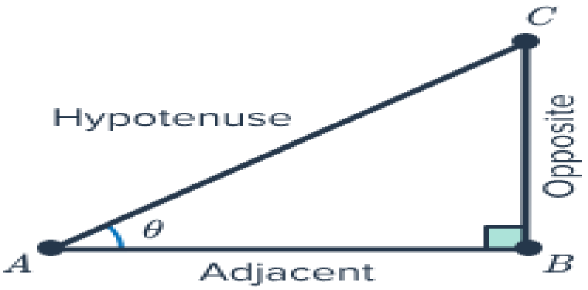
then, we get the variation table:

x	$-\infty$		$\ln(2)$		$+\infty$
$h'(x) = e^x - 2$		$-$	0	$+$	
$h(x) = e^x - 2x$	$+\infty$	$\searrow$	$h(\ln(2)) \approx 0.61$	$\nearrow$	$+\infty$

Based on this table, we see that $h(x) > 0$, which confirm us that equation has no roots.

2. Prove that $\cos^2(\theta) + \sin^2(\theta) = 1$.

Let ABC be a right Triangle which described down:



The geometric formulas of $\cos(\theta)$ and $\sin(\theta)$ are given as:

$$\cos(\theta) = \frac{Adjacent}{Hypotenuse} = \frac{AB}{AC}, \qquad \sin(\theta) = \frac{Opposite}{Hypotenuse} = \frac{BC}{AC}.$$

So,

$$\cos^2(\theta)+\sin^2(\theta)=\left(\frac{AB}{AC}\right)+\left(\frac{BC}{AC}\right)=\frac{AB^2}{AC^2}+\frac{BC^2}{AC^2}=\frac{AB^2+BC^2}{AC^2}.$$

Furthermore, Pythagorean theorem states that: $AB^2+BC^2=AC^2$, which allows to get:

$$\cos^2(\theta)+\sin^2(\theta)=\frac{AB^2+BC^2}{AC^2}=\frac{AC^2}{AC^2}=1.$$

3. To prove that matrix A is the inverse of matrix B, we must verify that $AB=BA=I$.

We have:

$$\begin{aligned} AB &= \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix}\begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix} \\ &= \begin{pmatrix} -14+6+9 & 56-22-34 & -35+14+21 \\ 0+9-9 & 0-33+34 & 0+21-21 \\ 6+12-18 & -24-44+68 & 15+28-42 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Also,

$$\begin{aligned} BA &= \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix}\begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \\ &= \begin{pmatrix} -14+0+15 & -4+24-20 & -2-8+10 \\ 21+0-21 & 6-33+28 & 3+11-14 \\ 63+0-63 & 18-102+84 & 9+34-42 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

So, $AB=BA=I$, then A is inverse of B.

Solution of exercise 2.2:

By using the proof by contradiction, we will prove the statements 1, 2 and 3, respectively.

1. To prove that there are no integers a and b for which $5a+10b=1$, we suppose that there are two integers a and b satisfying the equation $5a+10b=1$.

First, we have:

$$\begin{aligned} & 5a+10b=1, \\ \Rightarrow\ & 5(a+2b)=1, \\ \Rightarrow\ & (a+2b)=\frac{1}{5}, \\ \Rightarrow\ & a+2b=0.2. \end{aligned}$$

And, as $a,b\in\mathbb{Z}$, hence $a+2b\in\mathbb{Z}$, but we have found $a+2b=0.2\in\mathbb{R}$, which leads us to contradiction. So, we conclude that statement 1 is correct.

2. To prove that: If $a, b \in \mathbb{Z}$, then $a^2-4b \neq 2$, we suppose that for any $a, b \in \mathbb{Z}$, then $a^2-4b = 2$. First, we have:

$$\begin{aligned}
& a^2-4b = 2,\\
\Rightarrow\quad & a^2 = 4b+2,\\
\Rightarrow\quad & a^2 = 2(2b+1),\\
\Rightarrow\quad & a^2 = 2b', \quad where \quad b' = 2b+1 \in \mathbb{Z},
\end{aligned}$$

which means that a^2 is an even number, it follows that a is also an even number. We put $a = 2x$, where $x \in \mathbb{Z}$, and substitute again in the first equation:

$$\begin{aligned}
& a^2-4b = 2,\\
\Rightarrow\quad & (2x)^2-4b = 2, \quad (a = 2x),\\
\Rightarrow\quad & 4x^2-4b = 2,\\
\Rightarrow\quad & 4b = 4x^2+2,\\
\Rightarrow\quad & b = x^2+0.5.
\end{aligned}$$

And, like $x \in \mathbb{Z}$ then $x^2+0.5 \in \mathbb{R}$, but we have $b \in \mathbb{Z}$, which leads us to contradiction. So, we conclude that statement 2 is correct.

3. To prove that for all real numbers x and y, if $x \neq y$, $x > 0$, $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$, we suppose that $x \neq y$, $x > 0$, $y > 0$, then $\frac{x}{y} + \frac{y}{x} \leq 2$.

First, we have:

$$\begin{aligned}
& \frac{x}{y} + \frac{y}{x} \leq 2,\\
\Rightarrow\quad & \frac{x^2+y^2}{yx} \leq 2,\\
\Rightarrow\quad & x^2+y^2 \leq 2yx, \quad (due\ to \quad x > 0 \quad and \quad y > 0),\\
\Rightarrow\quad & x^2+y^2-2yx \leq 0,\\
\Rightarrow\quad & (x-y)^2 \leq 0,\\
\Rightarrow\quad & (x-y)^2 < 0, \quad (due\ to \quad x \neq y),
\end{aligned}$$

which is a contradiction, because the quantity $(x-y)^2 > 0$. So, we conclude that statement 3 is correct.

Solution of exercise 2.3:

By using the proof by induction, we will prove the statements 1, 2 and 3, respectively.

1. We prove that: $P_1(n): 2^n > n+4,\ \forall n \in \mathbb{N},\ n \geq 3.$

Base case: If $n=3$ we have:

$$2^3 = 8 > 7 = 3+4,$$

So $P_1(3)$ is true.

Induction hypothesis: We suppose that $P_1(k): 2^k > k+4,\ \forall k \in \mathbb{N},\ k \geq 3$ is true.

Induction step: We prove that $P_1(k+1): 2^{k+1} > k+5,\ \forall k \in \mathbb{N},\ k \geq 3$ is true.

We have:

$$\begin{aligned}
& 2^k > k+4, \quad (\textit{induction hypothesis}),\\
\Rightarrow\quad & 2^k \times 2 > (k+4) \times 2, \quad (\textit{product by} \quad 2),\\
\Rightarrow\quad & 2^{k+1} > 2k+8,\\
\Rightarrow\quad & 2^{k+1} > k+5+(k+3),\\
\Rightarrow\quad & 2^{k+1} > k+5, \quad (\textit{because} \quad k+3>0).
\end{aligned}$$

This means that $P_1(k+1)$ is true.

2. We prove that:

$$P_2(n):\ 1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6},\ n \in \mathbb{N}^*$$

. **Base case:** If $n=1$ we have:

$$\frac{1(1+1)(2+1)}{6} = \frac{6}{6} = 1 = 1^2,$$

So $P_2(1)$ is true.

Induction hypothesis: We suppose that:

$$P_2(k):\ 1^2+2^2+\ldots+k^2 = \frac{k(k+1)(2k+1)}{6},\ k \in \mathbb{N}^*.$$

Induction step: We prove that:

$$P_2(k+1):\ 1^2+2^2+\ldots+(k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6},\ k \in \mathbb{N}^*.$$

We have:

$$\begin{aligned}
1^2+2^2+\ldots+(k+1)^2 &= 1^2+2^2+\ldots+k^2+(k+1)^2,\\
&= \frac{k(k+1)(2k+1)}{6}+(k+1)^2, \quad (\textit{induction hypothesis}),\\
&= \frac{k(k+1)(2k+1)}{6}+\frac{6(k+1)(k+1)}{6},\\
&= \frac{(k+1)((2k+1)k+6(k+1))}{6},\\
&= \frac{(k+1)(2k^2+7k+6)}{6},\\
&= \frac{(k+1)(k+2)(2k+3)}{6}, \quad ((k+2)(2k+3)=2k^2+7k+6).
\end{aligned}$$

This means that $P_2(k+1)$ is true.

3. We prove that: $P_3(n): 3^{2n+2}+8n-9=8\alpha$, $\alpha\in\mathbb{Z}$, $n\in\mathbb{N}$.

Base case: If $n=0$ we have:

$$3^{0+2}+0-9=9-9=0=8\times 0,$$

So $P_3(0)$ is true.

Induction hypothesis: We suppose that $P_3(k): 3^{2k+2}+8k-9=8\alpha$, $\alpha\in\mathbb{Z}$, $k\in\mathbb{N}$. is true.

Induction step: We prove that $P_3(k+1): 3^{2(k+1)+2}+8(k+1)-9=8\beta$, $\beta\in\mathbb{Z}$, $k\in\mathbb{N}$ is true.

We have:

$$\begin{aligned}
3^{2(k+1)+2}+8(k+1)-9 &= 3^{2k+2+2}+8k+8-9,\\
&= 3^2\times 3^{2k+2}+8k+8-9,\\
&= 9\times 3^{2k+2}+8k-9+8,\\
&= (8+1)\times 3^{2k+2}+8k-9+8,\\
&= 8\times 3^{2k+2}+3^{2k+2}+8k-9+8,\\
&= 8\times 3^{2k+2}+8+(3^{2k+2}+8k-9),\\
&= 8\times 3^{2k+2}+8+8\alpha, \quad (\textit{induction hypothesis}),\\
&= 8(3^{2k+2}+1+\alpha),\\
&= 8\beta, \quad \beta=3^{2k+2}+1+\alpha\in\mathbb{Z}.
\end{aligned}$$

This means that $P_3(k+1)$ is true.

Solution of exercise 2.4:

1. We will prove that statement:

The sum of two square numbers is always a square number, is false using the proof by counterexample.

It's clear that:

$$\begin{aligned} a &= 16 \ \textit{is square number because } 16 = 4^2, \\ b &= 4 \ \textit{is square number because } 4 = 2^2, \end{aligned}$$

but,

$$a + b = 16 + 4 = 20 \ \textit{is not square number},$$

which conclude that the given statement is not true.

2. To prove that:

$$\textit{If } x^2 - 6x + 5 \ \textit{ is even, then } x \ \textit{ is odd},$$

we use the proof by contraposition. Thus, we prove instead that:

$$\textit{If } x \ \textit{ is even, then } x^2 - 6x + 5 \ \textit{ is odd}.$$

We take $x = 2\alpha$, $\alpha \in \mathbb{Z}$, then we get:

$$\begin{aligned} x^2 - 6x + 5 &= (2\alpha)^2 - 6(2\alpha) + 5, \\ &= 4\alpha^2 - 12\alpha + 5, \\ &= 4\alpha^2 - 12\alpha + 4 + 1, \\ &= 2(2\alpha^2 - 6\alpha + 2) + 1, \\ &= 2\beta + 1, \quad \beta = 2\alpha^2 - 6\alpha + 2 \in \mathbb{Z}, \end{aligned}$$

so, we obtain that $x^2 - 6x + 5$ is odd.

3. We will prove that statement:

$$\textit{If } n \ \textit{ is an integer, then } 3n^2 + n + 10 \ \textit{ is even},$$

is true using the proof by cases.

First, if n is even, so $n = 2\alpha$, $\alpha \in \mathbb{Z}$, then:

$$\begin{aligned} 3n^2 + n + 10 &= 3(2\alpha)^2 + 2\alpha + 10, \\ &= 12\alpha^2 + 2\alpha + 10, \\ &= 2(6\alpha^2 + \alpha + 5), \\ &= 2\beta, \quad \beta = 6\alpha^2 + \alpha + 5 \in \mathbb{Z}, \end{aligned}$$

which confirm that $3n^2+n+10$ is even.

Second, if n is odd, so $n=2\alpha+1$, $\alpha\in\mathbb{Z}$, then:

$$\begin{aligned}3n^2+n+10 &= 3(2\alpha+1)^2+(2\alpha+1)+10,\\ &= 3(4\alpha^2+4\alpha+1)+2\alpha+1+10,\\ &= 12\alpha^2+12\alpha+3+2\alpha+1+10,\\ &= 12\alpha^2+14\alpha+14,\\ &= 2(6\alpha^2+7\alpha+7),\\ &= 2\beta,\quad \beta=6\alpha^2+7\alpha+7\in\mathbb{Z},\end{aligned}$$

which confirm again that $3n^2+n+10$ is even.

Consequently, the given statement is true.

Solution of exercise 2.5:

We will prove the statement using the double induction proof.

Let $P(n)$ be the statement:

$$P(n):\ For\ all\quad n\in\mathbb{N},\quad (1+\sqrt{2})^n+(1-\sqrt{2})^n\in\mathbb{N}.$$

Base case: We have:

$$(1+\sqrt{2})^0+(1-\sqrt{2})^0=1+1=2\in\mathbb{N},\quad (1+\sqrt{2})^1+(1-\sqrt{1})^1=2\in\mathbb{N}.$$

So, $P(0)$ and $P(1)$ are true.

Induction hypothesis: We suppose that $P(k-1)$ and $P(k)$ are both true. This meaning:

$$(1+\sqrt{2})^{k-1}+(1-\sqrt{2})^{k-1}\in\mathbb{N}\quad and\quad (1+\sqrt{2})^k+(1-\sqrt{2})^k\in\mathbb{N}.$$

Induction step: We prove that $P(k+1)$ is true. This meaning:

$$(1+\sqrt{2})^{k+1}+(1-\sqrt{2})^{k+1}\in\mathbb{N}.$$

We have

$$\begin{aligned}
(1+\sqrt{2})^{k+1}+(1-\sqrt{2})^{k+1} &= (1+\sqrt{2})^2(1+\sqrt{2})^{k-1}+(1-\sqrt{2})^2(1-\sqrt{2})^{k-1},\\
&= (3+2\sqrt{2})(1+\sqrt{2})^{k-1}+(3-2\sqrt{2})(1-\sqrt{2})^{k-1},\\
&= (1+2(1+\sqrt{2}))(1+\sqrt{2})^{k-1}+(1+2(1-\sqrt{2}))(1-\sqrt{2})^{k-1},\\
&= (1+\sqrt{2})^{k-1}+2(1+\sqrt{2})^{k}+(1-\sqrt{2})^{k-1}+2(1-\sqrt{2})^{k},\\
&= (1+\sqrt{2})^{k-1}+(1-\sqrt{2})^{k-1}+2((1+\sqrt{2})^{k}+(1-\sqrt{2})^{k}),\\
&= \alpha+2\beta,\ \alpha,\beta\in\mathbb{N}\quad \textit{(induction hypothesis)},\\
&\in \mathbb{N}.
\end{aligned}$$

So, we conclude that $P(k+1)$ is true.

Solution of exercise 2.6:

We will prove the statement using the strong induction proof.

Let $P(n)$ be the statement:

$$P(n):\ \forall n\in\mathbb{N}^*, \exists(p,q)\in\mathbb{N}^2,\quad \textit{such that}\quad n=2^p(2q+1).$$

Base case: We have when $n=1$,

$$1=2^0(2\times 0+1).$$

So, $P(1)$ is true.

Induction hypothesis: We suppose that $P(m)$ is true for all $1\le m\le k$. This meaning:

$$\forall m\in\mathbb{N}^*,\ 1\le m\le k,\ \exists(p,q)\in\mathbb{N}^2,\quad \textit{such that}\quad m=2^p(2q+1).$$

Induction step: We prove that $P(k+1)$ is true. This meaning:

$$\exists(p,q)\in\mathbb{N}^2,\quad \textit{such that}\quad k+1=2^p(2q+1).$$

Here, we have two cases:

Case 1: If $k+1$ is odd, then exists $q\in\mathbb{N}$, such that:

$$k+1=2q+1=2^0(2q+1),$$

this implies that $P(k+1)$ is true directly.

Case 2: If $k+1$ is even, then exists $q \in \mathbb{N}$, such that:

$$\begin{aligned} k+1 &= 2m, \quad \textit{where,} \quad 1 \leq m < k+1, \\ &= 2m, \quad \textit{where,} \quad m \in [[1,k]], \\ &= 2 \times (2^p(2q+1)), \quad (\textit{by inductive hypothesis}), \\ &= 2^{p+1}(2q+1), \\ &= 2^{p'}(2q+1), \ \ p' = p+1 \in \mathbb{N}. \end{aligned}$$

So, we conclude that $P(k+1)$ is true.

3

Set theory

Set theory is a branch in mathematics, takes care of studying of sets and their properties. This branch has been been initiated by the German mathematician **Georg Cantor (1845-1918)**. Set theory have become one of the most field in mathematics, because it has an important role to explain the other fundamental concepts such as: relations, functions, sequences, probability, geometry, etc. In this chapter, we will going to discuss about:

1. Definitions and properties of sets.
2. Operations on sets.
3. Applications on sets.

3.1 Basic definitions

3.1.1 Definition of sets

Definition 3.1

In mathematics, the sets are considered as collection of objects. These objects can be numbers, points, symbols, etc, which are called elements or members.

3.1.2 Representation of sets

The sets can be represented in two ways:

1. Roster form.
2. Builder form.

Definition 3.2: (Roster form)

In Roster form, the elements of the set are listed, comma-separated and enclosed between curly braces {}.

Example 3.1

$$A = \{1996, 2000, 2004, 2008, 2012, 2016\}$$

$$B = \{A, D, R, E, S, G\}$$

$$C = \{Yellow, Blue, Red, Green\}$$

Definition 3.3: (Builder form)

In Builder form, the elements of the given have a common property. This property cannot be applicable to the objects which do not belong to this set.

Example 3.2

If S_1 is defined as the set of all ***odd prime numbers****. So, S_1 can represented by:*

$$S_1 = \{\alpha : \alpha \ \textit{is an odd prime number}\}$$

where $'\alpha'$ is a symbolic representation that is used to describe the element, and $':'$ means 'such that' (which can replaced by $'|'$).

Example 3.3

If S_2 is defined as the set of all ***odd natural numbers****. So, S_2 can represented by:*

$$S_2 = \{\alpha : \alpha \ \textit{is an odd natural number}\},$$

or

$$S_2 = \{\alpha \,|\, \alpha = 2k + 1 \, and \, k \in \mathbb{N}\},$$

or

$$S_2 = \{\alpha \,|\, \alpha = 2k + 1, \ k \in \mathbb{N}\},$$

or

$$S_2 = \{2k + 1 \,|\, k \in \mathbb{N}\}.$$

Remark 3.1

1. *The order doesn't matter for sets represented by the Roster form:*

$$S = \{A, F, D, R, E, B\} = \{F, E, B, D, A, R\}.$$

2. *Multiplication is ignored while representing the sets:*

$$S \neq \{A, D, D, B, R, E, F, F\}.$$

3. *Enumerate members of set, can be enclosed by curly braces ' ' or " ":*

$$V = \{'a', 'e', 'i', 'o', 'u', 'y'\}.$$

$$C = \{''Red'', ''Yellow'', ''Blue'', ''Green'', ''Black''\}.$$

4. *$a \in S$ denotes: a is **an element** of the set S.*
5. *$a \notin S$ denotes: a is **not an element** of the set S.*
6. *$\wedge$ denotes: **AND**, hence, $a \wedge b$ means a and b.*
7. *$\vee$ denotes: **OR**, hence, $a \vee b$ means a or b.*

3.1.3 Some important sets

There are several symbols that are adopted for common sets. They are given as follows:

1. $\mathbb{N}$: Define the set of Natural numbers.

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

2. $\mathbb{Z}$: Define the set of integers.

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

3. $\mathbb{Q}$: Define the set of Rational numbers.

$$\mathbb{Q} = \left\{ \frac{p_1}{p_2} \mid p_1 \in \mathbb{Z} \text{ and } p_2 \in \mathbb{Z} \ and \ p_2 \neq 0 \right\}.$$

$$\mathbb{Q} = \left\{ \frac{p_1}{p_2} \mid p_1 \in \mathbb{Z} \wedge p_2 \in \mathbb{Z} \wedge p_2 \neq 0 \right\}.$$

4. $\mathbb{R}$: Define the set of Real numbers.

5. $\mathbb{C}$: Define the set of Complex numbers.

6. **Closed interval:**
$$[\alpha,\beta]=\{x\in\mathbb{R}\,|\,\alpha\le x\le\beta\}.$$

7. **Open interval:**
$$(\alpha,\beta)=\{x\in\mathbb{R}\,|\,\alpha< x<\beta\}.$$

8. **Half-open interval:**
$$[\alpha,\beta)=\{x\in\mathbb{R}\,|\,\alpha\le x<\beta\}.$$
$$(\alpha,\beta]=\{x\in\mathbb{R}\,|\,\alpha< x\le\beta\}.$$

9. **The universal set:** denoted by U or Ω. It is the set of all elements under consideration.

10. **The empty set:** denoted by $\{\}$ or $\emptyset$. It is the set containing no elements.

3.2 Venn diagrams

Definition 3.4

A Venn diagram is a diagram that helps us to visualize the logical relationship between sets and their elements.

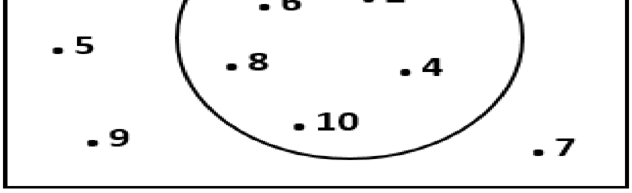
Example 3.4

Here, U is the universal set contains all the numbers $1-10$*, enclosed within the rectangle.*

$$U=\{1,2,3,4,5,6,7,8,9,10\}.$$

A *is the set contains the even numbers between* $1-10$. A *is a subset of universal set* U*, and it is placed inside the circle.*

$$A=\{2,4,6,8,10\}.$$



3.3 Types of sets

The sets are further categorized into different types, based on their elements or their types of elements. We list some of them:

1. **Universal set:** Denoted before.

2. **Empty set:** Denoted before.

3. **Singleton set:** It has one element. $S = \{901\}$.

4. **Finite set:** The number of its elements is finite.

$$S = \{E, L, G, H\},\ S = \{40, 41, 42, ..., 70\}.$$

5. **Infinite set:** The number of its elements is infinite.

$$S = \mathbb{N},\ S = \mathbb{R},\ S = [\alpha, \beta].$$

6. **Equal sets:** We say that two sets are equal, if they have the same elements.

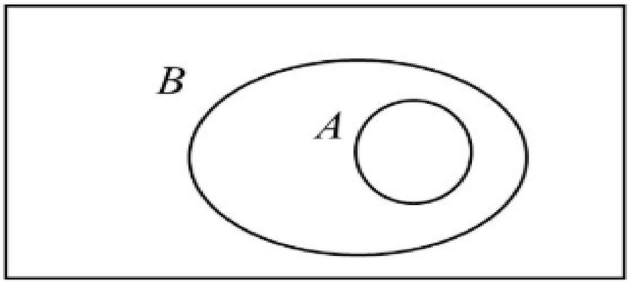
$$S_1 = \{56, 70, 11, 41\},\ S_2 = \{41, 70, 56, 11\} \Rightarrow S_1 = S_2.$$

7. **Equivalent sets:** We say that two sets are equivalent, if they have the same number of elements.

$$S_1 = \{671, 2009, 3, 94, 86\},\ S_2 = \{K, N, Z, H, O\}.$$

   So, S_1 and S_2 are equivalent.

8. **Subset:** We say that A is subset of the set B, if all elements of A belong to B. And we write $A \subseteq B$.



Remark 3.2

1. *The relationship represented by $A \subset B$ is read: A is a proper subset of B.*
2. *Any set A is a subset of itself. i.e. $A \subseteq A$.*
3. *The empty set $\emptyset$ is a subset of any set. i.e. $\forall S,\ \emptyset \subseteq S$.*

3.4 Cardinality of Sets

Definition 3.5

The cardinality of a set is defined by the number of its elements. Let S be a set. If there are exactly k (distinct) elements in S, we say that k is the cardinality of S. We write:

$$n(S) = |S| = k.$$

Example 3.5

It's clear that:

$$S_1 = \{'a','e','i','o','u','y'\} \Rightarrow |S_1| = 6.$$

$$S_2 = \{0.4, 24, 10, 0, -3, 1.6, 11\} \Rightarrow n(S_2) = 7.$$

3.4.1 Countable sets

Definition 3.6

We say that a set S is countable, if one of the conditions is satisfied:

1. If S is a finite set.
2. If there is a bijection application from this set S to the set of natural numbers $\mathbb{N}$.

If the set S is countable and infinite, then S called countably infinite set.

Example 3.6

The following sets $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are countable.

3.4.2 Uncountable sets

Definition 3.7

We say that S is uncountable (or uncountably infinite) if S is not countable.

Example 3.7

Real numbers $\mathbb{R}$ is an uncountable sets.

Intervals: $[a,b], (a,b], [a,b), (a,b)$ are also uncountable sets.

3.4.3 Power sets

Definition 3.8

Let S be a set. Power set of S is denoted by $P(S)$. It is defined by the set contains all subsets of S and including also the empty set $\{\}$.

Example 3.8

Let S be a set defined by:

$$S = \{1, 2, 3\}$$

Let us find the power set of S.

$$P(S) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Theorem 3.1

Let S be a finite set. So, if $n(S) = m$ then $n(P(S)) = 2^m$.

Proof: *Leave to the student.*

3.5 Operations on sets

The set operations are performed on two or more sets to obtain a combination of elements as per the operation performed on them. There are many different operations, such as:

1. Union.
2. Intersection.
3. Complement.
4. Difference.
5. Symmetric difference.

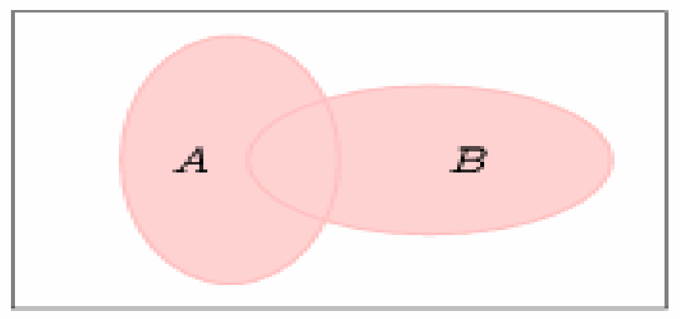
Let us discuss these operations one by one.

3.5.1 Union

Definition 3.9

Let A, B be two sets. The union of A and B is denoted by $A \cup B$. Which contains those elements that are either in A, or in B, or in both.

$$A \cup B = \{x | x \in A \vee x \in B\}.$$

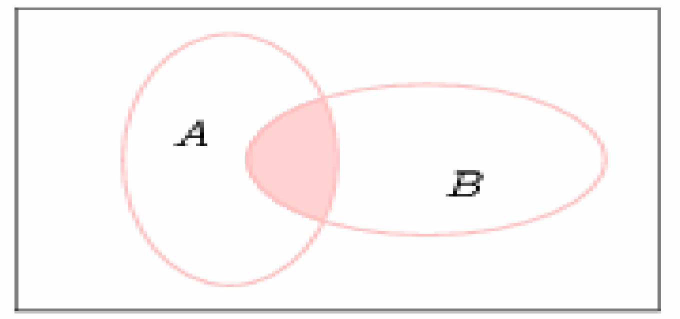


3.5.2 Intersection

Definition 3.10

Let A, B be two sets. The intersection of A and B is denoted by $A \cap B$. Which contains those elements which are in both A and B.

$$A \cap B = \{x | x \in A \wedge x \in B\}.$$



Remark 3.3

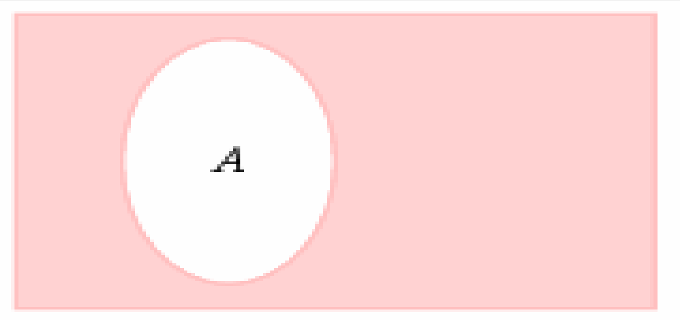
If $A \cap B = \emptyset$, then we say that A and B are disjoint sets.

3.5.3 Complement

Definition 3.11

Let U be the universal set. The complement of a set A is denoted by $\overline{A}$ (or A', $C_U A$, A^c). Which contains all elements of U but are not in A.

$$\overline{A} = \{x | x \in U \wedge x \notin A\}.$$

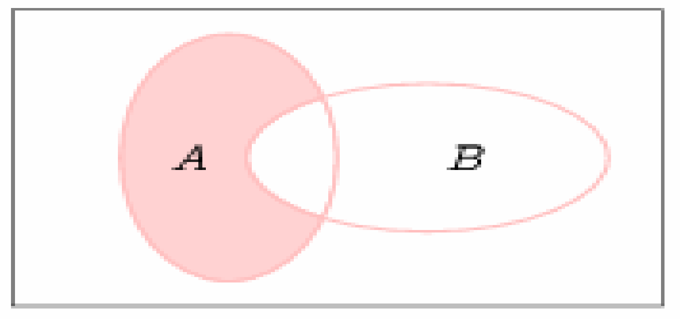


3.5.4 Difference

Definition 3.12

Let A, B be two sets. The difference of A and B is denoted by $A - B$ (or $A \backslash B$). Which contains those elements that are in A but are not in B.

$$A - B = \{x | x \in A \wedge x \notin B\}.$$



Proposition 3.1

We can see that: $A - B$ is the complement of B with respect to A, i.e.:

$$A - B = C_A B.$$

And

$$A - B = \{x | x \in A \wedge x \notin B\} = A \cap \overline{B}.$$

Exercise 3.1

Consider the sets U, A and B which given as:

$$U = \{a, b, c, d, e, f, g, h, i, j, k, l, o, u\},$$

$$A = \{a, b, c, d, e\}, \ B = \{a, e, i, o, u\}.$$

Perform the following operations:

$$A \cup B, \ A \cap B, \ \overline{A}, \ \overline{B}, \ A - B, \ B - A.$$

Solution:

$$A \cup B = \{a, b, c, d, e, i, o, u\}$$

$$A \cap B = \{a, e\}$$

$$\overline{A} = \{f, g, h, i, j, k, l, o, u\}$$

$$\overline{B} = \{b, c, d, f, g, h, j, k, l\}$$

$$A - B = \{b, c, d\}$$

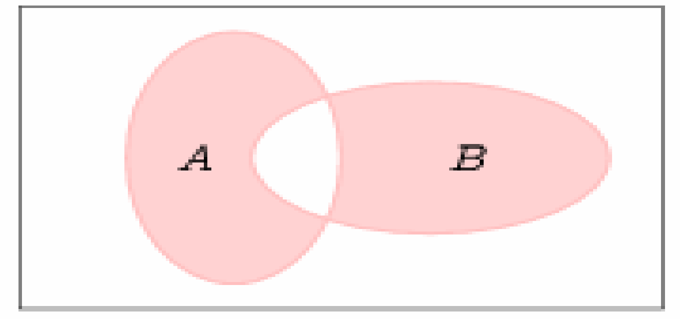
$$B - A = \{i, o, u\}$$

3.5.5 Symmetric difference

Definition 3.13

Let A, B be two sets. The symmetric difference of A and B is denoted by $A \Delta B$. Which contains all elements which are in either of the sets A and B, but not in their intersection.

$$A \Delta B = \{x | x \in A \cup B \wedge x \notin A \cap B\}.$$



Example 3.9

Consider the following sets:

$$A = \{1, 2, 3, 4, 5\}, \ B = \{2, 4, 6\}.$$

The symmetric difference between these sets is:

$$A\Delta B = \{1,3,5,6\}.$$

Proposition 3.2

From the above definition, it is clear that we may express the symmetric difference of A and B as follows:

1. first,
$$A\Delta B = (A\cup B) - (A\cap B).$$
2. second,
$$A\Delta B = (A\cup B)\cap\overline{(A\cap B)}.$$
3. third,
$$A\Delta B = B\Delta A.$$

3.6 Properties of sets operations

Based on the previous definitions of operations sets, we can extract some properties, which can be given as follows: Let A, B and C be three sets, then we have:

Identity laws:

$$A\cap U = A,$$

$$A\cup\emptyset = A.$$

Domination laws:

$$A\cup U = U,$$

$$A\cap\emptyset = \emptyset.$$

Idempotent laws:

$$A\cap A = A,$$

$$A\cup A = A.$$

Complementation laws:

$$A\cup\overline{A} = U,$$

$$A\cap\overline{A} = \emptyset,$$

$$\overline{\overline{A}} = A.$$

Commutative laws:

$$A \cap B = B \cap A,$$

$$A \cup B = B \cup A.$$

Associative laws:

$$(A \cap B) \cap C = A \cap (B \cap C),$$

$$(A \cup B) \cup C = A \cup (B \cup C).$$

Distributive laws:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

De Morgan's laws:

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B},$$

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}.$$

Proof of De Morgan's laws:

It is clear that:

$$\begin{aligned}
\overline{(A \cap B)} &= \{x | x \notin (A \cap B)\}, \\
&= \{x | \neg(x \in (A \cap B))\}, \\
&= \{x | \neg((x \in A) \wedge (x \in B))\}, \\
&= \{x | \neg(x \in A) \vee \neg(x \in B)\}, \\
&= \{x | (x \notin A) \vee (x \notin B)\}, \\
&= \{x | (x \in \overline{A}) \vee (x \in \overline{B})\}, \\
&= \overline{A} \cup \overline{B}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\overline{(A \cup B)} &= \{x | x \notin (A \cup B)\}, \\
&= \{x | \neg(x \in (A \cup B))\}, \\
&= \{x | \neg((x \in A) \vee (x \in B))\}, \\
&= \{x | \neg(x \in A) \wedge \neg(x \in B)\}, \\
&= \{x | (x \notin A) \wedge (x \notin B)\}, \\
&= \{x | (x \in \overline{A}) \wedge (x \in \overline{B})\}, \\
&= \overline{A} \cap \overline{B}.
\end{aligned}$$

Exercise 3.2

Let U be an universal set given by $U = \{1,2,3,4,5,6\}$. If $A = \{1,2\}$, $B = \{2,4,5\}$ and $C = \{1,5,6\}$ then, find the following sets:

1. $A \cup B$, $A \cap B$, $\overline{A}$, $\overline{B}$.
2. Check De Morgan's law by finding $\overline{(A \cup B)}$ and $\overline{A} \cap \overline{B}$.
3. Check the distributive law by finding $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$.

Solution: We have:

$$A \cup B = \{1,2,4,5\}.$$

$$A \cap B = \{2\}.$$

$$\overline{A} = \{3,4,5,6\}.$$

$$\overline{B} = \{1,3,6\}.$$

Now, we can see that

$$\overline{(A \cup B)} = \overline{\{1,2,4,5\}} = \{3,6\},$$

which is the same as

$$\overline{A} \cap \overline{B} = \{3,4,5,6\} \cap \{1,3,6\} = \{3,6\}.$$

Also

$$A \cap (B \cup C) = \{1,2\} \cap \{1,2,4,5,6\} = \{1,2\},$$

which is the same as

$$(A \cap B) \cup (A \cap C) = \{2\} \cup \{1\} = \{1,2\}.$$

Exercise 3.3

Using the properties of set operations, prove that:

$$\overline{A \cup (B \cap C)} = \overline{(A \cup B)} \cup \overline{(A \cup C)}.$$

Solution: We have:

$$\begin{aligned} \overline{A \cup (B \cap C)} &= \overline{(A \cup B) \cap (A \cup C)}, && (\textit{distributive law}),\\ &= \overline{(A \cup B)} \cup \overline{(A \cup C)}, && (\textit{complementation law}). \end{aligned}$$

Proposition 3.3

Using the properties of set operations, we can demontrate that the symmetric difference $A \triangle B$ is given by:

$$A \triangle B = (A - B) \cup (B - A).$$

Proof: *In the exercise series.*

Generalized union

Definition 3.14

For any collection of sets: $A_1, A_2, ..., A_n$. Their union is defined by the set of all elements which belong to at least one of these sets.

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n = \{x | \exists i \in \{1, 2, ..., n\}, x \in A_i\}.$$

Generalized intersection

Definition 3.15

Analogously, their intersection is the set of all elements which belong to all these sets simultaneously.

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap ... \cap A_n = \{x | \forall i \in \{1, 2, ..., n\}, x \in A_i\}.$$

Cardinality and sets operations

Definition 3.16

Let us consider two finite sets A and B. Then, we can see that:

1. If $A \subseteq B$ then
$$n(A) \leq n(B).$$
2. If A and B are disjoint, then
$$n(A \cup B) = n(A) + n(B).$$

Theorem 3.2

For any two finite sets A and B, we have:

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Theorem 3.3

For any three finite sets $A, B,$ and C, we have:

$$n(A \cup B \cup C) \quad = \quad n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(C \cap A) + n(A \cap B \cap C).$$

Proof: *The proof of first theorem in the exercise series.*

Cartesian product

Definition 3.17

The cartesian product of sets A and B is denoted by $A \times B$. Which involves the ordered pairs from A and B.

$$A \times B = \{(x, y) | x \in A \wedge y \in B\}.$$

$$A \times B = \{(x, y) | x \in A, y \in B\}.$$

Example 3.10

Consider $A = \{1, 2, 3\}$ *and* $B = \{H, T\}$*, then:*

$$A \times B = \{(1, H), (1, T), (2, H), (2, T), (3, H), (3, T)\}.$$

Remark 3.4

We point out that the pairs of the cartesian product are ordered. Thus:

$$A \times B \neq B \times A.$$

Proposition 3.4

Let A, B be two finite sets. If $n(A) = m_1$ and $n(B) = m_2$, therefore:

$$n(A \times B) = n(A)n(B) = m_1 m_2.$$

This rule is known by the multiplication principle. It is very useful in counting of elements in sets.

Proof: *Evident.*

Generalized cartesian product

Definition 3.18

Similarly, we can define the cartesian product of a collection of n sets: $A_1, A_2, ..., A_n$ by:

$$A_1 \times A_2 \times ... \times A_n = \{(x_1, x_2, ..., x_n) | x_1 \in A_1, x_2 \in A_2, ... x_n \in A_n\}.$$

The multiplication principle of $A_1 \times A_2 \times ... \times A_n$ is given as:

$$n(A_1 \times A_2 \times ... \times A_n) = n(A_1)n(A_2)...n(A_n).$$

Example 3.11

We mention that $\mathbb{R}^n$, $n \in \mathbb{N}$, *represents an important example of the cartesian product. For example if* $n = 2$*, we have*

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) | x \in \mathbb{R}, y \in \mathbb{R}\}.$$

Here, $\mathbb{R}^2$ *is the set incorporating by all points in the two-dimensional plane.*
Similarly,

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$$

and so on.

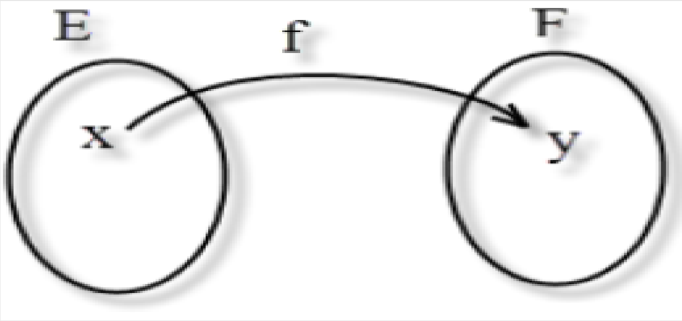
3.7 Applications on sets

In mathematics, applications are widely used to define and describe certain relationships or structures between sets and other mathematical objects.

3.7.1 Functions

Definition 3.19

We say that a relation f from the set E into F is a function, if every $x \in E$ has at most one image y in F. We write $y = f(x)$.



Domain, Codomain and Range

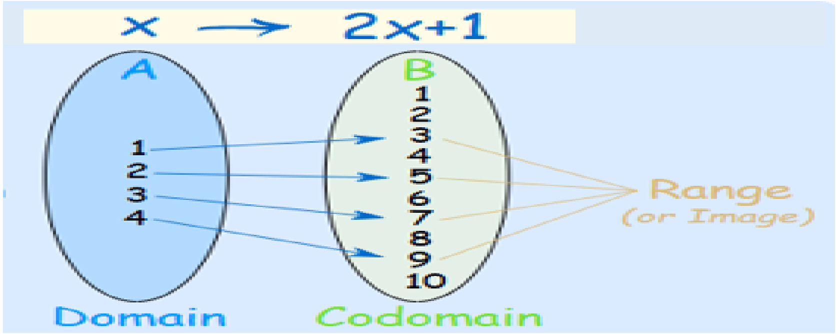
Definition 3.20

There are particular names for: what can go into a function, or what can come out of a function. We describe them as follows:

1. What can go into a function is called: **Domain**.
2. What may possibly come out of a function is called: **Codomain**.
3. What actually comes out of a function is called: **Range**.

Example 3.12

For the described example we have:



Domain: $\{1,2,3,4\}$.

Codomain: $\{1,2,3,4,5,6,7,8,9,10\}$.

Range: $\{3,5,7,9\}$.

The image and preimage

Definition 3.21

Let $f : E \longrightarrow F$ be a function, where A and B are subsets of E and F, respectively.

1. The image of A under f is defined as:

$$f(A)=\{f(x)|x\in A\}.$$

2. The preimage of B under f is defined as:

$$f^{-1}(B)=\{x\in E|f(x)\in B\}.$$

Restriction of a function

Definition 3.22

Let $f : E \longrightarrow F$ be a function. The restriction of f on the subset $A \in E$ is denoted $f|_A$. It is given as:

1. The domain of $f|_A$ is A, i.e., $dom(f|_A)=A$.
2. For any $x\in A$, then $f|_A(x)=f(x)$.

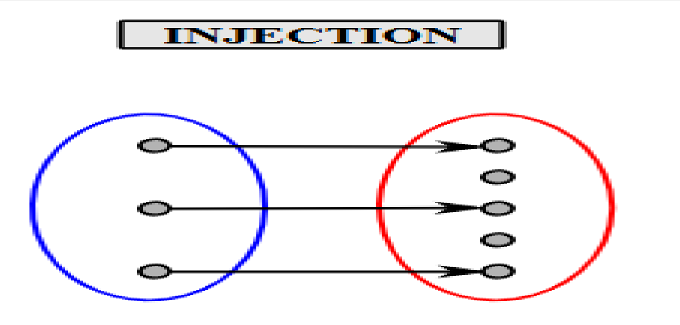
3.7.2 Injection, surjection and bijection

Injection

Definition 3.23

Let E and F be two sets. Consider the function $f : E \longrightarrow F$. We say that f is injective (One-to-One) if: For any element of F, it has at most one preimage in E. This meaning:

$$\forall x_1, x_2 \in E, f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

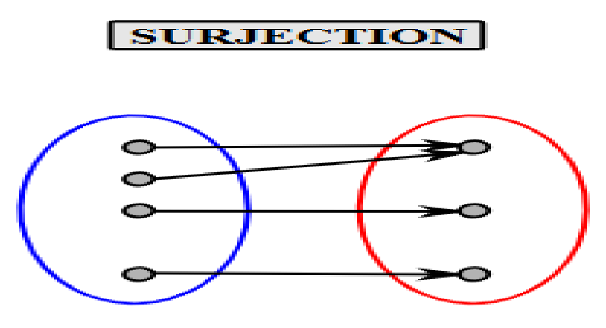


Surjection

Definition 3.24

Let E and F be two sets. Consider the function $f : E \longrightarrow F$. We say that f is surjective (Onto) if: For any element of F, it has at least one preimage in E. This meaning:

$$\forall y \in F, \exists x \in E \quad such\ that \quad f(x) = y.$$

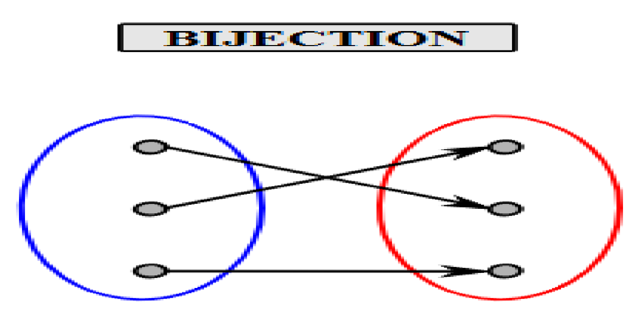


Bijection

Definition 3.25

Let E and F be two sets. Consider the function $f : E \to F$. We say that f is bijective (One-to-One Correspondence) if: f is both injective and surjective. Or: for any element of F, it has exactly one preimage in E. This meaning:

$$\forall y \in F, \exists! x \in E \quad \textit{such that} \quad f(x) = y.$$



Exercise 3.4

Prove that $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = 2x + 3$ is bijective.

Solution: For any $x_1, \ x_2 \in \mathbb{R}$, we have:

$$\begin{aligned} & f(x_1) = f(x_1), \\ \Rightarrow \quad & 2x_1 + 3 = 2x_2 + 3, \\ \Rightarrow \quad & 2x_1 = 2x_2, \\ \Rightarrow \quad & x_1 = x_2, \end{aligned}$$

then, f is injective.

For all $y \in \mathbb{R}$, there exists $x \in \mathbb{R}$, such that:

$$\begin{aligned} & f(x) = y, \\ \Rightarrow \quad & 2x + 3 = y, \\ \Rightarrow \quad & 2x = y - 3, \\ \Rightarrow \quad & x = \frac{y-3}{2}, \end{aligned}$$

hence, f is surjective. So, we conclude that f is bijective.

Exercise 3.5

Prove that $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = x^2$ is not bijective.

Solution: We can see for $x_1 = 2$ and $x_2 = -2$ that:

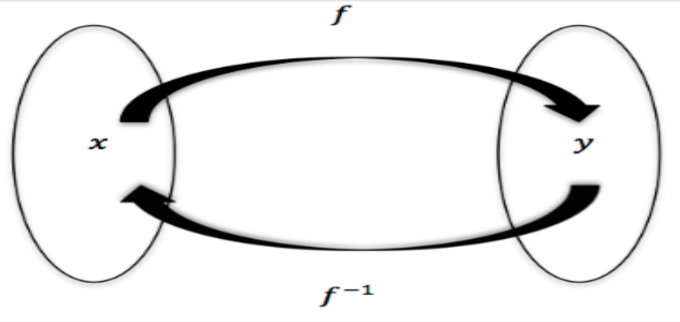
$$\begin{aligned} f(x_1) &= x_1^2 = 2^2 = 4, \\ f(x_2) &= x_2^2 = (-2)^2 = 4, \end{aligned}$$

then $f(x_1) = f(x_2)$, but $x_1 \neq x_2$. Thus, f is not injective, i.e., f is not bijective.

3.7.3 Inverse functions

Definition 3.26

The inverse of a function is denoted by $f^{-1}(x)$ which takes the output values produced by $f(x)$ and converts them back to the input values. The figure given below describes a function and its inverse.



Remark 3.5

1. *If functions $f(x)$ and $g(x)$ are inverses of each other, then:*

$$g(f(x)) = f(g(x)) = x.$$

2. *So,*

$$f^{-1}(f(x)) = f(f^{-1}(x)) = x.$$

3. *A function to have an inverse, the necessary and sufficient condition is: this function must be bijective.*

4. *An inverse of a function is the mirror image of this function when seen through the line $y = x$.*

Proposition 3.5

To find the inverse of a function, we need to follow the following steps:

1. **Step 1:** Substitute $f(x)$ in the given function by y.
2. **Step 2:** Solve for x the newly formed equation.
3. **Step 3:** Switch the positions of x and y.
4. **Step 4:** Substitute the y with notation of inverse function $f^{-1}(x)$.

Exercise 3.6

Determine the inverse of the following functions:

1. $f(x) = 6x + 10,\ D_f = \mathbb{R}$.
2. $f(x) = \frac{x+4}{2x+1},\ D_f = \mathbb{R}\backslash\{-\frac{1}{2}\}$.
3. $f(x) = \ln(x) + 5,\ D_f = \mathbb{R}_+^*$.

Solution:

Inverse of function $n^o 1$. We have:

$$\begin{aligned} & f(x) = y, \\ \Rightarrow\ & 6x + 10 = y, \\ \Rightarrow\ & 6x = y - 10, \\ \Rightarrow\ & x = \frac{y-10}{6}. \end{aligned}$$

So, we get: $f^{-1}(x) = \frac{x-10}{6}$, where $D_{f^{-1}} = \mathbb{R}$.

Inverse of function $n^o 2$. We have:

$$\begin{aligned} & f(x) = y, \\ \Rightarrow\ & \frac{x+4}{2x+1} = y, \\ \Rightarrow\ & x + 4 = 2xy + y, \\ \Rightarrow\ & x - 2xy = y - 4, \\ \Rightarrow\ & x(1-2y) = y - 4, \\ \Rightarrow\ & x = \frac{y-4}{1-2y}. \end{aligned}$$

So, we get: $f^{-1}(x) = \frac{x-4}{1-2x}$, where $D_{f^{-1}} = \mathbb{R}\backslash\{\frac{1}{2}\}$.

Inverse of function $n^o 3$. We have:

$$\begin{aligned} & f(x) = y, \\ \Rightarrow\ & \ln(x) + 5 = y, \\ \Rightarrow\ & \ln(x) = y - 5, \\ \Rightarrow\ & x = e^{y-5}. \end{aligned}$$

So, we get: $f^{-1}(x) = e^{x-5}$, where $D_{f^{-1}} = \mathbb{R}$.

3.8 Exercises

Exercise 3.7

For $n \in \mathbb{N}$, we consider the following sets:

$$A = \{x | x = 6n \wedge x < 41\},\ B = \{x | x = 9n \wedge x < 41\},\ C = \{x | x = 3n \wedge n^2 \leq 51\}.$$

1. Find the Roster form of the previous sets.
2. Determine $A \cup B$, $A \cap B$, $A \cap B \cap C$, $A - B$ and $B - C$.
3. Give the universal set U then find $\overline{A}$, $\overline{B}$ and $\overline{C}$.
4. Find $A \triangle C$ by using two different methods.

Exercise 3.8

We say that S is a convex set if: $\forall x, y \in S, \forall \theta \in [0,1], \theta x + (1-\theta) y \in S$.

1. Give the geometric representation of S, and two examples for a convex and non-convex sets.
2. Prove that: when S_1 and S_2 are two convex sets, then $S_1 \cap S_2$ is also a convex set.

Exercise 3.9

Use the properties of sets' operations to prove that:

1. $A \triangle B = (A - B) \cup (B - A)$.
2. $\overline{A \triangle B} = \overline{A} \triangle B = A \triangle \overline{B}$.
3. $\overline{(A \cap \overline{B}) \cup (\overline{A} \cap B)} = (A \cap B) \cup (\overline{A} \cap \overline{B})$.
4. $(A \cap B) \cup (A \cap C \cap D) \cup (\overline{B} \cap D) = (A \cap B) \cup (\overline{B} \cap D)$.

Exercise 3.10

Let A, B be finite non disjoint sets. In order to find the formula of $n(A\cup B)$, we follow the steps:

1. Rewrite the union $A\cup B$ as union of three disjoint sets.
2. Rewrite the set A and B as union of two disjoint sets, respectively.
3. Calculate $n(A\cup B)$, $n(A)$ and $n(B)$ from the previous obtained expressions.
4. Conclude that $n(A\cup B)=n(A)+n(B)-n(A\cap B)$.

Exercise 3.11

Consider the following function $f:\mathbb{R}\to\mathbb{R}$ defined by: $f(x)=\frac{2x}{1+x^2}$.

1. Calculate $f(2)$ and $f(\frac{1}{2})$.
2. Find the solutions of equation $f(x)=2$.
3. Explain why $f(x)$ is not bijective.

Exercise 3.12

Consider the function $g:\mathbb{R}\to\mathbb{R}_+^*$ defined by: $g(x)=\frac{e^x+2}{e^{-x}}$.

1. Prove that g is bijective.
2. Find its inverse g^{-1}.

3.9 Solutions

Solution of exercise 3.7:

1. Determine the Roster Form of sets A, B and C.

We have:

$$A=\{x|x=6n\wedge x<41\},\quad \textit{then,}\quad A=\{0,6,12,18,24,30,36\}.$$

And

$$B=\{x|x=9n\wedge x<41\},\quad \textit{then,}\quad B=\{0,9,18,27,36\}.$$

And

$$C=\{x|x=3n\wedge n^2\leq 51\}:=\{x|x=3n\wedge n\leq 7\},\quad \textit{then,}\quad C=\{0,3,6,9,12,15,18,21\}.$$

2. Find the given operations sets:

$$A\cup B=\{0,6,9,12,18,24,27,30,36\},$$

$$A \cap B = \{0,\ 18,\ 36\},$$

$$A \cap B \cap C = \{0,\ 18\},$$

$$A - B = \{6,\ 12,\ 24,\ 30\},$$

$$B - C = \{27,\ 36\}.$$

3. The universal set U is given by:

$$U := A \cup B \cup C = \{0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27,\ 30,\ 36\},$$

then,

$$\overline{A} = \{3,\ 9,\ 15,\ 21,\ 27\},$$

$$\overline{B} = \{3,\ 6,\ 12,\ 15,\ 21,\ 24,\ 30\},$$

$$\overline{C} = \{24,\ 27,\ 30,\ 36\}.$$

4. Find $A \triangle C$ using two different methods:

Method 1: We have:

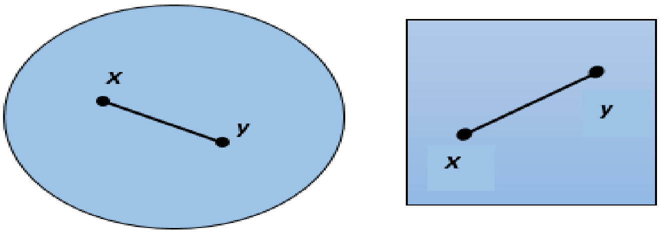
$$\begin{aligned} A \triangle C &= (A - C) \cup (C - A), \\ &= \{24,\ 30,\ 36\} \cup \{3,\ 9,\ 15,\ 21\}, \\ &= \{3,\ 9,\ 15,\ 21,\ 24,\ 30,\ 36\}. \end{aligned}$$

Method 2: We have:

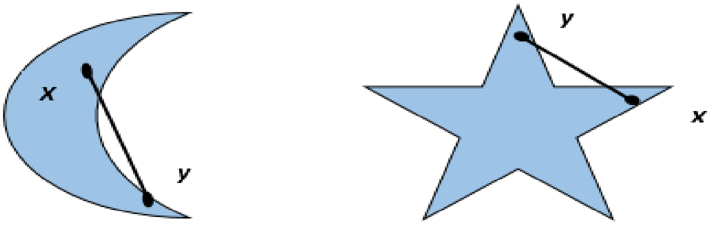
$$\begin{aligned} A \triangle C &= (A \cup C) - (A \cap C), \\ &= \{0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 30,\ 36\} - \{0,\ 6,\ 12,\ 18\}, \\ &= \{3,\ 9,\ 15,\ 21,\ 24,\ 30,\ 36\}. \end{aligned}$$

Solution of exercise 3.8:

1. The mathematical definition of a convex set S, is: $\forall x,\ y \in S, \forall \theta \in [0,1],\ \theta x + (1-\theta) y \in S$. Geometrically, we say that S is convex set, when for any two points x and y within the set, then the line segment connecting them $[x, y]$ is also contained within the set. For example, the **disc** and **square** are convex sets, also the **crescent** and **star** shapes are non convex sets.



Convex sets



Non Convex sets

2. Prove that $S_1 \cap S_2$ is convex set.

By the definition of intersection's set, we have:

$$\forall x,\, y \in S_1 \cap S_2, \quad then \quad x,\, y \in S_1 \quad and \quad x,\, y \in S_2.$$

Like S_1 and S_2 are two convex sets, we get:

$$\begin{cases} \forall x,\, y \in S_1, \forall \theta \in [0,1], \theta x + (1-\theta) y \in S_1, \\ \qquad\qquad\qquad\qquad \wedge \\ \forall x,\, y \in S_2, \forall \theta \in [0,1], \theta x + (1-\theta) y \in S_2, \end{cases}$$

like,

$$\theta x + (1-\theta) y \in S_1 \quad and \quad \theta x + (1-\theta) y \in S_2, \quad then \quad \theta x + (1-\theta) y \in S_1 \cap S_2,$$

which confirm that $S_1 \cap S_2$ is convex set.

Solution of exercise 3.9:

1. Prove that: $A \triangle B = (A - B) \cup (B - A)$.

We have:

$$\begin{aligned}
A\triangle B &= (A\cup B)-(A\cap B), \quad (\textit{by definition}),\\
&= (A\cup B)\cap\overline{(A\cap B)}, \quad (\textit{by definition}),\\
&= (A\cup B)\cap(\overline{A}\cup\overline{B}), \quad (\textit{due to De Morgan's law}),\\
&= ((A\cup B)\cap\overline{A})\cup((A\cup B)\cap\overline{B}), \quad (\textit{due to distributive law}),\\
&= ((A\cap\overline{A})\cup(B\cap\overline{A}))\cup((A\cap\overline{B})\cup(B\cap\overline{B})), \quad (\textit{due to distributive law}),\\
&= (\emptyset\cup(B\cap\overline{A}))\cup((A\cap\overline{B})\cup\emptyset), \quad (\textit{due to complementation law}),\\
&= (B\cap\overline{A})\cup(A\cap\overline{B}), \quad (\textit{due to identity law}),\\
&= (A\cap\overline{B})\cup(B\cap\overline{A}), \quad (\textit{due to commutative law}),\\
&= (A-B)\cup(B-A), \quad (\textit{by definition}).
\end{aligned}$$

2. Prove that: $\overline{A\triangle B}=\overline{A}\triangle B=A\triangle\overline{B}$.

We have:

$$\begin{aligned}
\overline{A\triangle B} &= \overline{(A-B)\cup(B-A)}, \quad (\textit{due to question 1}),\\
&= \overline{(A\cap\overline{B})\cup(B\cap\overline{A})}, \quad (\textit{by definition}),\\
&= (\overline{A}\cup B)\cap\overline{(B\cap\overline{A})}, \quad (\textit{due to De Morgan's law}),\\
&= (\overline{A}\cup B)\cap\overline{(\overline{A}\cap B)}, \quad (\textit{due to commutative law}),\\
&= (\overline{A}\cup B)-(\overline{A}\cap B), \quad (\textit{by definition}),\\
&= \overline{A}\triangle B, \quad (\textit{by definition}),
\end{aligned}$$

so,

$$\overline{A\triangle B}=\overline{A}\triangle B.$$

Similarly, we get:

$$\begin{aligned}
\overline{A\triangle B} &= \overline{(A-B)\cup(B-A)}, \quad (\textit{due to question 1}),\\
&= \overline{(A\cap\overline{B})\cup(B\cap\overline{A})}, \quad (\textit{by definition}),\\
&= \overline{(A\cap\overline{B})}\cap(\overline{B}\cup A), \quad (\textit{due to De Morgan's law}),\\
&= (A\cup\overline{B})\cap\overline{(A\cap\overline{B})}, \quad (\textit{due to commutative law}),\\
&= (A\cup\overline{B})-(A\cap\overline{B}), \quad (\textit{by definition}),\\
&= A\triangle\overline{B}, \quad (\textit{by definition}),
\end{aligned}$$

so,

$$\overline{A\triangle B}=A\triangle\overline{B}.$$

3. Prove that: $\overline{(A\cap\overline{B})\cup(\overline{A}\cap B)}=(A\cap B)\cup(\overline{A}\cap\overline{B})$.

$$\begin{aligned}
\overline{(A\cap\overline{B})\cup(\overline{A}\cap B)} &= (\overline{A}\cup B)\cap(A\cup\overline{B}), \quad (\textit{due to De Morgan's law}),\\
&= ((\overline{A}\cup B)\cap A)\cup((\overline{A}\cup B)\cap\overline{B}), \quad (\textit{due to distributive law}),\\
&= ((\overline{A}\cap A)\cup(B\cap A))\cup((\overline{A}\cap\overline{B})\cup(B\cap\overline{B})), \quad (\textit{due to distributive law}),\\
&= (\emptyset\cup(B\cap A))\cup((\overline{A}\cap\overline{B})\cup\emptyset), \quad (\textit{due to complementation law}),\\
&= (B\cap A)\cup(\overline{A}\cap\overline{B}), \quad (\textit{due to identity law}),\\
&= (A\cap B)\cup(\overline{A}\cap\overline{B}), \quad (\textit{due to commutative law}).
\end{aligned}$$

4. Prove that: $(A\cap B)\cup(A\cap C\cap D)\cup(\overline{B}\cap D)=(A\cap B)\cup(\overline{B}\cap D)$.

$$\begin{aligned}
(A\cap B) \quad \cup & \quad (A\cap C\cap D)\cup(\overline{B}\cap D)=\\
&= (A\cap B)\cup((A\cap C\cap D)\cap U)\cup(\overline{B}\cap D), \quad (\textit{due to identity law}),\\
&= (A\cap B)\cup((A\cap C\cap D)\cap(B\cup\overline{B}))\cup(\overline{B}\cap D), \quad (\textit{due to complementation law}),\\
&= (A\cap B)\cup(A\cap C\cap D\cap B)\cup(A\cap C\cap D\cap\overline{B})\cup(\overline{B}\cap D), \quad (\textit{due to distributive law}),\\
&= ((A\cap B)\cup(A\cap C\cap D\cap B))\cup((A\cap C\cap D\cap\overline{B})\cup(\overline{B}\cap D)), \quad (\textit{due to associative law}),\\
&= ((A\cap B\cap U)\cup(A\cap C\cap D\cap B))\cup((A\cap C\cap D\cap\overline{B})\cup(\overline{B}\cap D\cap U)), \quad (\textit{due to identity law}),\\
&= ((A\cap B)\cap(U\cup(C\cap D)))\cup((\overline{B}\cap D)\cap(U\cup(A\cap C))), \quad (\textit{due to anti-distributive law}),\\
&= ((A\cap B)\cap U)\cup((\overline{B}\cap D)\cap U), \quad (\textit{due to domination law}),\\
&= (A\cap B)\cup(\overline{B}\cap D), \quad (\textit{due to identity law}).
\end{aligned}$$

Solution of exercise 3.10:

1. Clearly, we can rewrite the union $A\cup B$ as union of three disjoint sets as:

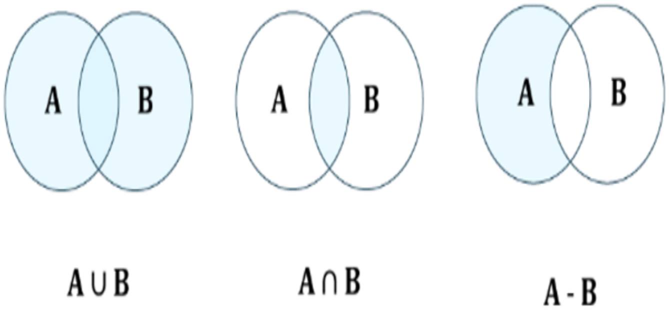
$$A\cup B=(A-B)\cup(A\cap B)\cup(B-A).$$

2. We can represent A as union of two disjoint sets as:

$$A=(A-B)\cup(A\cap B).$$

And B also can be represented as union of two disjoint sets as:

$$B=(B-A)\cup(A\cap B).$$



3. Based on previous obtained expressions in questions 1 and 2, we obtain directly that:

$$n(A\cup B)=n((A-B)\cup(A\cap B)\cup(B-A))=n(A-B)+n(A\cap B)+n(B-A),$$

$$n(A)=n((A-B)\cup(A\cap B))=n(A-B)+n(A\cap B),$$

$$n(B)=n((B-A)\cup(A\cap B))=n(B-A)+n(A\cap B).$$

4. Prove that $n(A\cup B)=n(A)+n(B)-n(A\cap B)$.

From the last two equalities we get:

$$\begin{cases} n(A-B)=n(A)-n(A\cap B), \\ n(B-A)=n(B)-n(A\cap B), \end{cases}$$

by subsisting them in the formula of $n(A\cup B)$ we obtain:

$$\begin{aligned} n(A\cup B) &= n(A-B)+n(A\cap B)+n(B-A), \\ &= n(A)-n(A\cap B)+n(A\cap B)+n(B)-n(A\cap B), \\ &= n(A)+n(B)-n(A\cap B). \end{aligned}$$

Solution of exercise 3.11:

1. Calculate $f(2)$ and $f\left(\frac{1}{2}\right)$:

$$f(2)=\frac{2\times 2}{1+2^2}=\frac{4}{5}, \qquad f\left(\frac{1}{2}\right)=\frac{2\times\frac{1}{2}}{1+(\frac{1}{2})^2}=\frac{1}{1+\frac{1}{4}}=\frac{4}{5}.$$

2. Find solutions of equation $f(x)=2$:

$$f(x)=2\Rightarrow\frac{2x}{1+x^2}=2\Rightarrow 2+2x^2=2x\Rightarrow 2x^2-2x+2=0\Rightarrow x^2-x+1=0,$$

by using $\Delta=1^2-4\times1\times1=-3<0$, thus equation $f(x)=2$ has no solutions in $\mathbb{R}$.

3. Why $f(x)$ is not bijective?

From question 1, there exist $x_1=2$ and $x_2=\frac{1}{2}$, where $f(x_1)=f(x_2)=\frac{4}{5}$ but $x_1\neq x_2$. Which means that f is not injective.

From question 2, there exists $y = 2 \in \mathbb{R}$, for which there not exists $x \in \mathbb{R}$ satisfy $f(x) = 2$. Which means that f is not surjective.

Consequently, $f(x)$ is not bijective.

Solution of exercise 3.12:

Consider the function $g : \mathbb{R} \to \mathbb{R}_+^*$ defined by: $g(x) = \frac{e^x+2}{e^{-x}}$.

1. To prove that g is bijective, we need to verify that g is injective and surjective. But in this time, we will use the following definition:

$$\forall y \in F, \exists!\, x \in E, \quad \textit{such that} \quad g(x) = y.$$

Let $y \in \mathbb{R}_+^*$ then,

$$g(x) = y \Rightarrow \frac{e^x+2}{e^{-x}} = y \Rightarrow e^x + 2 = ye^{-x} \Rightarrow e^{2x} + 2e^x - y = 0.$$

To solve this equation we use the new variable $e^x = w$, thus:

$$w^2 + 2w - y = 0,$$

by using $\Delta = 2^2 - 4 \times 1 \times (-y) = 4 + 4y > 0$ (because $y > 0$), then we have two solutions in $\mathbb{R}$ given by:

$$\begin{cases} w_1 = \frac{-2+\sqrt{4+4y}}{2} = -1 + \sqrt{1+y}, \\ w_2 = \frac{-2-\sqrt{4+4y}}{2} = -1 - \sqrt{1+y}. \end{cases}$$

On the other hand, like $w > 0$, so we cannot accept the second solution w_2. Which leads that equation has one solution w_1. Therefore,

$$\begin{aligned} & w_1 = -1 + \sqrt{1+y}, \\ \Rightarrow \quad & e^x = -1 + \sqrt{1+y}, \\ \Rightarrow \quad & x = \ln(-1 + \sqrt{1+y}). \end{aligned}$$

Consequently,

$$\forall y \in \mathbb{R}_+^*, \exists!\, x = \ln(-1 + \sqrt{1+y}) \in \mathbb{R}, \quad \textit{such that} \quad g(x) = y.$$

So, we conclude that g is bijective.

2. Find the inverse g^{-1}:

It's clear that:

$$\textit{when} \quad g(x) = y \quad \textit{then} \quad x = \ln(-1 + \sqrt{1+y}).$$

So, we obtain:

$$g^{-1}(x) = \ln(-1 + \sqrt{1+x}), \quad \textit{where} \quad D_{g^{-1}} = \mathbb{R}_+^*.$$

4

Propositional logic

Propositional logic is a branch in mathematics. Is also known by the propositional calculus. This branch studies the relationships between propositions, which are defined via logical connectives. Propositional logic has a useful applications in a variety of domains such as: logic gates, game strategies, computer science, workflow problems, electrical systems, etc. In this chapter, we will going to discuss the following points:

1. Propositional logic.
2. Truth tables.
3. Propositional logic and applications.

4.1 What is a proposition?

Definition 4.1

In propositional logic, propositions are statements that can be evaluated as true or false.

Example 4.1

We provide some examples of propositions by:

1. *Thales was a human.*
2. *It is raining today.*
3. $9+1=10$.
4. $9+11=7$.

Example 4.2

The following expressions are not propositions:

1. *Let's go!.*
2. *What time is it?*
3. $x+2=3$.
4. $y=x^2-1$.

Remark 4.1

In propositional logic, any proposition can be represented by a capital letter $(A, B, C, ...)$*, or by small alphabets* $(p, q, r, s, t, ...)$.

Example 4.3

For constructing propositions, we use a propositional variables as follows:

1. $p :=$ ***The moon is shining***.
2. $q :=$ ***The sun sets in the west***.
3. $A :=$ ***Blood is red***.
4. $B := 8+1=3\times 3$.

Definition 4.2

Any proposition is designated by a truth value, of either true or false. We denote these truth values by:

1. True may be denoted by the letter "T".
2. False may be denoted by the letter "F".

In areas of computer logic gates, these values are given by the following binary representations:

1. True may be denoted by the number "1".
2. False may be denoted by the number "0".

4.2 Truth tables

Definition 4.3

Truth table of a logical proposition is a mathematical table used to know the functional values of this expression for all possible input variables. This table helps us to analyze statements, clarify propositions, and represent a way for visualizing the truth or falsity of them.

4.3 Logic connectives

Definition 4.4

In propositional logic, the relationships between propositional variables, are introduced by connectives. We have 5 main connectives, outlined in the following table:

Connectives	Symbols	Interpretations
Negation	$\neg$	Not
Conjunction	$\wedge$	And
Disjunction	$\vee$	Or
Conditional	$\longrightarrow$	If ...then
Biconditional	$\longleftrightarrow$	If and only if

Each connective has a corresponding description, as we will see.

4.3.1 Negation

Definition 4.5

Negation is an unary logical connective. For the proposition P, the negation of P is denoted by $\neg P$ or $\overline{P}$. It evaluates as false if P is true, and true if P is false. Truth table of the negation is defined as:

P	$\neg P$
1	0
0	1

Example 4.4

We have:

1. *For* $p :=$ ***The moon is shining****. Then,* $\neg p :=$ ***The moon is not shining****.*
2. *For* $q := 2+2=5$*. Then,* $\neg q := 2+2\neq 5$*.*

4.3.2 Conjunction

Definition 4.6

Conjunction is a binary logical connective. The conjunction for a given propositions P and Q is denoted by $P \wedge Q$. It evaluates as true only if both propositions P and Q are true. Truth table of the conjunction is defined as:

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

Example 4.5

When we have:

$p :=$ ***Today is Sunday.***

$q :=$ ***Today it is raining.***

Then,

$p \wedge q :=$ ***Today is Sunday and it is raining.***

4.3.3 Disjunction

Definition 4.7

Disjunction is a binary logical connective. The disjunction for a given propositions P and Q is denoted by $P \vee Q$. It evaluates as true if either of the propositions P or Q are true. Truth table of the disjunction is defined as:

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

Example 4.6

When we have:

$p :=$ ***You can have a cookie.***

$q :=$ ***You can have a piece of cake.***

Then,

$p \vee q :=$ ***You can have a cookie or a piece of cake.***

4.3.4 Conditional (Implication)

Definition 4.8

The conditional connective is equivalent to the expression: ***If*** P ***then*** Q. Implication of propositions P and Q is denoted by $P \longrightarrow Q$. Here, P is called the hypothesis or antecedent and Q is called the conclusion or consequence. The conditional is only false if P is true and Q is false, otherwise it is true. Truth table of the conditional is defined as:

P	Q	$P \longrightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Example 4.7

When we have:

$p :=$ ***Amina finishes her homework.***

$q :=$ ***Amina watches TV.***

Then,

$p \longrightarrow q :=$ ***If Amina finishes her homework, then she can watch TV.***

Remark 4.2

There are many equivalent strategies for reasoning to the conditional $p \longrightarrow q$*:*

1. p *implies* q.
2. q *when* p.
3. q *follows from* p.
4. p *is sufficient for* q.
5. q *is necessary for* p.

4.3.5 Biconditional (Double Implication, Bi-implication)

Definition 4.9

Biconditional is a connective that represents the condition: ***If and only if.*** Biconditional of propositions P and Q is denoted by $P \longleftrightarrow Q$. It evaluates as true if P and Q have same truth values, and false otherwise. Truth table of the Biconditional is defined as:

P	Q	$P \longleftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Example 4.8

When we have:

$p :=$ ***We will cancel the picnic.***

$q :=$ ***It rains.***

Then,

$p \longleftrightarrow q :=$ ***We will cancel the picnic if and only if it rains.***

Remark 4.3

The biconditional $p \longleftrightarrow q$ can be described by many ways, like:

1. *p iff q.*
2. *if p then q, and if q then p.*
3. *p is necessary and sufficient for q.*

Summary

In summary, a truth table showing the functionality of all connectives:

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \longrightarrow Q$	$P \longleftrightarrow Q$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Priority of logical connectives

Proposition 4.1

The previous connectives are applied in the following order:

1. **Negation:** $\neg$,
2. **Conjunction:** $\wedge$,
3. **Disjunction:** $\vee$,
4. **Implication:** $\longrightarrow$,
5. **Bi-implication:** $\longleftrightarrow$.

This order must be used in expressions does not have a brackets.

Example 4.9

We can see that:

1. *The expression:* $\neg p \vee q$ *must be clarified as:* $(\neg p) \vee q$.
2. *The expression:* $p \vee q \wedge r$ *must be clarified as:* $p \vee (q \wedge r)$.
3. *The expression:* $p \longrightarrow q \longleftrightarrow r$ *must be clarified as:* $(p \longrightarrow q) \longleftrightarrow r$.

Exercise 4.1

Let p, q and r be propositional variables. Determine the truth tables of the formulas:

1. $(p \wedge q) \vee r$.
2. $(p \wedge r) \longrightarrow (q \vee \neg r)$.

Solutions:

First formula:

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$
1	1	1	1	1
1	1	0	1	1
1	0	1	0	1
1	0	0	0	0
0	1	1	0	1
0	1	0	0	0
0	0	1	0	1
0	0	0	0	0

Second formula:

p	q	r	$p \wedge r$	$\neg r$	$q \vee \neg r$	$(p \wedge r) \to (q \vee \neg r)$
1	1	1	1	0	1	1
1	1	0	0	1	1	1
1	0	1	1	0	0	0
1	0	0	0	1	1	1
0	1	1	0	0	1	1
0	1	0	0	1	1	1
0	0	1	0	0	0	1
0	0	0	0	1	1	1

Inverse, Converse, and Contrapositive of implication

Definition 4.10

Consider the propositional formula $p \to q$. Then, we have:

1. Converse: $q \to p$.
2. Inverse: $\neg p \to \neg q$.
3. Contrapositive: $\neg q \to \neg p$.

Example 4.10

Consider the conditional statement:

If he does his homework, he will not be punished.

Here, ***he does his homework*** *is the hypothesis p, and* ***he will not be punished*** *is the conclusion q. Then,*

1. *The Inverse $\neg p \to \neg q$ is:*

   If he does not do his homework, he will be punished.

2. *Converse $q \to p$ is:*

   If he will not be punished, he does his homework.

3. *Contrapositive $\neg q \to \neg p$ is:*

   If he is punished, he did not do his homework.

4.4 Tautologies, Contradictions and Contingency

4.4.1 Tautologies

Definition 4.11

Tautology is a formula which evaluates as true for all value of its propositional variables. The tautology can be denoted by $\mathbb{1}$ or T.

Example 4.11

It is clear that $((A \to B)\wedge A) \to B$ *is a tautology, from its truth table:*

A	B	$(A \to B)$	$((A \to B)\wedge A)$	$((A \to B)\wedge A) \to B$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

4.4.2 Contradictions

Definition 4.12

Contradiction is a formula which evaluates as false for all value of its propositional variables. The contradiction can be denoted by 0 or F.

Example 4.12

Prove that $(A \vee B)\wedge((\neg A)\wedge(\neg B))$ *is a contradiction.*

The truth table of this formula is given by:

A	B	$A \vee B$	$\neg A$	$\neg B$	$(\neg A)\wedge(\neg B)$	$(A \vee B)\wedge((\neg A)\wedge(\neg B))$
1	1	1	0	0	0	0
1	0	1	0	1	0	0
0	1	1	1	0	0	0
0	0	0	1	1	1	0

So, we confirm that is a contradiction.

4.4.3 Contingency

Definition 4.13

Contingency is a formula which evaluates as both true and false, according to values of its propositional variables.

Example 4.13

We can show that $(A \vee B) \wedge (\neg A)$ *is a contingency via its truth table:*

A	B	$A \vee B$	$\neg A$	$(A \vee B) \wedge (\neg A)$
1	1	1	0	0
1	0	1	0	0
0	1	1	1	1
0	0	0	1	0

4.5 Propositional equivalences

Theorem 4.1

We say that formulas A and B are logically equivalent if: $A \longleftrightarrow B$ is a tautology. And, we write $A \Longleftrightarrow B$ or $A \equiv B$.

Proof: *Evident.*

Remark 4.4

To determine if two expressions A *and* B *are logically equivalent, we need to verify that their two columns in a truth table are identical.*

Lemma 4.1

The conditional connective $p \longrightarrow q$ is equivalent to $\neg p \vee q$.

Proof: *Test by matching of truth tables.*

p	q	$p \longrightarrow q$	$\neg p$	$\neg p \vee q$
1	1	1	0	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

So,

$$p \longrightarrow q \equiv \neg p \vee q.$$

Lemma 4.2

The Bi-Conditional connective $p \longleftrightarrow q$ is equivalent to $(p \longrightarrow q) \wedge (q \longrightarrow p)$.

Proof: *Test by matching of truth tables.*

p	q	$p \longleftrightarrow q$	$p \longrightarrow q$	$q \longrightarrow p$	$(p \longrightarrow q) \wedge (q \longrightarrow p)$
1	1	1	1	1	1
1	0	0	0	1	0
0	1	0	1	0	0
0	0	1	1	1	1

So,

$$p \longleftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p).$$

Lemma 4.3

There are several interesting logical equivalences contain one, two or more propositional variables, which would be good to memorize. Going to list them one by one and verify them using the truth tables.

Identity laws:

$$p \wedge T \equiv p, \qquad p \vee F \equiv p.$$

Verification through truth table:

p	T	$p \wedge T$
1	1	1
0	1	0

p	F	$p \vee F$
1	0	1
0	0	0

Domination laws:

$$p \wedge F \equiv F, \qquad p \vee T \equiv T.$$

Verification through truth table:

p	F	$p \wedge F$
1	0	0
0	0	0

p	T	$p \vee T$
1	1	1
0	1	1

Idempotent laws:

$$p \wedge p \equiv p, \qquad p \vee p \equiv p.$$

Verification through truth table:

p	p	$p \wedge p$
1	1	1
0	0	0

p	p	$p \vee p$
1	1	1
0	0	0

Complementation laws:

$$p \wedge \neg p \equiv F, \qquad p \vee \neg p \equiv T.$$

Verification through truth table:

p	$\neg p$	$p\wedge\neg p$	F
1	0	0	0
0	1	0	0

p	$\neg p$	$p\vee\neg p$	T
1	0	1	1
0	1	1	1

Double negation:

$$\neg(\neg p)\equiv p.$$

Verification through truth table:

p	$\neg p$	$\neg(\neg p)$
1	0	1
0	1	0

Commutativity:

$$p\wedge q\equiv q\wedge p,\qquad p\vee q\equiv q\vee p.$$

Verification through truth table:

p	q	$p\wedge q$	$q\wedge p$
1	1	1	1
1	0	0	0
0	1	0	0
0	0	0	0

p	q	$p\vee q$	$q\vee p$
1	1	1	1
1	0	1	1
0	1	1	1
0	0	0	0

Associativity:

$$(p\wedge q)\wedge r\equiv p\wedge(q\wedge r),\qquad (p\vee q)\vee r\equiv p\vee(q\vee r).$$

Verification through truth table:

p	q	r	$p\wedge q$	$(p\wedge q)\wedge r$	$q\wedge r$	$p\wedge(q\wedge r)$
1	1	1	1	1	1	1
1	1	0	1	0	0	0
1	0	1	0	0	0	0
1	0	0	0	0	0	0
0	1	1	0	0	1	0
0	1	0	0	0	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$q \vee r$	$p \vee (q \vee r)$
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	1	1	1
1	0	0	1	1	0	1
0	1	1	1	1	1	1
0	1	0	1	1	1	1
0	0	1	0	1	1	1
0	0	0	0	0	0	0

Distributivity:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r), \quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r).$$

Verification through truth table:

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

Absorption:

$$p \wedge (p \vee q) \equiv p, \qquad p \vee (p \wedge q) \equiv p.$$

Verification through truth table:

p	q	$p \vee q$	$p \wedge (p \vee q)$
1	1	1	1
1	0	1	1
0	1	1	0
0	0	0	0

p	q	$p \wedge q$	$p \vee (p \wedge q)$
1	1	1	1
1	0	0	1
0	1	0	0
0	0	0	0

De Morgan's laws:

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

Verification through truth table:

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

Equivalence proof

Proposition 4.2

To prove that two expressions A and B are logically equivalent, we can build a sequence of logically equivalent steps involving laws and properties, which begins by A and terminus with B.

Example 4.14

We can prove the equivalence:

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

according to the following steps:

$$\begin{aligned} p \wedge (\neg p \vee q) &\equiv (p \wedge \neg p) \vee (p \wedge \neg q), \quad (\textit{due to distributivity law}),\\ &\equiv F \vee (p \wedge \neg q), \quad (\textit{due to complementation law}),\\ &\equiv p \wedge \neg q, \quad (\textit{due to identity law}). \end{aligned}$$

Exercise 4.2

Prove that:

$$p \to ((q \to r) \to p) \equiv T,$$

then test it by using truth table.

Solution: We have:

$$\begin{aligned}
p \longrightarrow ((q \longrightarrow r) \longrightarrow p) &\equiv \neg p \vee (\neg(\neg q \vee r) \vee p), \quad (\textit{due to conditional law}),\\
&\equiv \neg p \vee ((q \wedge \neg r) \vee p), \quad (\textit{due to De Morgan's law}),\\
&\equiv (q \wedge \neg r) \vee (\neg p \vee p), \quad (\textit{due to associativity law}),\\
&\equiv (q \wedge \neg r) \vee T, \quad (\textit{due to complementation law}),\\
&\equiv T, \quad (\textit{due to domination law}).
\end{aligned}$$

Test it by using truth table.

p	q	r	$q \longrightarrow r$	$(q \longrightarrow r) \longrightarrow p$	$p \longrightarrow ((q \longrightarrow r) \longrightarrow p)$	T
1	1	1	1	1	1	1
1	1	0	0	1	1	1
1	0	1	1	1	1	1
1	0	0	1	1	1	1
0	1	1	1	0	1	1
0	1	0	0	1	1	1
0	0	1	1	0	1	1
0	0	0	1	0	1	1

4.6 Normal forms

Definition 4.14

In propositional logic, any logical expressions can be rewritten in particular formats using specific connectives, these formats are called normal forms. There are two normal form:

1. Conjunctive normal form.
2. Disjunctive normal form.

Normal forms make the logical expressions easier to analyze and manipulate.

In this section we go to discuss them in details.

4.6.1 Complete connectives system

Definition 4.15

A set Γ of connectives is said complete, when for all logical formulas, we can find an equivalent formulas for them, defined using only the elements of Γ.

Theorem 4.2

The following sets of connectives:

$$\Gamma_1 = \{\neg, \vee\}, \; \Gamma_2 = \{\neg, \wedge\},$$

are complete.

Proof: The first set Γ_1***:***

Let p *and* q *be two logical variables, it's clear that connectives' space is designed to:*

$$\neg, \; \vee, \; \wedge, \; \longrightarrow, \; \longleftrightarrow.$$

So, for the two connectives $\neg$ *and* $\vee$*, we don't have a problem, because they are included in* Γ_1*. Now, for* $p \wedge q$*, we can use De Morgan's law to get:*

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

For the conditional connective $p \longrightarrow q$*, we use directly its equivalence formula which given in Lemma 4.1:*

$$p \longrightarrow q \equiv \neg p \vee q.$$

Also, for $p \longleftrightarrow q$*, we use Lemma 4.2 to obtain:*

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

Consequently, we have represented all connectives' space using only elements of Γ_1*, which means that it's complete.*

The second set Γ_2***:***

Similarly, the connectives $\neg$ *and* $\wedge$ *belong to* Γ_2*, and for the other connectives, we have:*

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

And,

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

Also,

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

Which conclude that Γ_2 *is a complete set.*

Corollary 4.1

Based on the previous theorem, we conclude that we can represent any logical formula using one of the complete set Γ_1 or Γ_2. This is what leads us to construct the normal forms. As we will show in the next definitions.

4.6.2 Conjunctive normal form

Definition 4.16

We say that expressions are written in conjunctive normal form, when they obtained by operating disjunctive $\vee$ among their variables and connected with conjunctive $\wedge$.

Example 4.15

These expressions are in conjunctive normal form:

$$(p \vee q) \wedge (\neg p \vee \neg r),$$

$$(p \vee q) \wedge (p \vee r) \wedge (q \vee r \vee s).$$

4.6.3 Disjunctive normal form

Definition 4.17

We say that expressions are written in disjunctive normal form, when they obtained by operating conjunctive $\wedge$ among their variables and connected with disjunctive $\vee$.

Example 4.16

These expressions are in disjunctive normal form:

$$(p \wedge q) \vee (\neg p \wedge \neg r),$$

$$(p \wedge q) \vee (p \wedge r) \vee (q \wedge r \wedge s).$$

How to find the normal forms?

Definition 4.18

In order to find the conjunctive or disjunctive normal form for a given logical formula, we can use the principle of propositional equivalences.

Example 4.17

We can rewrite the following proposition:

$$A \equiv p \wedge \neg(\neg q \wedge r)$$

in its disjunctive normal form, as follows:

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

Remark 4.5

The previous described method to find the conjunctive or disjunctive normal forms, becomes complicate when we have a long logical expressions which contain many variables. For this reason we can use the truth table for finding them easily.

Finding the normal forms via truth table

Lemma 4.4

Consider a logical expressions A which contain n variables $r_1, r_2, ..., r_n$. To find the disjunctive normal forms for A, we follow the steps:

1. We draw the truth table of expression A.
2. We consider p the number of lines of truth table, in which truth value of A equals 1, $(v(A) = 1)$.
3. For each line i, $1 \leq i \leq p$, we define the conjunctive monomial M_i by:

$$M_i = \bigwedge_{k=1}^{n} m_{ik}, \quad \textit{where,} \quad m_{ik} = \begin{cases} r_k, & \textit{if} \quad v(r_k) = 1, \\ \neg r_k, & \textit{if} \quad v(r_k) = 0. \end{cases}$$

4. Disjunctive normal form of A is denoted by $D_{nf}(A)$, it is given by:

$$D_{nf}(A) := \bigvee_{i=1}^{p} M_i.$$

Lemma 4.5

Consider a logical expressions A which contain n variables $r_1, r_2, ..., r_n$. To find the conjunctive normal forms for A, we follow the steps:

1. We draw the truth table of expression A.
2. We consider $\widetilde{p}$ the number of lines of truth table, in which truth value of A equals 0, $(v(A) = 0)$.
3. For each line i, $1 \leq i \leq \widetilde{p}$, we define the conjunctive monomial $\widetilde{M_i}$ by:

$$\widetilde{M_i} = \bigvee_{k=1}^{n} \widetilde{m}_{ik}, \quad \textit{where,} \quad \widetilde{m}_{ik} = \begin{cases} r_k, & \textit{if} \quad v(r_k) = 0, \\ \neg r_k, & \textit{if} \quad v(r_k) = 1. \end{cases}$$

4. Conjunctive normal form of A is denoted by $C_{nf}(A)$, it is given by:

$$C_{nf}(A) := \bigwedge_{i=1}^{\widetilde{p}} \widetilde{M_i}.$$

Exercise 4.3

Consider the following logical statement:

$$A \equiv p \to (q \wedge r).$$

Find the conjunctive and disjunctive normal forms of A.

Solution: First, we draw the truth table of A.

p	q	r	$q\wedge r$	$p\longrightarrow(q\wedge r)$
1	1	1	1	1
1	1	0	0	0
1	0	1	0	0
1	0	0	0	0
0	1	1	1	1
0	1	0	0	1
0	0	1	0	1
0	0	0	0	1

Thus, conjunctive normal forms of A is given by:

$$C_{nf}(A):=(\neg p\vee\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)\wedge(\neg p\vee q\vee r).$$

And disjunctive normal forms of A is given by:

$$D_{nf}(A):=((p\wedge q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge q\wedge\neg r)\vee(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge\neg q\wedge\neg r).$$

Remark 4.6

We can see easily that:

1. $A\equiv C_{nf}(A)\equiv D_{nf}(A)$.
2. *If A is tautology, then $D_{nf}(A)\equiv T$.*
3. *If A is contradiction, then $C_{nf}(A)\equiv F$.*
4. *Disjunctive normal form of tautologies can be represented by:*

$$\begin{aligned}D_{nf}(T) &\equiv (p\wedge q)\vee(p\wedge\neg q)\vee(\neg p\wedge q)\vee(\neg p\wedge\neg q),\\ &\equiv (p\wedge q\wedge r)\vee(p\wedge q\wedge\neg r)....\vee(\neg p\wedge\neg q\wedge\neg r),\\ &\equiv (p\wedge q\wedge r\wedge s)....\vee(\neg p\wedge\neg q\wedge\neg r\wedge\neg s),\\ &\equiv ....\end{aligned}$$

5. *Conjunctive normal form of contradictions can be represented by:*

$$\begin{aligned}C_{nf}(F) &\equiv (\neg p\vee\neg q)\wedge(\neg p\vee q)\wedge(p\vee\neg q)\wedge(p\vee q),\\ &\equiv (\neg p\vee\neg q\vee\neg r)\wedge(\neg p\vee\neg q\vee r)....\wedge(p\vee q\vee r),\\ &\equiv (\neg p\vee\neg q\vee\neg r\vee\neg s)....\wedge(p\vee q\vee r\vee s),\\ &\equiv ....\end{aligned}$$

6. $\neg(D_{nf}(T)):=C_{nf}(F)$.

Duality principle

Definition 4.19

Dual of a statement A is denoted by A^*. Duality principle states to interchange unions into intersections and vice versa.

Example 4.18

The dual of the statement:

$$A := (p \wedge q) \vee r,$$

is

$$A^* := (p \vee q) \wedge r.$$

Remark 4.7

1. *We have:* $(A^*)^* := A$.
2. *If the dual of a statement remains the same statement:* $A^* := A$ *it is said self-dual statement.*

4.7 Propositional calculus via Hilbert systems

4.7.1 Hilbert proof systems

Definition 4.20

The Hilbert proof systems are called Hilbert style formalizations. In 1922, he launched his Proof Theory, which aimed to justify the use of modern methods for mathematical reasoning using formal axiomatic systems.

Hilbert proof systems are based on a language with implication using a set of axioms, a set of logical rules and only Modus Ponens as inference rule, in order to obtain, to demonstrate or for deducing new formulas which are called theorems. As we will show in next parts.

Definition 4.21

A **formal theory** T is introduced by:

1. The alphabet,
2. The formulas of T,
3. The formulas of axioms,
4. The inference rules.

Definition 4.22

A **proof** in formal theory T, is a sequence of formulas: $a_1, a_2, ..., a_n$, which are represent axioms, already demonstrated theorems or obtained from the inference rules.

Definition 4.23

If a formula A admits a proof, we say that A is **provable** or A is a **theorem** and we denote $\vdash A$.

Remark 4.8

If there is a ***proof*** *of a* ***theorem*** *A from a certain set Γ of axioms, elements or formulas, then we write: $\Gamma \vdash A$.*

4.7.2 List of Hilbert-Ackerman axioms

Definition 4.24

Axioms are formulas that are accepted without formally demonstration. Here the list of Hilbert-Ackerman axioms are denoted by $(H.A)$ and given as follows:

$$\begin{array}{ll} (H.A)_1. & (x \vee x) \Rightarrow x, \\ (H.A)_2. & x \Rightarrow (x \vee y), \\ (H.A)_3. & x \vee y \Rightarrow y \vee x, \\ (H.A)_4. & (x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y). \end{array}$$

4.7.3 Inference rule of Modus Ponens

Definition 4.25

Modus Ponens can be considered as the oldest of all known rules of inference. It plays a special role in formal logic. Modus Ponens is denoted by $(M.P)$ and expressed through a conditional syllogism which takes the following form:

$$\begin{array}{l} \vdash A \\ \vdash A \Rightarrow B \\ \hline \vdash B \end{array}$$

This rule can be formulated as follows: let A, B be two formulas, such that A and $A \Rightarrow B$ are **theorems**, then B is a **theorem**.

4.7.4 Substitution rule

Definition 4.26

Let A be a theorem in which the propositional variable x appears. Substitution rule involves replacing variable x within a formula B, where B is not necessarily a theorem. This substitution rule in each of its occurrences generates a theorem, which means that:

$$\textit{if} \quad \vdash A \quad \textit{then} \quad \vdash A(x := B).$$

4.7.5 Proof of some common theorems

Theorem 4.3

Prove that:

$$\vdash \neg x \vee x.$$

Proof: *We demonstrate this theorem via Hilbert systems by the following steps:*

Step	Theorem	Followed rule
(1)	$(x \vee x) \Rightarrow x$	$(H.A)_1$
(2)	$x \Rightarrow x \vee y$	$(H.A)_2$
(3)	$x \Rightarrow x \vee x$	Sub. $y := x$ in (2)
(4)	$(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(5)	$(x \vee x \Rightarrow y) \Rightarrow (z \vee (x \vee x) \Rightarrow z \vee y)$	Sub. $x := x \vee x$ in (4)
(6)	$(x \vee x \Rightarrow x) \Rightarrow (z \vee (x \vee x) \Rightarrow z \vee x)$	Sub. $y := x$ in (5)
(7)	$(z \vee (x \vee x) \Rightarrow z \vee x)$	Modus Ponens (1), (6) $\longrightarrow$ (7)
(8)	$(\neg z \vee (x \vee x) \Rightarrow \neg z \vee x)$	Sub. $z := \neg z$ in (7)
(9)	$(z \Rightarrow (x \vee x) \Rightarrow z \Rightarrow x)$	Definition of $\Rightarrow$
(10)	$(x \Rightarrow (x \vee x) \Rightarrow x \Rightarrow x)$	Sub. $z := x$ in (9)
(11)	$x \Rightarrow x$	Modus Ponens (3), (10) $\longrightarrow$ (11)
(12)	$\neg x \vee x$	Definition of $\Rightarrow$

Theorem 4.4

Prove that:

$$\textit{if} \quad \vdash \alpha \Rightarrow \beta \quad \textit{and} \quad \vdash \beta \Rightarrow \gamma \quad \textit{then} \quad \vdash \alpha \Rightarrow \gamma.$$

Proof: *We demonstrate this theorem via Hilbert systems by the following steps:*

Step	Theorem	Followed rule
(1)	$\alpha \Rightarrow \beta$	Hypothesis
(2)	$\beta \Rightarrow \gamma$	Hypothesis
(3)	$(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(4)	$(\beta \Rightarrow \gamma) \Rightarrow (\neg\alpha \vee \beta \Rightarrow \neg\alpha \vee \gamma)$	Sub. $x := \beta$, $y := \gamma$, $z := \neg\alpha$
(5)	$(\beta \Rightarrow \gamma) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$	Definition of $\Rightarrow$
(6)	$(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)$	Modus Ponens (2), (5) $\longrightarrow$ (6)
(7)	$\alpha \Rightarrow \gamma$	Modus Ponens (1), (6) $\longrightarrow$ (7)

Theorem 4.5

Prove that:

$$\textit{if} \quad \vdash \alpha \vee \alpha \quad \textit{then} \quad \vdash \alpha.$$

Proof: *We demonstrate this theorem via Hilbert systems by the following steps:*

Step	Theorem	Followed rule
(1)	$(x \vee x) \Rightarrow x$	$(H.A)_1$
(2)	$(\alpha \vee \alpha) \Rightarrow \alpha$	Sub. $x := \alpha$
(3)	$\alpha \vee \alpha$	Hypothesis
(4)	α	Modus Ponens (3), (2) → (4)

Theorem 4.6

Prove that:

$$\textit{if} \quad \vdash \alpha \quad \textit{then} \quad \vdash \alpha \vee \beta.$$

Proof: *We demonstrate this theorem via Hilbert systems by the following steps:*

Step	Theorem	Followed rule
(1)	$x \Rightarrow x \vee y$	$(H.A)_2$
(2)	$\alpha \Rightarrow \alpha \vee \beta$	Sub. $x := \alpha,\ y := \beta$
(3)	α	Hypothesis
(4)	$\alpha \vee \beta$	Modus Ponens (3), (2) → (4)

Theorem 4.7

Prove that:

$$\textit{if} \quad \vdash \alpha \vee \beta \quad \textit{then} \quad \vdash \beta \vee \alpha.$$

Proof: *We demonstrate this theorem via Hilbert systems by the following steps:*

Step	Theorem	Followed rule
(1)	$x \vee y \Rightarrow y \vee x$	$(H.A)_3$
(2)	$\alpha \vee \beta \Rightarrow \beta \vee \alpha$	Sub. $x := \alpha,\ y := \beta$
(3)	$\alpha \vee \beta$	Hypothesis
(4)	$\beta \vee \alpha$	Modus Ponens (3), (2) → (4)

Theorem 4.8

Prove that:

$$\textit{if} \quad \vdash \alpha \Rightarrow \beta \quad \textit{then} \quad \vdash \gamma \vee \alpha \Rightarrow \gamma \vee \beta.$$

Proof: *We demonstrate this theorem via Hilbert systems by the following steps:*

Step	Theorem	Followed rule
(1)	$(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(2)	$(\alpha \Rightarrow \beta) \Rightarrow (\gamma \vee \alpha \Rightarrow \gamma \vee \beta)$	Sub. $x := \alpha$, $y := \beta$, $z := \gamma$
(3)	$\alpha \Rightarrow \beta$	Hypothesis
(4)	$\gamma \vee \alpha \Rightarrow \gamma \vee \beta$	Modus Ponens (3), (2) ⟶ (4)

4.8 Exercises

Exercise 4.4

Give the truth tables of the statements:

1. $(p \vee q) \wedge \neg(p \wedge q)$.
2. $\neg p \rightarrow p \vee q$.
3. $(p \wedge (\neg q \rightarrow p)) \longleftrightarrow r$.
4. $(p \wedge \neg q) \rightarrow (r \vee s)$.

Exercise 4.5

Consider the statements:

$$\begin{aligned} A_1 &:= (p \rightarrow q) \vee (p \rightarrow \neg q), \\ A_2 &:= ((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r), \\ B_1 &:= (p \longleftrightarrow q) \wedge \neg p \wedge q, \\ B_2 &:= (p \wedge r) \wedge \neg(q \rightarrow p). \end{aligned}$$

1. Verify that A_1 and A_2 are tautologies.
2. Verify that B_1 and B_2 are contradictions.

Exercise 4.6

Let A and B be two logical expressions given by:

$$\begin{aligned} A &:= ((p \vee q) \wedge \neg p) \rightarrow q, \\ B &:= ((p \rightarrow \neg q) \wedge q) \wedge p. \end{aligned}$$

1. Prove that A is tautology, then justify your answer via truth table.
2. Prove that A is contradiction, then justify your answer via truth table.

Exercise 4.7

1. Prove the following equivalences:

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

2. Justify your proof.

Exercise 4.8

Find conjunctive and disjunctive normal form of the formulas:

$$\begin{aligned}A_1 &:= (p \wedge \neg q) \to (p \wedge q),\\A_2 &:= (p \to (q \wedge \neg q)) \wedge q,\\A_3 &:= (\neg(p \wedge q) \vee \neg r) \wedge p,\\A_4 &:= (p \vee (q \to r)) \wedge q.\end{aligned}$$

Exercise 4.9

Let A, B and C be three propositions given by:

$$\begin{aligned}A &:= (\neg p \to q) \to (q \to \neg r),\\B &:= \neg(\neg p \vee q) \vee (r \to \neg s),\\C &:= p \wedge q \vee r.\end{aligned}$$

1. Rewrite formulas A and B in conjunctive normal form, respectively.
2. Rewrite formula C in conjunctive normal form.
3. Rewrite formula C in disjunctive normal form.

Exercise 4.10

Consider A, B and C three logical statements which represent the Conditional, Biconditional and Exclusive Disjunction (XOR) connectives, respectively, given by:

$$\begin{aligned}A &:= p \to q,\\B &:= p \longleftrightarrow q,\\C &:= p \oplus q := (p \vee q) \wedge \neg(p \wedge q).\end{aligned}$$

1. Determine the conjunctive and disjunctive normal form of A, B and C, respectively.
2. Prove that:

$$A \equiv C_{nf}(A) \equiv D_{nf}(A),\ B \equiv C_{nf}(B) \equiv D_{nf}(B) \quad and \quad C \equiv C_{nf}(C) \equiv D_{nf}(C).$$

Exercise 4.11

Let A_1 and A_2 be theorems which have demonstrated in course:

$$(A)_1. \quad \textit{If} \quad \vdash \alpha \Rightarrow \beta \quad \textit{and} \quad \vdash \beta \Rightarrow \gamma \quad \textit{then} \quad \vdash \alpha \Rightarrow \gamma.$$
$$(A)_2. \quad \textit{If} \quad \vdash \alpha \vee \beta \quad \textit{then} \quad \vdash \beta \vee \alpha.$$

Based on these theorems and Hilbert-Ackerman axioms, prove that:

1. $(R)_1$. $\vdash \neg\alpha \Rightarrow (\alpha \Rightarrow \beta)$.
2. $(R)_2$. $\vdash \alpha \Rightarrow (\beta \Rightarrow \alpha)$.
3. $(R)_3$. *If* $\vdash \alpha$ *then* $\vdash \beta \Rightarrow \alpha$.
4. $(R)_4$. *If* $\vdash \alpha \Rightarrow \gamma$ *and* $\vdash \beta \Rightarrow \sigma$ *and* $\vdash \neg\gamma \vee \neg\sigma$ *then* $\vdash \neg\alpha \vee \neg\beta$.

4.9 Solutions

Solution of exercise 4.4: (The truth tables)

1. First proposition:

p	q	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	0	0	1	0

2. For the second proposition, we must rewritten it as: $\neg p \to p \vee q := \neg p \to (p \vee q)$, then we draw the truth table:

p	q	$\neg p$	$p \vee q$	$\neg p \to (p \vee q)$
1	1	0	1	1
1	0	0	1	1
0	1	1	1	1
0	0	1	0	0

3. Third proposition:

p	q	r	$\neg q$	$\neg q \to p$	$p \wedge (\neg q \to p)$	$(p \wedge (\neg q \to p)) \longleftrightarrow r$
1	1	1	0	1	1	1
1	1	0	0	1	1	0
1	0	1	1	1	1	1
1	0	0	1	1	1	0
0	1	1	0	1	0	0
0	1	0	0	1	0	1
0	0	1	1	0	0	0
0	0	0	1	0	0	1

4. Last proposition:

p	q	r	s	$\neg q$	$p \wedge \neg q$	$r \vee s$	$(p \wedge \neg q) \to (r \vee s)$
1	1	1	1	0	0	1	1
1	1	1	0	0	0	1	1
1	1	0	1	0	0	1	1
1	1	0	0	0	0	0	1
1	0	1	1	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	1	1	1	1	1
1	0	0	0	1	1	0	0
1	1	1	1	0	0	1	1
0	1	1	0	0	0	1	1
0	1	0	1	0	0	1	1
0	1	0	0	0	0	0	1
0	0	1	1	1	0	1	1
0	0	1	0	1	0	1	1
0	0	0	1	1	0	1	1
0	0	0	0	1	0	0	1

Solution of exercise 4.5:

1. We verify that A_1 and A_2 are tautologies via the truth tables:

p	q	$p \to q$	$\neg q$	$p \to \neg q$	$A_1 := (p \to q) \vee (p \to \neg q)$
1	1	1	0	0	1
1	0	0	1	1	1
0	1	1	0	1	1
0	0	1	1	1	1

p	q	r	$p\rightarrow q$	$q\rightarrow r$	$(p\rightarrow q)\wedge(q\rightarrow r)$	$p\rightarrow r$	$A_2 := ((p\rightarrow q)\wedge(q\rightarrow r))\rightarrow(p\rightarrow r)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

So, we conclude that A_1 and A_2 are tautologies.

2. We verify that B_1 and B_2 are contradictions via the truth tables:

p	q	$p\longleftrightarrow q$	$\neg p$	$(p\longleftrightarrow q)\wedge\neg p$	$B_1 := (p\longleftrightarrow q)\wedge\neg p\wedge q$
1	1	1	0	0	0
1	0	0	0	0	0
0	1	0	1	0	0
0	0	1	1	1	0

p	q	r	$p\wedge r$	$q\rightarrow p$	$\neg(q\rightarrow p)$	$B_2 := (p\wedge r)\wedge\neg(q\rightarrow p)$
1	1	1	1	1	0	0
1	1	0	0	1	0	0
1	0	1	1	1	0	0
1	0	0	0	1	0	0
0	1	1	0	0	1	0
0	1	0	0	0	1	0
0	0	1	0	1	0	0
0	0	0	0	1	0	0

So, we conclude that B_1 and B_2 are contradictions.

Solution of exercise 4.6:

1. Prove that A is a tautology. We have:

$$\begin{aligned}
A &:= ((p\vee q)\wedge\neg p)\longrightarrow q, && (\textit{formula}),\\
&\equiv ((p\wedge\neg p)\vee(q\wedge\neg p))\longrightarrow q, && (\textit{distributivity}),\\
&\equiv (F\vee(q\wedge\neg p))\longrightarrow q, && (\textit{complementation}),\\
&\equiv (q\wedge\neg p)\longrightarrow q, && (\textit{identity}),\\
&\equiv \neg(q\wedge\neg p)\vee q, && (\textit{definition}),\\
&\equiv (\neg q\vee p)\vee q, && (\textit{De Morgan's law}),\\
&\equiv (\neg q\vee q)\vee p, && (\textit{associativity}),\\
&\equiv T\vee p, && (\textit{complementation}),\\
&\equiv T. && (\textit{domination}).
\end{aligned}$$

Justify the answer via truth table.

p	q	$p\vee q$	$\neg p$	$(p\vee q)\wedge\neg p$	$A:=((p\vee q)\wedge\neg p)\longrightarrow q$
1	1	1	0	0	1
1	0	1	0	0	1
0	1	1	1	1	1
0	0	0	1	0	1

2. Prove that B is a contradiction. We have:

$$\begin{aligned}
B &:= ((p\longrightarrow\neg q)\wedge q)\wedge p, && (\textit{formula}),\\
&\equiv ((\neg p\vee\neg q)\wedge q)\wedge p, && (\textit{definition}),\\
&\equiv ((\neg p\wedge q)\vee(\neg q\wedge q))\wedge p, && (\textit{distributivity}),\\
&\equiv ((\neg p\wedge q)\vee F)\wedge p, && (\textit{complementation}),\\
&\equiv (\neg p\wedge q)\wedge p, && (\textit{identity}),\\
&\equiv (\neg p\wedge p)\wedge q, && (\textit{associativity}),\\
&\equiv F\wedge q, && (\textit{complementation}),\\
&\equiv F. && (\textit{domination}).
\end{aligned}$$

Justify the answer via truth table.

p	q	$\neg q$	$p\longrightarrow\neg q$	$(p\longrightarrow\neg q)\wedge q$	$B:=((p\longrightarrow\neg q)\wedge q)\wedge p$
1	1	0	0	0	0
1	0	1	1	0	0
0	1	0	1	1	0
0	0	1	1	0	0

Solution of exercise 4.7:

1. Proof of the first equivalence:

$$\begin{aligned}(p\to q)\land(p\land\neg q) &\equiv (\neg p\lor q)\land(p\land\neg q), \quad (\textit{definition}),\\ &\equiv (\neg p\land(p\land\neg q))\lor(q\land(p\land\neg q)), \quad (\textit{distributivity}),\\ &\equiv ((\neg p\land p)\land\neg q)\lor((q\land\neg q)\land p), \quad (\textit{associativity}),\\ &\equiv (F\land\neg q)\lor(F\land p), \quad (\textit{complementation}),\\ &\equiv F\lor F, \quad (\textit{domination}),\\ &\equiv F. \quad (\textit{identity}).\end{aligned}$$

Justify the proof via truth table.

p	q	$p\to q$	$\neg q$	$p\land\neg q$	$(p\to q)\land(p\land\neg q)$	F
1	1	1	0	0	0	0
1	0	0	1	1	0	0
0	1	1	0	0	0	0
0	0	1	1	0	0	0

Proof of the second equivalence:

$$\begin{aligned}(\neg p\lor q)\land(p\lor\neg q) &\equiv (\neg p\land(p\lor\neg q))\lor(q\land(p\lor\neg q)), \quad (\textit{distributivity}),\\ &\equiv ((\neg p\land p)\lor(\neg p\land\neg q))\lor((q\land p)\lor(q\land\neg q)), \quad (\textit{distributivity}),\\ &\equiv (F\lor(\neg p\land\neg q))\lor((q\land p)\lor F), \quad (\textit{complementation}),\\ &\equiv (\neg p\land\neg q)\lor(p\land q). \quad (\textit{identity}).\end{aligned}$$

Justify the proof via truth table.

p	q	$\neg p$	$\neg q$	$\neg p\lor q$	$p\lor\neg q$	$(\neg p\lor q)\land(p\lor\neg q)$	$\neg p\land\neg q$	$p\land q$	$(\neg p\land\neg q)\lor(p\land q)$
1	1	0	0	1	1	1	0	1	1
1	0	0	1	0	1	0	0	0	0
0	1	1	0	1	0	0	0	0	0
0	0	1	1	1	1	1	1	0	1

Proof of the third equivalence:

$$\begin{aligned}
(\neg p \wedge (q \vee r)) \to q &\equiv \neg(\neg p \wedge (q \vee r)) \vee q, \quad (\textit{definition}),\\
&\equiv (p \vee \neg(q \vee r)) \vee q, \quad (\textit{De Morgan's law}),\\
&\equiv (p \vee (\neg q \wedge \neg r)) \vee q, \quad (\textit{De Morgan's law}),\\
&\equiv p \vee ((\neg q \wedge \neg r) \vee q), \quad (\textit{associativity}),\\
&\equiv p \vee ((\neg q \vee q) \wedge (\neg r \vee q)), \quad (\textit{distributivity}),\\
&\equiv p \vee (T \wedge (\neg r \vee q)), \quad (\textit{complementation}),\\
&\equiv p \vee (\neg r \vee q), \quad (\textit{identity}),\\
&\equiv p \vee q \vee \neg r. \quad (\textit{associativity}).
\end{aligned}$$

Justify the proof via truth table.

p	q	r	$\neg p$	$q \vee r$	$\neg p \wedge (q \vee r)$	$(\neg p \wedge (q \vee r)) \to q$	$p \vee q$	$\neg r$	$p \vee q \vee \neg r$
1	1	1	0	1	0	1	1	0	1
1	1	0	0	1	0	1	1	1	1
1	0	1	0	1	0	1	1	0	1
1	0	0	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1	0	1
0	1	0	1	1	1	1	1	1	1
0	0	1	1	1	1	0	0	0	0
0	0	0	1	0	0	1	0	1	1

Solution of exercise 4.8:

Find the C_{nf} and D_{nf} of A_1 via its truth table:

p	q	$\neg q$	$p \wedge \neg q$	$p \wedge q$	$A_1 := (p \wedge \neg q) \to (p \wedge q)$
1	1	0	0	1	1
1	0	1	1	0	0
0	1	0	0	0	1
0	0	1	0	0	1

Thus,

$$\begin{aligned}
C_{nf}(A_1) &:= (\neg p \vee q),\\
D_{nf}(A_1) &:= (p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q).
\end{aligned}$$

Find the C_{nf} and D_{nf} of A_2 via its truth table:

p	q	$\neg q$	$q\wedge\neg q$	$p\to(q\wedge\neg q)$	$A_2 := (p\to(q\wedge\neg q))\wedge q$
1	1	0	0	0	0
1	0	1	0	0	0
0	1	0	0	1	1
0	0	1	0	1	0

Thus,

$$\begin{aligned} C_{nf}(A_2) &:= (\neg p\vee\neg q)\wedge(\neg p\vee q)\wedge(p\vee q),\\ D_{nf}(A_2) &:= (\neg p\wedge q). \end{aligned}$$

Find the C_{nf} and D_{nf} of A_3 via its truth table:

p	q	r	$p\wedge q$	$\neg(p\wedge q)$	$\neg r$	$\neg(p\wedge q)\vee\neg r$	$A_3 := (\neg(p\wedge q)\vee\neg r)\wedge p$
1	1	1	1	0	0	0	0
1	1	0	1	0	1	1	1
1	0	1	0	1	0	1	1
1	0	0	0	1	1	1	1
0	1	1	0	1	0	1	0
0	1	0	0	1	1	1	0
0	0	1	0	1	0	1	0
0	0	0	0	1	1	1	0

Thus,

$$\begin{aligned} C_{nf}(A_3) &:= (\neg p\vee\neg q\vee\neg r)\wedge(p\vee\neg q\vee\neg r)\wedge(p\vee\neg q\vee r)\wedge(p\vee q\vee\neg r)\wedge(p\vee q\vee r),\\ D_{nf}(A_3) &:= (p\wedge q\wedge\neg r)\vee(p\wedge\neg q\wedge r)\vee(p\wedge\neg q\wedge\neg r). \end{aligned}$$

Find the C_{nf} and D_{nf} of A_4 via its truth table:

p	q	r	$q\to r$	$p\vee(q\to r)$	$A_4 := (p\vee(q\to r))\wedge q$
1	1	1	1	1	1
1	1	0	0	1	1
1	0	1	1	1	0
1	0	0	1	1	0
0	1	1	1	1	1
0	1	0	0	0	0
0	0	1	1	1	0
0	0	0	1	1	0

Thus,

$$\begin{aligned} C_{nf}(A_4) &:= (\neg p\vee q\vee\neg r)\wedge(\neg p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(p\vee q\vee\neg r)\wedge(p\vee q\vee r),\\ D_{nf}(A_4) &:= (p\wedge q\wedge r)\vee(p\wedge q\wedge\neg r)\vee(\neg p\wedge q\wedge r). \end{aligned}$$

Solution of exercise 4.9:

1. Rewrite the formula A in conjunctive normal form:

$$\begin{aligned} A &:= (\neg p \rightarrow q) \rightarrow (q \rightarrow \neg r), \quad (formula),\\ &\equiv \neg(\neg p \rightarrow q) \vee (q \rightarrow \neg r), \quad (definition),\\ &\equiv \neg(p \vee q) \vee (\neg q \vee \neg r), \quad (definition),\\ &\equiv (\neg p \wedge \neg q) \vee (\neg q \vee \neg r), \quad (De\ Morgan's\ law),\\ &\equiv ((\neg q \vee \neg r) \vee \neg p) \wedge ((\neg q \vee \neg r) \vee \neg q), \quad (distributivity),\\ &\equiv (\neg p \vee \neg q \vee \neg r) \wedge (\neg q \vee \neg q \vee \neg r), \quad (associativity),\\ &\equiv (\neg p \vee \neg q \vee \neg r) \wedge (\neg q \vee \neg r), \quad (idempotent). \end{aligned}$$

So,

$$C_{nf}(A) := (\neg p \vee \neg q \vee \neg r) \wedge (\neg q \vee \neg r).$$

1. Rewrite formula B in conjunctive normal form:

$$\begin{aligned} B &:= \neg(\neg p \vee q) \vee (r \rightarrow \neg s), \quad (formula),\\ &\equiv (p \wedge \neg q) \vee (r \rightarrow \neg s), \quad (De\ Morgan's\ law),\\ &\equiv (p \wedge \neg q) \vee (\neg r \vee \neg s), \quad (definition),\\ &\equiv ((\neg r \vee \neg s) \vee p) \wedge ((\neg r \vee \neg s) \vee \neg q), \quad (distributivity),\\ &\equiv (p \vee \neg r \vee \neg s) \wedge (\neg q \vee \neg r \vee \neg s), \quad (associativity). \end{aligned}$$

So,

$$C_{nf}(B) := (p \vee \neg r \vee \neg s) \wedge (\neg q \vee \neg r \vee \neg s).$$

2. Rewrite formula C in conjunctive normal form:

$$\begin{aligned} C &:= p \wedge q \vee r, \quad (formula),\\ &\equiv (p \wedge q) \vee r, \quad (priority),\\ &\equiv (r \vee p) \wedge (r \vee q), \quad (distributivity),\\ &\equiv (p \vee r) \wedge (q \vee r), \quad (commutativity). \end{aligned}$$

So,

$$C_{nf}(C) := (p \vee r) \wedge (q \vee r).$$

3. Rewrite formula C in disjunctive normal form:

$$\begin{aligned} C &:= p \wedge q \vee r, \quad (formula), \\ &\equiv (p \wedge q) \vee r, \quad (priority). \end{aligned}$$

So,

$$D_{nf}(C) := (p \wedge q) \vee r.$$

Solution of exercise 4.10:

1. Determine the C_{nf} and D_{nf} of the formula A through its truth table:

p	q	$A := p \longrightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Thus,

$$\begin{aligned} C_{nf}(A) &:= (\neg p \vee q), \\ D_{nf}(A) &:= (p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q). \end{aligned}$$

1. Determine the C_{nf} and D_{nf} of the formula B through its truth table:

p	q	$B := p \longleftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Thus,

$$\begin{aligned} C_{nf}(B) &:= (\neg p \vee q) \wedge (p \vee \neg q), \\ D_{nf}(B) &:= (p \wedge q) \vee (\neg p \wedge \neg q). \end{aligned}$$

1. Determine the C_{nf} and D_{nf} of the formula C through its truth table: (The table has been drawn in exercise 01)

p	q	$C := p \oplus q := (p \vee q) \wedge \neg(p \wedge q)$
1	1	0
1	0	1
0	1	1
0	0	0

Thus,

$$\begin{aligned} C_{nf}(C) &:= (\neg p \vee \neg q) \wedge (p \vee q), \\ D_{nf}(C) &:= (p \wedge \neg q) \vee (\neg p \wedge q). \end{aligned}$$

2. Prove that $A \equiv C_{nf}(A) \equiv D_{nf}(A)$:

$$\begin{aligned} A &:= p \to q, \quad (\textit{formula}), \\ &\equiv (\neg p \vee q), \quad (\textit{definition}), \\ &:= C_{nf}(A), \quad (\textit{truth table}). \end{aligned}$$

And,

$$\begin{aligned} D_{nf}(A) &:= (p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q), \quad (\textit{truth table}), \\ &\equiv ((p \wedge q) \vee (\neg p \wedge q)) \vee (\neg p \wedge \neg q), \quad (\textit{associativity}), \\ &\equiv (q \wedge (p \vee \neg p)) \vee (\neg p \wedge \neg q), \quad (\textit{anti-distributivity}), \\ &\equiv (q \wedge T) \vee (\neg p \wedge \neg q), \quad (\textit{complementation}), \\ &\equiv q \vee (\neg p \wedge \neg q), \quad (\textit{identity}), \\ &\equiv (q \vee \neg p) \wedge (q \vee \neg q), \quad (\textit{distributivity}), \\ &\equiv (q \vee \neg p) \wedge T, \quad (\textit{complementation}), \\ &\equiv (q \vee \neg p), \quad (\textit{identity}), \\ &\equiv (\neg p \vee q), \quad (\textit{commutativity}), \\ &:= A, \quad (\textit{definition}). \end{aligned}$$

So,

$$A \equiv C_{nf}(A) \equiv D_{nf}(A).$$

2. Prove that $B \equiv C_{nf}(B) \equiv D_{nf}(B)$:

$$\begin{aligned} B &:= p \longleftrightarrow q, \quad (\textit{formula}), \\ &\equiv (p \to q) \wedge (q \to p), \quad (\textit{definition}), \\ &\equiv (\neg p \vee q) \wedge (\neg q \vee p), \quad (\textit{definition}), \\ &:= C_{nf}(B), \quad (\textit{truth table}). \end{aligned}$$

And,

$$\begin{aligned} D_{nf}(B) &:= (p\wedge q)\vee(\neg p\wedge\neg q), \quad (\textit{truth table}),\\ &\equiv (\neg p\vee q)\wedge(\neg q\vee p), \quad (\textit{exercise 04, second formula}),\\ &:= C_{nf}(B), \quad (\textit{truth table}). \end{aligned}$$

So,

$$B\equiv C_{nf}(B)\equiv D_{nf}(B).$$

2. Prove that $C\equiv C_{nf}(C)\equiv D_{nf}(C)$:

$$\begin{aligned} C &:= p\oplus q, \quad (\textit{formula}),\\ &\equiv (p\vee q)\wedge\neg(p\wedge q), \quad (\textit{definition}),\\ &\equiv (p\vee q)\wedge(\neg p\vee\neg q), \quad (\textit{De Morgan's law}),\\ &:= C_{nf}(C), \quad (\textit{truth table}). \end{aligned}$$

And,

$$\begin{aligned} D_{nf}(C) &:= (p\wedge\neg q)\vee(\neg p\wedge q), \quad (\textit{truth table}),\\ &\equiv ((p\wedge\neg q)\vee\neg p)\wedge((p\wedge\neg q)\vee q), \quad (\textit{distributivity}),\\ &\equiv ((p\vee\neg p)\wedge(\neg q\vee\neg p))\wedge((p\vee q)\wedge(\neg q\vee q)), \quad (\textit{distributivity}),\\ &\equiv (T\wedge(\neg q\vee\neg p))\wedge((p\vee q)\wedge T), \quad (\textit{complementation}),\\ &\equiv (\neg q\vee\neg p)\wedge(p\vee q), \quad (\textit{identity}),\\ &\equiv (\neg p\vee\neg q)\wedge(p\vee q), \quad (\textit{commutativity}),\\ &:= C_{nf}(C), \quad (\textit{truth table}). \end{aligned}$$

So,

$$C\equiv C_{nf}(C)\equiv D_{nf}(C).$$

Solution of exercise 4.11:

1. Proof of $(R)_1$. We have:

Step	Theorem	Followed rule
(1)	$x\Rightarrow(x\vee y)$	$(H.A)_2$
(2)	$\neg\alpha\Rightarrow(\neg\alpha\vee\beta)$	Sub. $x:=\neg\alpha,\ y:=\beta$
(3)	$\neg\alpha\Rightarrow(\alpha\Rightarrow\beta)$	Definition of $\Rightarrow$

2. Proof of $(R)_2$. We have:

Step	Theorem	Followed rule
(1)	$x \Rightarrow (x \vee y)$	$(H.A)_2$
(2)	$(x \vee y) \Rightarrow (y \vee x)$	$(H.A)_3$
(3)	$x \Rightarrow (y \vee x)$	$(A)_1$ for (1), (2)
(4)	$\alpha \Rightarrow (\neg\beta \vee \alpha)$	Sub. $x := \alpha$, $y := \neg\beta$
(5)	$\alpha \Rightarrow (\beta \Rightarrow \alpha)$	Definition of $\Rightarrow$

3. Proof of $(R)_3$. We have:

Step	Theorem	Followed rule
(1)	α	Hypothesis
(2)	$\alpha \Rightarrow (\beta \Rightarrow \alpha)$	$(R)_2$
(3)	$(\beta \Rightarrow \alpha)$	Modus Ponens (1), (2) → (3)

4. Proof of $(R)_4$. We have:

Step	Theorem	Followed rule
(1)	$\alpha \Rightarrow \gamma$	Hypothesis
(2)	$\beta \Rightarrow \sigma$	Hypothesis
(3)	$\neg\gamma \vee \neg\sigma$	Hypothesis
(4)	$\neg\sigma \vee \neg\gamma$	$(A)_2$ for (3)
(5)	$\sigma \Rightarrow \neg\gamma$	Definition of $\Rightarrow$
(6)	$\beta \Rightarrow \neg\gamma$	$(A)_1$ for (2), (5)
(7)	$\neg\beta \vee \neg\gamma$	Definition of $\Rightarrow$
(8)	$\neg\gamma \vee \neg\beta$	$(A)_2$ for (7)
(9)	$\gamma \Rightarrow \neg\beta$	Definition of $\Rightarrow$
(10)	$\alpha \Rightarrow \neg\beta$	$(A)_1$ for (1), (9)
(11)	$\neg\alpha \vee \neg\beta$	Definition of $\Rightarrow$

5

Predicate calculus

In the previous chapter, we have seen that propositional calculus allow us to examine the expression of boolean operations on propositions. However, there are a lot of mathematical assertions cannot be analyzed using propositional calculus. This is what led to the emergence of predicate calculus. Predicate calculus also known as first-order logic. Is a formal system in mathematical logic, which uses a richer construction by incorporating predicates, quantifiers, connectives and variables in order to represent relationships between objects. Predicate calculus represent powerful role in various fields such as: formalizing mathematical theories and structures in a precise, artificial intelligence, software and hardware designs, database query languages, etc. This chapter is dedicated for introducing the predicate calculus, their essential properties and applications.

5.1 Predicates

Definition 5.1

In mathematical logic, we call ***predicates***, every propositions whose truth value is depended on their variables (or objects).

Example 5.1

Consider the proposition $P(x)$:

$$P(x):\ x^2 = 4.$$

We can see that truth value of proposition $P(x)$ depends on the object x. $P(x)$ is true if $x = 2$ or $x = -2$, and $P(x)$ is false elsewhere.

Example 5.2

Consider the proposition $Q(x,y)$*:*

$$Q(x,y):\ x+y=9.$$

We can see that truth value of proposition $Q(x,y)$ *depends on the objects* x *and* y*. Here,* $Q(2,7)$, $Q(9,0)$ *are true, and* $Q(-5,8)$, $Q(1,1)$ *are false.*

5.2 Language of predicates

Definition 5.2

To construct predicates, we need to use: alphabets, terms and formulas, which are introduced as follows:

Definition 5.3: (Alphabets)

Are formed by:

1. Connectives: $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$.
2. Universal quantifier: $\forall$ and Existential quantifier: $\exists$.
3. Constant symbols: $a,\ b,\ c,\ d,\dots$.
4. Variable symbols: $x,\ y,\ z,\ t,\dots$.
5. Function symbols: $f_0,\ f_1,\ g_0,\ g_1,\dots$.
6. Predicate symbols: $P_0,\ P_1,\ Q_0,\ Q_1,\dots$.

Definition 5.4: (Terms)

Are formed by:

1. Every constant: is a term.
2. Every variable: is a term.
3. If $t_1,\ t_2,\dots,\ t_n$ are terms. Then: the function symbols $f(t_1,\ t_2,\dots,\ t_n)$ is a term.

We point out that everything not obtained under rules 1, 2 and 3: is not a term.

Definition 5.5: (Formulas)

Are formed by:

1. Propositional variable: is a formula.
2. If $t_1, t_2, ..., t_n$ are terms. Then: the predicate symbols $P(t_1, t_2, ..., t_n)$ is a formula.
3. If α, β are formulas. Then: $\neg\alpha$, $\alpha\wedge\beta$, $\alpha\vee\beta$, $\alpha\Rightarrow\beta$, $\alpha\Leftrightarrow\beta$ are formulas.
4. If α is formula, and x is variable. Then: $\forall x\,\alpha$ and $\exists x\,\alpha$ are formulas.

We point out that everything not obtained under rules 1, 2, 3 and 3: is not a formula.

Remark 5.1 ***(Predicate domain)***

In practice, for any predicate formula, we must insert a domain of discourse D. This domain allows as substituting variables for values from it. Hence, we can give a truth value of this predicate formula. In addition, we introduce the following usual definitions:

Definition 5.6

1. The sentence: **For all elements x of D, the proposition $P(x)$ is true**, is written as:
$$\forall x\in D,\ P(x).$$
2. The sentence: **there exists at least one element x of D, such that the proposition $P(x)$ is true**, is written as:
$$\exists x\in D,\ P(x).$$
3. The sentence: **there exists one and only one element x of D, such that the proposition $P(x)$ is true**, is written as:
$$\exists!\,x\in D,\ P(x).$$

Corollary 5.1

Let P be a predicate and its domain D is given as: $D=\{x_1,x_2,...,x_n\}$. Then, we have:

$$\forall x P(x)\Leftrightarrow P(x_1)\wedge P(x_2)\wedge...\wedge P(x_n).$$

$$\exists x P(x)\Leftrightarrow P(x_1)\vee P(x_2)\vee...\vee P(x_n).$$

Exercise 5.1

Represent the following sentence using the predicate language.

1. The graph of function $f(x,y)$ intersects the plane $z=2x+y$.
2. $(u_n)_{n\in\mathbb{N}}$ is an increasing sequence.
3. The function: $f:\mathbb{R}\to\mathbb{R}$ is strictly monotonous on $\mathbb{R}$.

Solution:

Sentence 1, is described as:

$$\exists (x,y)\in\mathbb{R}^2,\ f(x,y)=2x+y.$$

Sentence 2, is described as:

$$\forall n\in\mathbb{N},\ u_{n+1}-u_n\geq 0.$$

Sentence 3, is described as:

$$(\forall (x,y)\in\mathbb{R}^2, (x<y\Rightarrow f(x)<f(y)))\vee(\forall (x,y)\in\mathbb{R}^2, (x<y\Rightarrow f(x)>f(y))).$$

5.3 Properties of quantifiers

5.3.1 Priority of order

Proposition 5.1

Logical connectives and quantifiers are applied in the following order:

1. **Negation:** $\neg$,
2. **Conjunction:** $\wedge$,
3. **Disjunction:** $\vee$,
4. **Universal quantifier:** $\forall$,
5. **Existential quantifier:** $\exists$,
6. **Implication:** $\Rightarrow$,
7. **Bi-implication:** $\Leftrightarrow$.

Example 5.3

1. *The formula:*

$$\forall x P(x)\vee\exists y Q(y)\wedge P(x),$$

must be replaced by:

$$\forall x(P(x)\vee\exists y(Q(y)\wedge P(x))).$$

2. *The formula:*

$$\forall (x,y)\in\mathbb{R}^2, x\leq y\Rightarrow f(x)\leq f(y),$$

must be replaced by:

$$\forall (x,y)\in\mathbb{R}^2, (x\leq y\Rightarrow f(x)\leq f(y)).$$

5.3.2 Free and bound variables

Definition 5.7: (Scope of quantifiers)

We call scope of a quantifier, the part of the formula which is covered by this quantifier. Here, the quantifier binds its variable within its scope.

Example 5.4

In the formula:

$$\forall x P(x) \wedge \exists y Q(y) \Rightarrow P(x),$$

the scope of quantifier $\exists$ *is:* $Q(y)$, *and scope of quantifier* $\forall$ *is:* $P(x) \wedge \exists y Q(y)$.

Definition 5.8: (Free and bound variables)

The occurrence of variable in predicate formula has two cases: ***Bound*** if it lies in scope of some quantifier of the same variable. Otherwise the occurrence of this variable is ***Free***.

Remark 5.2

1. *Every variable appears immediately after* $\forall$ *or* $\exists$ *is neither free nor bound.*
2. *If formula contains a variable multiple times, we must consider each occurrence of these variables separately.*
3. *We call every formula with no free variables by:* ***closed formula***.

Example 5.5

1. *In formula:* $P(x) \Rightarrow Q(y,z)$ *variables:* x, y *and* z *are* ***free***.
2. *In formula:* $\forall x P(x) \wedge Q(y,z)$ *variable:* x *is* ***bound***, *and variables:* y *and* z *are* ***free***.
3. *In formula:*

   $$\forall y P(x,y) \wedge Q(y) \Rightarrow \exists x Q(x) \Rightarrow R(z),$$

   variables: y *and* x *are* ***bound***,

   variables: x *and* z *are* ***free***.
4. *The formula:* $\forall x \forall y \exists z P(x,y) \wedge Q(y,z)$ *is* ***closed***.

Definition 5.9: (Renaming)

Let α be a formula, x be a bound variable and y be a variable not appearing in α. The replacement of variable x with y in α is called renaming, and gives an equivalent formula to α.

5.3.3 Negation of quantifiers

Definition 5.10

We can see that negation of predicate formulas is similar to De Morgan's law for propositional logic. Negation of universal quantifier is existential quantifier and visa versa. Hence, we have:

1. $\neg(\forall x P(x)) \Leftrightarrow \exists x \neg P(x)$.
2. $\neg(\exists x P(x)) \Leftrightarrow \forall x \neg P(x)$.

Remark 5.3

To determine negation of predicate formulas, one may be use that:

1. *Negation of:* $>$ *is* $\leq$.
2. *Negation of:* $\geq$ *is* $<$.
3. *Negation of:* $=$ *is* $\neq$.
4. *Negation of:* $P \Rightarrow Q$ *is* $P \wedge \neg Q$.

Example 5.6

Negation of: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 1$ *is:* $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \neq 1$.

Example 5.7

Clearly, that definition of a continuous function g *on point* x_0 *is given by:*

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in D_g, (|x - x_0| < \delta \Rightarrow |g(x) - g(x_0)| < \varepsilon).$$

So, we say that: g *is not continuous on point* x_0 *if:*

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x \in D_g, (|x - x_0| < \delta \wedge |g(x) - g(x_0)| \geq \varepsilon).$$

Corollary 5.2

In the propositional logic, we have shown that sets $\Gamma_1 = \{\neg, \vee\}$ and $\Gamma_2 = \{\neg, \wedge\}$ are complete. Beside, negating a universal or existential quantifier flips it to become the other one. So, we conclude that sets $\widetilde{\Gamma}_1 = \{\neg, \vee, \forall\}$, $\widehat{\Gamma}_1 = \{\neg, \vee, \exists\}$, $\widetilde{\Gamma}_2 = \{\neg, \wedge, \forall\}$ and $\widehat{\Gamma}_2 = \{\neg, \wedge, \exists\}$ are complete in predicate calculus.

5.3.4 Precedence of quantifiers

Quantifiers have a different precedence based on: parentheses of the formula, type of connectives and number of variables. We list the essential of them in the following propositions, and we will prove some of them in exercise series.

Proposition 5.2: (Predicate formulas of one variable)

1. $\forall x P(x) \wedge \forall x Q(x) \Leftrightarrow \forall x (P(x) \wedge Q(x))$.
2. $\forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x (P(x) \vee Q(x))$.
3. $\forall x P(x) \Rightarrow \forall x Q(x) \Leftarrow \forall x (P(x) \Rightarrow Q(x))$.
4. $\exists x P(x) \vee \exists x Q(x) \Leftrightarrow \exists x (P(x) \vee Q(x))$.
5. $\exists x P(x) \wedge \exists x Q(x) \Leftarrow \exists x (P(x) \wedge Q(x))$.
6. $\exists x P(x) \Rightarrow \exists x Q(x) \Rightarrow \exists x (P(x) \Rightarrow Q(x))$.

Proposition 5.3: (Predicate formulas of two variables)

1. $\forall x \forall y P(x,y) \Leftrightarrow \forall y \forall x P(x,y)$.
2. $\exists x \exists y P(x,y) \Leftrightarrow \exists y \exists x P(x,y)$.
3. $\exists x \forall y P(x,y) \Rightarrow \forall y \exists x P(x,y)$.

Proposition 5.4: (Predicate formulas without parentheses)

In predicate formulas without parentheses, the quantifiers must apply to the smallest possible part of the formula to their right. Such as:

1. $\forall x P(x) \vee Q(x) \Leftrightarrow (\forall x P(x)) \vee Q(x)$.
2. $\exists x P(x) \wedge Q(x) \Leftrightarrow (\exists x P(x)) \wedge Q(x)$.
3. $\forall x P(x) \Rightarrow Q(x) \Leftrightarrow (\forall x P(x)) \Rightarrow Q(x)$.
4. $P(x) \Rightarrow \exists x Q(x) \Leftrightarrow P(x) \Rightarrow (\exists x Q(x))$.

But, when parentheses appear in the formulas, their presence overrides the default precedence of quantifiers.

5.4 Semantics of predicate calculus

5.4.1 Interpretation

In predicate calculus, to say that formulas are true or false, we must know the signification of each symbols that appear in these formula. As we will show in the next definitions.

Definition 5.11: (Interpretation)

In predicate calculus, an interpretation I is a function from a domain D, which gives a signification of each: predicate, function and constant symbols.

Definition 5.12: (Valuation)

In predicate calculus, an evaluation ν consists of giving a value for each variable of the formula an element of domain D.

Definition 5.13: (Interpretation of terms)

We denote $I(t)_\nu$ the interpretation of term t and valuation ν over the domain D. $I(t)_\nu$ takes different forms depending on the term t, which are given as follows:

1. If t is a constant symbol $t = c$, then $I(t)_\nu = I(c)_\nu = I(c)$.
2. If t is a variable symbol $t = x$, then $I(t)_\nu = I(x)_\nu = \nu(x)$.
3. If t is a function term $t = f(t_1, t_2, ..., t_n)$, then

$$I(t)_\nu = I(f(t_1, t_2, ..., t_n))_\nu = I(f)(I(t_1)_\nu, I(t_2)_\nu, ..., I(t_n)_\nu).$$

Definition 5.14: (Interpretation of formulas)

We denote $I(\alpha)_\nu$ the interpretation of formula α and valuation ν over the domain D. $I(\alpha)_\nu$ takes different forms depending on the formula α, which are given as follows:

1. If α is an atomic formula $\alpha = P(t_1, t_2, ..., t_n)$, where P is predicate symbol with image towards the set $\{0, 1\}$, then

$$I(\alpha)_\nu = I(P(t_1, t_2, ..., t_n))_\nu = I(P)(I(t_1)_\nu, I(t_2)_\nu, ..., I(t_n)_\nu).$$

2. If $\alpha = \neg\alpha_1$, then $I(\alpha)_\nu = I(\neg\alpha_1)_\nu = \neg I(\alpha_1)_\nu$.
3. If $\alpha = \alpha_1 \wedge \alpha_2$, then $I(\alpha)_\nu = I(\alpha_1 \wedge \alpha_2)_\nu = I(\alpha_1)_\nu \wedge I(\alpha_2)_\nu$.
4. If $\alpha = \alpha_1 \vee \alpha_2$, then $I(\alpha)_\nu = I(\alpha_1 \vee \alpha_2)_\nu = I(\alpha_1)_\nu \vee I(\alpha_2)_\nu$.
5. If $\alpha = \alpha_1 \Rightarrow \alpha_2$, then $I(\alpha)_\nu = I(\alpha_1 \Rightarrow \alpha_2)_\nu = I(\alpha_1)_\nu \Rightarrow I(\alpha_2)_\nu$.
6. If $\alpha = \alpha_1 \Leftrightarrow \alpha_2$, then $I(\alpha)_\nu = I(\alpha_1 \Leftrightarrow \alpha_2)_\nu = I(\alpha_1)_\nu \Leftrightarrow I(\alpha_2)_\nu$.

5.4.2 Satisfiability of formulas

Definition 5.15

A formula α is called **satisfiable**, if and only if, there exists an interpretation I and a valuation ν for which α is true. We say that the valuation ν satisfies formula α for interpretation I, and we write: $I \models \alpha_\nu$.

Example 5.8

Consider the formula $\alpha \equiv P(f(x,y),y)$. *We define the interpretation* I *over a domain* $D = \mathbb{N}$ *as follows:* $I(P) = " > "$ *(greater than), and* $I(f) = " - "$*(subtraction). In addition, we define the valuation* ν *as follows:* $\nu(x) = 7$ *and* $\nu(y) = 2$. *Thus, we have:*

$$\begin{aligned} I(\alpha)_\nu &= I(P(f(x,y),y))_\nu, \\ &= I(P)(I(f(x,y))_\nu, I(y)_\nu), \\ &= I(P)(I(f)(I(x)_\nu, I(y)_\nu), I(y)_\nu), \\ &= I(P)(I(f)(\nu(x),\nu(y)),\nu(y)), \\ &= I(P)(I(f)(7,2),2), \\ &= I(P)((7-2),2), \\ &= I(P)(5,2), \\ &= 5 > 2, \text{ is true.} \end{aligned}$$

We conclude that valuation ν *satisfies* α *for interpretation* I, *i.e.* $I \models \alpha_\nu$.

We mention that for the valuation $\widetilde{\nu}$ *such that:* $\widetilde{\nu}(x) = 1$ *and* $\widetilde{\nu}(y) = 2$, *we find a false proposition* $(-1 > 2)$. *Which means that valuation* $\widetilde{\nu}$ *not satisfies* α *for interpretation* I, *i.e.* $I \not\models \alpha_{\widetilde{\nu}}$.

Definition 5.16

We say that a set of formulas $\Gamma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ is satisfiable, if and only if, there exists an interpretation I and a valuation ν for which:

$$I \models (\alpha_1)_\nu,\ I \models (\alpha_2)_\nu,\ ...,\ I \models (\alpha_n)_\nu.$$

Definition 5.17

We say that interpretation I is a **model** of the formula α, if and only if, every valuation ν satisfies α for interpretation I, and we write: $I \models \alpha$.

Example 5.9

Consider the formula $\alpha \equiv P(f(x,y),y)$. *We define the interpretation* I *over a domain* $D = \mathbb{R}^*$ *as follows:* $I(P) = " > "$ *(greater than), and* $I(f) = " + "$*(addition). Let* ν *be valuation such that:*

$\nu(x), \nu(y) \in \mathbb{R}^*$, then we have:

$$\begin{aligned}
I(\alpha)_\nu &= I(P(f(x,y),y))_\nu, \\
&= I(P)(I(f(x,y))_\nu, I(y)_\nu), \\
&= I(P)(I(f)(I(x)_\nu, I(y)_\nu), I(y)_\nu), \\
&= I(P)(I(f)(\nu(x), \nu(y)), \nu(y)), \\
&= I(P)(\nu(x)+\nu(y), \nu(y)), \\
&= \nu(x)+\nu(y) > \nu(y), \ \textit{is true for every } \nu(x), \nu(y) \in \mathbb{R}^*.
\end{aligned}$$

We conclude that interpretation I is a model of the formula α, i.e. $I \models \alpha$.

Definition 5.18

We say that interpretation I is a model of set of formulas $\Gamma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, if and only if, I is a model of each formula of Γ, i.e.:

$$I \models \alpha_1, \ I \models \alpha_2, \ ..., \ I \models \alpha_n.$$

Definition 5.19

We say that formula α is **valid**, if and only if, every interpretation I is a model of α, and we write: $\models \alpha$.

Remark 5.4

Generally, to prove that formula α is valid, we use proof by contradiction. We assume that there exist an interpretation I and a valuation ν for which $I \not\models \alpha_\nu$, then leads us to contradiction.

Example 5.10

Consider the formula $\alpha \equiv \neg P(x) \vee P(x)$. Prove that: $\models \alpha$.

We use the proof by contradiction. We suppose that $\not\models \alpha$, which means that exist an interpretation I and a valuation ν for which $I \not\models \alpha_\nu$. Therefore:

$$\begin{aligned}
I \not\models \alpha_\nu &\Leftrightarrow I \not\models (\neg P(x) \vee P(x))_\nu, \\
&\Leftrightarrow \exists I, \exists \nu, \ I \models \neg(\neg P(x) \vee P(x))_\nu, \\
&\Leftrightarrow \exists I, \exists \nu, \ I \models (P(x) \wedge \neg P(x))_\nu, \\
&\Leftrightarrow \exists I, \exists \nu, \ I \models (P(x))_\nu \wedge I \models (\neg P(x))_\nu, \\
&\Leftrightarrow \exists I, \exists \nu, \ I \models (P(x))_\nu \wedge I \not\models (P(x))_\nu, \\
&\Leftrightarrow \ \textit{contradiction}.
\end{aligned}$$

Consequently, we find that: $\models \alpha$.

Definition 5.20

We say that a formula β is a **logical consequence** of set of formulas Γ, if and only if, for any interpretation I, any valuation v which satisfies each formula of Γ, also satisfies β.

5.5 Normalization forms

In the propositional calculus, we have shown that every formula can be rewritten in conjunctive and disjunctive normal form. In a similar way, we will see how to define the normal forms concerning predicate calculus.

5.5.1 Prenex form

Definition 5.21

We say that a formula α is written in Prenex form if:

$$\alpha \equiv \Lambda_1 x_1 \Lambda_2 x_2 ... \Lambda_n x_n M,$$

where, each $\Lambda_.$ represents an universal or existential quantifier $(\forall, \exists)$, $x_1, ..., x_n$ are variables, and M is predicate expression contains only logical connectives. Here, M is called quantifier-free part or matrix.

Example 5.11

The formula $\alpha \equiv \exists x \forall y (P(x) \wedge Q(x, y))$ *is written in Prenex form.*

Remark 5.5

It is always possible to transform any formula into an equivalent formula in Prenex form. To do this, the following points should be taken into consideration:

1. *Move all occurrences of negation inwards.*
2. *When same variable is used in different parts of the formula, rename them as needed to avoid ambiguity.*
3. *One can use the following equivalences:*

$$\left.\begin{array}{l} \forall x \alpha \wedge \beta \equiv \forall x(\alpha \wedge \beta) \\ \forall x \alpha \vee \beta \equiv \forall x(\alpha \vee \beta) \\ \exists x \alpha \wedge \beta \equiv \exists x(\alpha \wedge \beta) \\ \exists x \alpha \vee \beta \equiv \exists x(\alpha \vee \beta) \\ \forall x \alpha \Rightarrow \beta \equiv \exists x(\alpha \Rightarrow \beta) \\ \exists x \alpha \Rightarrow \beta \equiv \forall x(\alpha \Rightarrow \beta) \end{array}\right\} \text{ when } x \text{ not occurring in } \beta.$$

And,

$$\left.\begin{array}{l}\alpha\wedge\forall x\beta\equiv\forall x(\alpha\wedge\beta)\\ \alpha\vee\forall x\beta\equiv\forall x(\alpha\vee\beta)\\ \alpha\wedge\exists x\beta\equiv\exists x(\alpha\wedge\beta)\\ \alpha\vee\exists x\beta\equiv\exists x(\alpha\vee\beta)\\ \alpha\Rightarrow\forall x\beta\equiv\forall x(\alpha\Rightarrow\beta)\\ \alpha\Rightarrow\exists x\beta\equiv\exists x(\alpha\Rightarrow\beta)\end{array}\right\}\ \textit{when } x \textit{ not occurring in } \alpha.$$

Example 5.12

Determine Prenex form of the formula: $\alpha\equiv\forall x\forall yP(x,y)\Rightarrow\exists zQ(x,z)$.

We have:

$$\begin{aligned}\alpha &\equiv \forall x\forall yP(x,y)\Rightarrow\exists zQ(x,z),\\ &\equiv \forall x\forall yP(x,y)\Rightarrow\exists zQ(t,z), \quad (\textit{rename variable}),\\ &\equiv \exists x\exists y(P(x,y)\Rightarrow\exists zQ(t,z)), \quad (\textit{because } x,y \textit{ not occurring in } Q(t,z)),\\ &\equiv \exists x\exists y\exists z(P(x,y)\Rightarrow Q(t,z)), \quad (\textit{because } z \textit{ not occurring in } P(x,y)).\end{aligned}$$

5.5.2 Skolem form

Definition 5.22

We say that a formula α is written in Skolem form if it is in Prenex form with only universal quantifiers.
To transform any formula α into Skolem form, we follow the steps:

1. Rewrite the formula α into Prenex form.
2. Eliminate the existential quantifiers.
3. Replace each existentially quantified variable by a function depended with all variables which are universally quantified before. This function is called Skolem function.

Example 5.13

Consider the following formulas written in Prenex form:

$$\begin{aligned}\alpha &\equiv \exists x\exists yP(x,y),\\ \beta &\equiv \exists x\forall y\exists z(P(x,y,z)\vee Q(y,z)),\\ \gamma &\equiv \forall x\exists y\forall z\exists t(P(x,y)\Rightarrow(Q(y,z)\wedge R(z,t))).\end{aligned}$$

So, their Skolem form are given as:

$$\begin{aligned} \alpha_{sk} &\equiv P(a,b), \quad (a,b \text{ are constants}), \\ \beta_{sk} &\equiv \forall y(P(a,y,f(y)) \vee Q(y,f(y))), \quad (a \text{ is a constant}), \\ \gamma_{sk} &\equiv \forall x \forall z(P(x,f(x)) \Rightarrow (Q(f(x),z) \wedge R(z,g(x,z)))). \end{aligned}$$

Remark 5.6

1. *The formulas α and α_{sk} are not necessarily equivalent.*
2. *We say that formula α_{sk} is satisfiable, if and only if, the formula α is satisfiable.*

5.5.3 Clausal form

Definition 5.23

We say that a formula α is written in Clausal form if it is in Skolem form, without universal quantifiers and its quantifier-free part M is converted to conjunctive normal form, i.e.,

$$M \equiv C_1 \wedge C_2 \wedge \ldots \wedge C_n.$$

Here, $S = \{C_1, C_2, \ldots, C_n\}$ is called set of clauses.

Example 5.14

In the previous example, we have found the Skolem form of γ is given as:

$$\gamma_{sk} \equiv \forall x \forall z(P(x,f(x)) \Rightarrow (Q(f(x),z) \wedge R(z,g(x,z)))).$$

By elimination universal quantifiers, we get:

$$M \equiv P(x,f(x)) \Rightarrow (Q(f(x),z) \wedge R(z,g(x,z))).$$

We convert the quantifier-free part M to conjunctive normal form. It is clear that:

$$\begin{aligned} M &\equiv P(x,f(x)) \Rightarrow (Q(f(x),z) \wedge R(z,g(x,z))), \\ &\equiv \neg P(x,f(x)) \vee (Q(f(x),z) \wedge R(z,g(x,z))), \quad (\text{definition of } \Rightarrow), \\ &\equiv (\neg P(x,f(x)) \vee Q(f(x),z)) \wedge (\neg P(x,f(x)) \vee R(z,g(x,z))), \quad (\text{by distributivity}), \\ &\equiv C_1 \wedge C_2, \quad \text{where, } C_1 = \neg P(x,f(x)) \vee Q(f(x),z), \ C_2 = \neg P(x,f(x)) \vee R(z,g(x,z)). \end{aligned}$$

Which means that we have two clauses C_1 and C_2.

Proposition 5.5

Let S be a set of clauses concerning of the formula α. Then, α is not satisfiable, if and only if, S is not satisfiable.

Exercise 5.2

Consider the formula:

$$\alpha \equiv \exists x P(x) \vee Q(y) \Rightarrow \exists y R(y,x).$$

Find the Prenex, Skolem and Clausal form of α.

Solution:

1. Determine Prenex form of α.

We have:

$$\begin{aligned}
\alpha &\equiv \exists x P(x) \vee Q(y) \Rightarrow \exists y R(y,x),\\
&\equiv \exists x(P(x) \vee Q(y)) \Rightarrow \exists y R(y,x), \quad (\textit{because } x \textit{ not occurring in } Q(y)),\\
&\equiv \exists x(P(x) \vee Q(z)) \Rightarrow \exists y R(y,t), \quad (\textit{rename variables}),\\
&\equiv \forall x((P(x) \vee Q(z)) \Rightarrow \exists y R(y,t)), \quad (\textit{because } x \textit{ not occurring in } R(y,t)),\\
&\equiv \forall x \exists y((P(x) \vee Q(z)) \Rightarrow R(y,t)), \quad (\textit{because } y \textit{ not occurring in } P(x) \vee Q(z)).
\end{aligned}$$

2. Determine Skolem form of α.

We have:

$$\alpha_{sk} \equiv \forall x((P(x) \vee Q(z)) \Rightarrow R(f(x),t)).$$

3. Determine Clausal form of α.

We have:

$$\alpha_{sk} \equiv \forall x((P(x) \vee Q(z)) \Rightarrow R(f(x),t)).$$

By elimination universal quantifiers, we get:

$$M \equiv (P(x) \vee Q(z)) \Rightarrow R(f(x),t).$$

We convert the quantifier-free part M to conjunctive normal form.

$$\begin{aligned}
M &\equiv (P(x) \vee Q(z)) \Rightarrow R(f(x),t),\\
&\equiv \neg(P(x) \vee Q(z)) \vee R(f(x),t), \quad (\textit{definition of } \Rightarrow),\\
&\equiv (\neg P(x) \wedge \neg Q(z)) \vee R(f(x),t), \quad (\textit{De Morgan's law}),\\
&\equiv (\neg P(x) \vee R(f(x),t)) \wedge (\neg Q(z) \vee R(f(x),t)), \quad (\textit{by distributivity}),\\
&\equiv C_1 \wedge C_2, \quad \textit{where, } C_1 = \neg P(x) \vee R(f(x),t),\ C_2 = \neg Q(z) \vee R(f(x),t).
\end{aligned}$$

Which means that we have two clauses C_1 and C_2.

5.6 Exercises

Exercise 5.3

Translate the following sentences to predicate formulas:

1. Archimedean property of positive real numbers.
2. Every natural number n is either even or odd.
3. The function $g : \mathbb{R} \to \mathbb{R}$, is constant on $\mathbb{R}$.
4. The function $g : \mathbb{R} \to \mathbb{R}$, is increasing on $\mathbb{R}$.
5. The function $g : \mathbb{R} \to \mathbb{R}$, is lipschitz on $[a, b]$.
6. The function g has a limit l as x approaches infinity.
7. For any point M on the space S, we say that M in the closed ball B with center O and radius R, if and only if the distance between M and O less or equal to R.

Exercise 5.4

Translate the following sentences:

1. The set S is non convex.
2. The vector v is non eigenvector of the matrix A.
3. The function $g : \mathbb{R} \to \mathbb{R}$, is not lipschitz on $[a, b]$.
4. The function $g : \mathbb{R} \to \mathbb{R}$, is not decreasing on $\mathbb{R}$.
5. The function $g : \mathbb{R} \to \mathbb{R}$, is not monotonous on $\mathbb{R}$.
6. $(w_n)_{n\in\mathbb{N}}$ is non-Cauchy sequence.
7. The function $g : \mathbb{R} \to \mathbb{R}$, is not uniformly continuous on $[a, b]$.

Exercise 5.5

Let D_x and D_y, domain of x and y, respectively. Where,

$$D_x = \{x_1, x_2, x_3\} \quad and \quad D_y = \{y_1, y_2\}.$$

Prove that:

1. $\forall x(P(x) \wedge Q(x)) \Leftrightarrow \forall x P(x) \wedge \forall x Q(x)$.
2. $\exists x(P(x) \vee Q(x)) \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$.
3. $\neg(\forall x P(x)) \Leftrightarrow \exists x \neg P(x)$.
4. $\neg(\exists y Q(y)) \Leftrightarrow \forall y \neg Q(y)$.
5. $\forall x P(x) \vee Q(y) \Leftrightarrow \forall x(P(x) \vee Q(y))$.
6. $P(x) \wedge \exists y Q(y) \Leftrightarrow \exists y(P(x) \wedge Q(y))$.
7. $\forall x P(x) \Rightarrow Q(y) \Leftrightarrow \exists x(P(x) \Rightarrow Q(y))$.
8. $P(x) \Rightarrow \exists y Q(y) \Leftrightarrow \exists y(P(x) \Rightarrow Q(y))$.
9. $\forall x \forall y P(x,y) \Leftrightarrow \forall y \forall x P(x,y)$.

Exercise 5.6

We define the formulas α, β and γ, according their interpretations I and domains D, as follows:

1. $\alpha \equiv P(x, f(x))$, $I(P) =$ ".. < ..", $I(f) =$ "*double of* .." and $D = \mathbb{N}^*$.
2. $\beta \equiv Q(x, f(y))$, $I(Q) =$ ".. *divides* ..", $I(f) =$ ".. *power of 2*" and $D = \{1, 2\}$.
3. $\gamma \equiv \forall x \forall y R(f(x,y), x)$, $I(R) =$ ".. *is multiple of* ..", $I(f) =$ ".. + .." and $D = \{4, 6\}$.

Prove if whether the interpretation I is a model or not.

Exercise 5.7

Consider the following formulas:

$$\begin{aligned} \alpha &\equiv \forall x \exists y P(x,y) \Rightarrow \exists x(\neg \forall y Q(y) \Rightarrow R(x)), \\ \beta &\equiv \forall x P(x) \wedge \exists y Q(y) \Rightarrow \exists y(R(x,y) \wedge \exists z S(z,x)). \end{aligned}$$

1. Determine the Prenex form of α and β.
2. Rewrite α and β in Skolem form.
3. Deduce the Clausal form of α and β.

5.7 Solutions

Solution of exercise 5.3:

Sentence $n01$:

$$\forall a, b \in \mathbb{R}_+^*, \exists n \in \mathbb{N}, (na > b).$$

Sentence $n02$:

$$\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, ((n = 2k) \vee (n = 2k+1)).$$

Sentence $n03$:

$$\exists \beta \in \mathbb{R}, \forall x \in \mathbb{R}, g(x) = \beta.$$

Sentence $n04$:

$$\forall x, y \in \mathbb{R}, (x \leq y \Rightarrow g(x) \leq g(y)).$$

Sentence $n05$:

$$\exists L > 0, \forall x, y \in [a, b], |g(x) - g(y)| \leq L|x - y|.$$

Sentence $n06$:

$$\forall \varepsilon > 0, \exists R > 0, \forall x \in D_g, (x > R \Rightarrow |g(x) - l| < \varepsilon).$$

Sentence $n07$:

$$\forall M \in S, (M \in B \Leftrightarrow MO = R).$$

Solution of exercise 5.4:

Sentence $n01$:

$$\exists x, y \in S, \exists \theta \in [0, 1], \theta x + (1 - \theta) y \notin S.$$

Sentence $n02$:

$$\forall \lambda \in \mathbb{C}, Av \neq \lambda v.$$

Sentence $n03$:

$$\forall L > 0, \exists x, y \in [a, b], |g(x) - g(y)| > L|x - y|.$$

Sentence $n04$:

$$\exists x, y \in \mathbb{R}, ((x \leq y) \wedge g(x) < g(y)).$$

Sentence $n05$:

$$(\exists (x, y) \in \mathbb{R}^2, ((x \leq y) \wedge g(x) > g(y))) \wedge (\exists (x, y) \in \mathbb{R}^2, ((x \leq y) \wedge g(x) < g(y))).$$

Sentence $n06$:

$$\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists p, q \geq N, |w_p - w_q| \geq \varepsilon.$$

Sentence $n07$:

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x, y \in [a,b], (|x-y| < \delta \wedge |g(x) - g(y)| \geq \varepsilon).$$

Solution of exercise 5.5:

Proof of equivalence n^o1: We have:

$$\begin{aligned} \forall x (P(x) \wedge Q(x)) &\Leftrightarrow (P(x_1) \wedge Q(x_1)) \wedge (P(x_2) \wedge Q(x_2)) \wedge (P(x_3) \wedge Q(x_3)), \\ &\Leftrightarrow (P(x_1) \wedge P(x_2) \wedge P(x_3)) \wedge (Q(x_1) \wedge Q(x_2) \wedge Q(x_3)), \ (\textit{associativity of} \wedge), \\ &\Leftrightarrow \forall x P(x) \wedge \forall x Q(x). \end{aligned}$$

Proof of equivalence n^o2: We have:

$$\begin{aligned} \exists x (P(x) \vee Q(x)) &\Leftrightarrow (P(x_1) \vee Q(x_1)) \vee (P(x_2) \vee Q(x_2)) \vee (P(x_3) \vee Q(x_3)), \\ &\Leftrightarrow (P(x_1) \vee P(x_2) \vee P(x_3)) \vee (Q(x_1) \vee Q(x_2) \vee Q(x_3)), \ (\textit{associativity of} \vee), \\ &\Leftrightarrow \exists x P(x) \vee \exists x Q(x). \end{aligned}$$

Proof of equivalence n^o3: We have:

$$\begin{aligned} \neg(\forall x P(x)) &\Leftrightarrow \neg(P(x_1) \wedge P(x_2) \wedge P(x_3)), \\ &\Leftrightarrow \neg P(x_1) \vee \neg P(x_2) \vee \neg P(x_3), \ (\textit{De Morgan's law}), \\ &\Leftrightarrow \exists x \neg P(x). \end{aligned}$$

Proof of equivalence n^o4: We have:

$$\begin{aligned} \neg(\exists y Q(y)) &\Leftrightarrow \neg(Q(y_1) \vee Q(y_2)), \\ &\Leftrightarrow \neg Q(y_1) \wedge \neg Q(y_2), \ (\textit{De Morgan's law}), \\ &\Leftrightarrow \forall y \neg Q(y). \end{aligned}$$

Proof of equivalence n^o5: We have:

$$\begin{aligned} \forall x P(x) \vee Q(y) &\Leftrightarrow (\forall x P(x)) \vee Q(y), \\ &\Leftrightarrow (P(x_1) \wedge P(x_2) \wedge P(x_3)) \vee Q(y), \\ &\Leftrightarrow (P(x_1) \vee Q(y)) \wedge (P(x_2) \vee Q(y)) \wedge (P(x_3) \vee Q(y)), \quad (\textit{by distributivity}), \\ &\Leftrightarrow \forall x (P(x) \vee Q(y)). \end{aligned}$$

Proof of equivalence $n^o 6$: We have:

$$\begin{aligned} P(x)\wedge\exists y Q(y) &\Leftrightarrow P(x)\wedge(\exists y Q(y)),\\ &\Leftrightarrow P(x)\wedge(Q(y_1)\vee Q(y_2)),\\ &\Leftrightarrow (P(x)\wedge Q(y_1))\vee(P(x)\wedge Q(y_2)), \quad \textit{(by distributivity)},\\ &\Leftrightarrow \exists y(P(x)\wedge Q(y)). \end{aligned}$$

Proof of equivalence $n^o 7$: We have:

$$\begin{aligned} \forall x P(x)\Rightarrow Q(y) &\Leftrightarrow (\forall x P(x))\Rightarrow Q(y),\\ &\Leftrightarrow (P(x_1)\wedge P(x_2)\wedge P(x_3))\Rightarrow Q(y),\\ &\Leftrightarrow \neg(P(x_1)\wedge P(x_2)\wedge P(x_3))\vee Q(y), \quad (\textit{definition of } \Rightarrow),\\ &\Leftrightarrow (\neg P(x_1)\vee\neg P(x_2)\vee\neg P(x_3))\vee Q(y), \quad (\textit{De Morgan's law}),\\ &\Leftrightarrow (\neg P(x_1)\vee Q(y))\vee(\neg P(x_2)\vee Q(y))\vee(\neg P(x_3)\vee Q(y)), \quad (\textit{by distributivity}),\\ &\Leftrightarrow \exists x(\neg P(x)\vee Q(y)),\\ &\Leftrightarrow \exists x(P(x)\Rightarrow Q(y)), \quad (\textit{definition of } \Rightarrow). \end{aligned}$$

Proof of equivalence $n^o 8$: We have:

$$\begin{aligned} P(x)\Rightarrow\exists y Q(y) &\Leftrightarrow P(x)\Rightarrow(\exists y Q(y)),\\ &\Leftrightarrow P(x)\Rightarrow(Q(y_1)\vee Q(y_2)),\\ &\Leftrightarrow (\neg P(x))\vee(Q(y_1)\vee Q(y_2)), \quad (\textit{definition of } \Rightarrow),\\ &\Leftrightarrow (\neg P(x)\vee Q(y_1))\vee(\neg P(x)\vee Q(y_2)), \quad (\textit{by distributivity}),\\ &\Leftrightarrow \exists y(\neg P(x)\vee Q(y)),\\ &\Leftrightarrow \exists y(P(x)\Rightarrow Q(y)), \quad (\textit{definition of } \Rightarrow). \end{aligned}$$

Proof of equivalence $n^o 9$: We have:

$$\begin{aligned} \forall x\forall y P(x,y) &\Leftrightarrow \forall x(P(x,y_1)\wedge P(x,y_2)),\\ &\Leftrightarrow (P(x_1,y_1)\wedge P(x_1,y_2))\wedge(P(x_2,y_1)\wedge P(x_2,y_2))\wedge(P(x_3,y_1)\wedge P(x_3,y_2)),\\ &\Leftrightarrow (P(x_1,y_1)\wedge P(x_2,y_1)\wedge P(x_3,y_1))\wedge(P(x_1,y_2)\wedge P(x_2,y_2)\wedge P(x_3,y_2)), (\textit{associativity of} \wedge),\\ &\Leftrightarrow \forall y(P(x_1,y)\wedge P(x_2,y)\wedge P(x_3,y)),\\ &\Leftrightarrow \forall y\forall x P(x,y), \end{aligned}$$

Solution of exercise 5.6:

1. Prove that interpretation I is a model of α or not.

Let $v(x) \in \mathbb{N}^*$ be a valuation, then we have:

$$\begin{aligned}
I(\alpha)_v &= I(P(x, f(x)))_v, \\
&= I(P)(I(x)_v, I(f(x))_v), \\
&= I(P)(I(x)_v, I(f)(I(x)_v)), \\
&= I(P)(v(x), I(f)(v(x))), \\
&= I(P)(v(x), 2v(x)), \\
&= v(x) < 2v(x), \ \textit{is true for every } v(x) \in \mathbb{N}^*.
\end{aligned}$$

So, we conclude that interpretation I is a model of the formula α, i.e. $I \models \alpha$.

2. Prove that interpretation I is a model of β or not.

Let $v(x)$, $v(y) \in D = \{1, 2\}$ be valuations, then we have:

$$\begin{aligned}
I(\beta)_v &= I(Q(x, f(y)))_v, \\
&= I(Q)(I(x)_v, I(f(y))_v), \\
&= I(Q)(I(x)_v, I(f)(I(y)_v)), \\
&= I(Q)(v(x), I(f)(v(y))), \\
&= I(P)(v(x), v(y)^2), \\
&= v(x) \ \textit{divides ?} \ v(y)^2.
\end{aligned}$$

To see that $v(x)$ divides $v(y)^2$ or not, we use proof by cases, which is shown in the following table:

v	v_1	v_2	v_3	v_4
x	1	1	2	2
y^2	1	4	1	4
β	T	T	F	T

So, we conclude that interpretation I is not model of the formula β, i.e. $I \not\models \beta$. But formula β is satisfiable.

3. Prove that interpretation I is a model of γ or not.

Let $\nu(x),\ \nu(y) \in D = \{4,6\}$ be valuations, then we have:

$$\begin{aligned}
I(\gamma)_\nu &= I(\forall x \forall y R(f(x,y),x))_\nu,\\
&= I(\forall x)_\nu I(\forall y)_\nu I(R)(I(f(x,y))_\nu, I(x)_\nu),\\
&= \forall I(x)_\nu,\ \forall I(y)_\nu,\ I(R)(I(f)(I(x)_\nu, I(y)_\nu), I(x)_\nu),\\
&= \forall \nu(x),\ \forall \nu(y),\ I(R)(I(f)(\nu(x),\ \nu(y)),\ \nu(x)),\\
&= \forall \nu(x),\ \forall \nu(y),\ I(R)(\nu(x)+\nu(y),\ \nu(x)),\\
&= \forall \nu(x),\ \forall \nu(y),\ \nu(x)+\nu(y)\ \textit{is multiple of ?}\ \nu(x).
\end{aligned}$$

To see that $\nu(x)+\nu(y)$ is multiple of $\nu(x)$ or not, we use proof by cases, which is shown in the following table:

ν	ν_1	ν_2	ν_3	ν_4
$x+y$	8	10	10	12
x	4	4	6	6
$x+y$ is multiple of x	T	F	F	T

So, we conclude that interpretation I is not model of the formula γ, i.e. $I \not\models \gamma$. But formula γ is satisfiable.

Solution of exercise 5.7:

1. Determine Prenex form of α.

We have:

$$\begin{aligned}
\alpha &\equiv \forall x \exists y P(x,y) \Rightarrow \exists x(\neg \forall y Q(y) \Rightarrow R(x)),\\
&\equiv \forall x \exists y P(x,y) \Rightarrow \exists x(\exists y \neg Q(y) \Rightarrow R(x)),\\
&\equiv \forall x \exists y P(x,y) \Rightarrow \exists x \forall y(\neg Q(y) \Rightarrow R(x)), \quad (\textit{because } y \textit{ not occurring in } R(x)),\\
&\equiv \exists x \forall y \neg P(x,y) \vee \exists x \forall y(\neg Q(y) \Rightarrow R(x)), \quad (\textit{definition of } \Rightarrow),\\
&\equiv \exists x(\forall y \neg P(x,y) \vee \forall y(\neg Q(y) \Rightarrow R(x))), \quad (\textit{equivalence}),\\
&\equiv \exists x(\forall y \neg P(x,y) \vee \forall z(\neg Q(z) \Rightarrow R(x))), \quad (\textit{rename variable}),\\
&\equiv \exists x \forall y(\neg P(x,y) \vee \forall z(\neg Q(z) \Rightarrow R(x))), \quad (\textit{because } y \textit{ not occurring in } \neg Q(z) \Rightarrow R(x)),\\
&\equiv \exists x \forall y \forall z(\neg P(x,y) \vee (\neg Q(z) \Rightarrow R(x))), \quad (\textit{because } z \textit{ not occurring in } \neg P(x,y)).
\end{aligned}$$

Remark: We point out that α can be reduced as:

$$\begin{aligned}
\alpha &\Leftrightarrow \exists x(\forall y \neg P(x,y) \vee \forall y(\neg Q(y) \Rightarrow R(x))), \quad (\textit{equivalence}),\\
&\Rightarrow \exists x \forall y(\neg P(x,y) \vee (\neg Q(y) \Rightarrow R(x))), \quad (\textit{implication}).
\end{aligned}$$

But, the last formula is not equivalent to α.

1. Determine Prenex form of β.

We have:

$$\begin{aligned}
\beta &\equiv \forall x P(x) \wedge \exists y Q(y) \Rightarrow \exists y(R(x,y) \wedge \exists z S(z,x)),\\
&\equiv \forall x(P(x) \wedge \exists y Q(y)) \Rightarrow \exists y(R(x,y) \wedge \exists z S(z,x)), \quad (\textit{because } x \textit{ not occurring in } Q(y)),\\
&\equiv \forall x \exists y(P(x) \wedge Q(y)) \Rightarrow \exists y(R(x,y) \wedge \exists z S(z,x)), \quad (\textit{because } y \textit{ not occurring in } P(x)),\\
&\equiv \forall x \exists y(P(x) \wedge Q(y)) \Rightarrow \exists y \exists z(R(x,y) \wedge S(z,x)), \quad (\textit{because } z \textit{ not occurring in } R(x,y)),\\
&\equiv \exists x \forall y \neg(P(x) \wedge Q(y)) \vee \exists y \exists z(R(x,y) \wedge S(z,x)), \quad (\textit{definition of } z \Rightarrow),\\
&\equiv \exists x \forall y \neg(P(x) \wedge Q(y)) \vee \exists t \exists z(R(r,t) \wedge S(z,r)), \quad (\textit{rename variables}),\\
&\equiv \exists x \forall y(\neg(P(x) \wedge Q(y)) \vee \exists t \exists z(R(r,t) \wedge S(z,r))), \quad (\textit{because } x, y \textit{ not occurring in } R(r,t) \wedge S(z,r)),\\
&\equiv \exists x \forall y \exists t \exists z(\neg(P(x) \wedge Q(y)) \vee (R(r,t) \wedge S(z,r))), \quad (\textit{because } t, z \textit{ not occurring in } \neg(P(x) \wedge Q(y))).
\end{aligned}$$

2. Find Skolem form of α.

We have:

$$\alpha_{sk} \equiv \forall y \forall z(\neg P(a,y) \vee (\neg Q(z) \Rightarrow R(a))), \quad (a \textit{ is a constant}).$$

2. Find Skolem form of β.

We have:

$$\beta_{sk} \equiv \forall y(\neg(P(a) \wedge Q(y)) \vee (R(r, f(y)) \wedge S(g(y), r))), \quad (a \textit{ is a constant}).$$

3. Deduce Clausal form of α.

We have:

$$\alpha_{sk} \equiv \forall y \forall z(\neg P(a,y) \vee (\neg Q(z) \Rightarrow R(a))).$$

By elimination universal quantifiers, we get:

$$M \equiv \neg P(a,y) \vee (\neg Q(z) \Rightarrow R(a)).$$

We convert the quantifier-free part M to conjunctive normal form.

$$\begin{aligned}
M &\equiv \neg P(a,y) \vee (\neg Q(z) \Rightarrow R(a)),\\
&\equiv \neg P(a,y) \vee (Q(z) \vee R(a)), \quad (\textit{definition of } \Rightarrow),\\
&\equiv (\neg P(a,y) \vee Q(z) \vee R(a)), \quad (\textit{associativity}),\\
&\equiv C_1, \quad \textit{where, } C_1 = \neg P(a,y) \vee Q(z) \vee R(a).
\end{aligned}$$

Which means that we have one clause C_1.

3. Deduce Clausal form of β.

We have:

$$\beta_{sk} \equiv \forall y(\neg(P(a) \wedge Q(y)) \vee (R(r, f(y)) \wedge S(g(y), r))).$$

By elimination universal quantifiers, we get:

$$M \equiv \neg(P(a) \wedge Q(y)) \vee (R(r, f(y)) \wedge S(g(y), r)).$$

We convert the quantifier-free part M to conjunctive normal form.

$$\begin{aligned} M &\equiv \neg(P(a) \wedge Q(y)) \vee (R(r, f(y)) \wedge S(g(y), r)), \\ &\equiv (\neg P(a) \vee \neg Q(y)) \vee (R(r, f(y)) \wedge S(g(y), r)), \quad (\textit{De Morgan's law}), \\ &\equiv (\neg P(a) \vee \neg Q(y) \vee R(r, f(y))) \wedge (\neg P(a) \vee \neg Q(y) \vee S(g(y), r)), \quad (\textit{by distributivity}), \\ &\equiv C_1 \wedge C_2, \quad \textit{where,}\ C_1 = \neg P(a) \vee \neg Q(y) \vee R(r, f(y)),\ C_2 = \neg P(a) \vee \neg Q(y) \vee S(g(y), r). \end{aligned}$$

Which means that we have two clauses C_1 and C_2.

Bibliography

[1] Benzeghli Brahim. (2023). Logique-Mathematique. Polycopié de cours. Université Batna 2. https://www.scribd.com/document/786897685/Cours1-Logique-Mathematique

[2] Chiara Ghidini, Luciano Serafini. (2013). Mathematical Logic Exercises. Booklet. https://www.studocu.com/ph/u/101850695?sid=01753611544

[3] Daniel J. Velleman. (1994). How to prove it. Cambridge university press.

[4] Jean-Claude Dupin, Jean-Luc Valein. (1993). Initiation au raisonnement mathématique: Logique et théorie des ensembles. Paris: Armand Colin, 1993. Print.

[5] Christophe Raffalli, René David, Karim Nour. (2004). Introduction à la Logique: Théorie de la démonstration. Sciences Sup. Dunod.

[6] Christian Retoré. (2013). Logique mathématique et linguistique formelle. Géraud Sénizergues. Leçons de mathématiques d'aujourd'hui, Cassini, pp.24, hal-00607693.