الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف بالمسيلة

كلية الرياضيات والإعلام الآلي

قسم الرياضيات

اللجنة العلمية

رقم : 151/ل.ق.ر/ 2024

المسيلة في: 2024-11-05

مستخلص محضر اللجنة العلمية ليوم: 2024/11/05
بخصوص اعتماد مطبوعة دروس

وافقت اللجنة العلمية على اعتماد مطبوعة الدروس الخاصة بالأستاذ

سعداوي الخير المعنونة بـ:

Lecture Notes for Mathematical logic

كمرجع للدروس لطلبة **السنة الثانية ليسانس رياضيات**.

وهذا بعد الاطلاع على التقارير الإيجابية للأستاذ الخبير المكلف بالمطبوعة.

رئيس اللجنة العلمية

جامعة المسيلة
رئيس اللجنة العلمية
لقسم الرياضيات
كلية الرياضيات والإعلام الآلي

رئيس اللجنة العلمية
لقسم الرياضيات
مرزوقي عبد الكريم

سلمت هذه الشهادة للمعني لاستعمالها في حدود ما يسمح به القانون.

Faculty of Mathematics and Computer Science

Department of Mathematics

university of Msila.

Lecture Notes for

Mathematical logic

Courses and Tutorials for Mathematical logic of the second-year Bachelor's in Mathematics

Author | **kheir.saadaoui**

Mail |
kheir.saadaoui@univ-msila.dz

2024/2025

Contents

1 Introduction **1**

1.1 Introduction . . . 1

1.1.1 Objectives of Teaching . . . 1

1.2 Elements of Mathematical Language . . . 1

1.3 Writing Mathematical Proofs . . . 3

1.3.1 Deductive Reasoning . . . 3

1.3.2 Proof by Contradiction . . . 3

1.3.3 Proof by Contrapositive . . . 4

1.4 Mathematical Theories . . . 4

1.5 Logical Connectors . . . 6

1.6 Logical Quantifiers . . . 8

1.6.1 Negation Rules . . . 9

1.7 Proof Methods . . . 10

2 Propositional Calculus **11**

2.1 Alphabet and Word . . . 11

2.2 Syntax of Propositional Formulas . . . 12

2.3 Principle of Indication on the Set of Formulas . . . 15

2.4 The Interpretation of a Logical Formula . . . 16

2.4.1 Decomposition Tree of a Formula . . . 16

2.4.2 Substitution in a Formula . . . 19

2.5 Semantics . . . 21

2.6 Tautologies and Logical Equivalences . . . 25

2.6.1 Normal Forms . . . 29

2.7 Complete Systems of Connectors . . . 29

2.7.1 Normal Forms . . . 31
2.8 Complete Systems of Connectives . . . 35
2.8.1 Theories . . . 35

3 Predicate Calculus **37**
3.1 Syntax of Predicate Calculus . . . 37
3.1.1 First-Order Alphabet . . . 37
3.1.2 Terms . . . 38
3.1.3 Formula . . . 39
3.2 Free and Bound Variables . . . 40
3.2.1 Scope of a Quantifier . . . 41
3.2.2 Substitution in Terms . . . 41
3.2.3 Substitution in Formulas . . . 42
3.3 Semantics of Predicate Calculus . . . 42
3.3.1 Definition of a Structure . . . 43
3.3.2 Satisfaction of a Formula in a Structure . . . 46

4 Axiomatic of Z F and AC **51**
4.1 Paradoxes, Naive Set Theory . . . 51
4.1.1 Russell's Paradox . . . 52
4.1.2 The Barber Paradox . . . 53
4.1.3 The Liar Paradox . . . 54
4.1.4 Cantor's Paradox . . . 56
4.1.5 Richard's Paradox . . . 57
4.1.6 Grelling's Paradox . . . 59
4.2 Zermelo-Fraenkel Axioms (ZF) . . . 61
4.2.1 Axiom of Extensionality . . . 61
4.2.2 Axioms of Construction . . . 61
4.2.3 Zermelo's Set Theory . . . 65
4.2.4 Zermelo-Fraenkel Set Theory . . . 65
4.3 Axiom of Choice (AC) . . . 66
4.3.1 Axiom of Choice . . . 66
4.3.2 Some Equivalent Forms . . . 66
4.3.3 Zorn's Lemma . . . 67
4.3.4 Applications of the Axiom of Choice . . . 69

4.3.5 Independence of the Axiom of Choice . . . 70
4.4 Exercises . . . 70

5 Well-Ordering and Proof by Induction **72**
5.1 Proof by Induction . . . 72
5.1.1 Simple Induction Proof . . . 72
5.1.2 Proof Schema Using the Well-Ordering Principle . . . 73
5.1.3 Generalized Proof by Induction . . . 75
5.1.4 Strong Induction . . . 76
5.1.5 Special Case of Proof by Induction (Cauchy's Induction) . . . 77
5.1.6 Proof of the Cauchy-Schwarz Inequality by Induction . . . 77
5.2 Well-Founded Order . . . 77
5.2.1 Order and Strict Order . . . 77
5.2.2 Minorants, Majorants, Minimizers, and Maximizers . . . 79

Bibliography **81**

Chapter 1

Introduction

1.1 Introduction

1.1.1 Objectives of Teaching

To acquire the fundamentals of mathematical reasoning, the foundations of set theory, and the elements of mathematical proof writing.

1.2 Elements of Mathematical Language

Axiom. An axiom is a statement assumed to be true a priori and is not subject to proof.

For example, Euclid formulated five axioms ("Euclid's five postulates"), which he did not attempt to prove and were to form the basis of (Euclidean) geometry. The fifth of these axioms states: "Through a point not on a line, there is exactly one line parallel to that line."

Another example of axioms is provided by the (five) Peano axioms. These define the set of natural numbers. The fifth axiom asserts: "If P is a subset of $\mathbb{N}$ containing 0 and such that the successor of each element of P is in P (the successor of n is $n+1$), then $P = \mathbb{N}$." This axiom is known as the "axiom of induction" or "recurrence axiom."

These statements are commonly accepted as "obvious" by everyone.

Proposition1.1 (or assertion or statement). A proposition is a statement that can be either true or false. For example, "every prime number is odd" and "every square of a real number is a positive real number" are two propositions. It is easy to prove that the first is false and the second is true. The term proposition is clear: something is proposed, but it remains to be proven.

Theorem1.1. A theorem is a true proposition (and in any case, proven as such). In common practice, the term proposition often refers to an intermediate or lesser important theorem, and there is a tendency to refer to most theorems as propositions, reserving the term theorem for the more significant ones (e.g., the Pythagorean Theorem). This is the perspective we will adopt in later chapters (though not in this first chapter, where the term "proposition" would have two different meanings).

Corollary. A corollary to a theorem is a theorem that follows as a consequence of that theorem. For example, in the chapter on "continuity," the intermediate value theorem states that the image of an interval of $\mathbb{R}$ by a continuous real-valued function is an interval in $\mathbb{R}$. A corollary of this theorem asserts that if a function defined and continuous on an interval of $\mathbb{R}$ takes at least one positive value and at least one negative value, then the function must have at least one root in that interval.

Lemma1.1. A lemma is a preparatory theorem used to establish a more significant theorem.

Conjecture. A conjecture is a proposition believed to be true without being proven. Conjectures drive mathematical progress. A mathematician may suspect that an important result is true and state it without being able to prove it, leaving the mathematical community to either confirm it with a convincing proof or disprove it. The following conjectures are famous:

- (Fermat's conjecture) If n is an integer greater than or equal to 3, there are no non-zero natural numbers x, y, and z such that $x^n + y^n = z^n$. (This conjecture dates back to the 17th century and was recently proven true.)

Definition1.1. A definition is a statement that describes the characteristics of an object. It should be noted that the term "axiom" is sometimes synonymous with "definition." For example, when you read "definition of a vector space," you might just as well read "axioms of vector space structure," and vice versa.

1.3 Writing Mathematical Proofs

1.3.1 Deductive Reasoning

The schema of deductive reasoning is as follows:

When P is a true proposition, and $P \Rightarrow Q$ is a true proposition, one can assert that Q is a true proposition.

A result known to be true (i.e., a theorem) can only lead to another true result. This rule is known as "modus ponens." It is the basic reasoning that you will reproduce many times. In fact, you will employ this reasoning so often (or find yourself so frequently in the situation where the hypothesis P is true) that you might eventually confuse the simple phrase "$P \Rightarrow Q$ is true" with the more complete phrase "P is true, and $P \Rightarrow Q$ is true." Only the latter allows you to assert that Q is true.

Given that implication is transitive, a proof often takes the following form: P is true, and $P \Rightarrow Q \Rightarrow R \Rightarrow \ldots \Rightarrow S \Rightarrow T$ is true, and thus we have shown that T is true.

1.3.2 Proof by Contradiction

To show that a proposition P is true, we assume its negation $\bar{P}$ is true and demonstrate that this leads to a false proposition. We then conclude that P must be true (since Q is false, the implication $\bar{P} \Rightarrow Q$ can only be true if $\bar{P}$ is false, or equivalently, if P is true). The structure of proof by contradiction is as follows:

When $\bar{P} \Rightarrow Q$ is a true proposition, and Q is a false proposition, we can assert that P is a true proposition.

Example. Let's prove that $\sqrt{2}$ is irrational. Assume, by contradiction, that $\sqrt{2} \in \mathbb{Q}$. Then, there exist two non-zero natural numbers a and b such that $\sqrt{2} = \frac{a}{b}$, or equivalently $a^2 = 2b^2$. Now, in the prime factorization of the integer a^2 (which is evidently greater than 2), the prime number 2 appears with an even exponent (if $a = 2^\alpha \times \ldots$, then $a^2 = 2^{2\alpha}$), while it appears with an odd exponent in $2b^2$ (if $b = 2^\beta \times \ldots$, then $2b^2 = 2^{2\beta+1} \times \ldots$). If we accept the uniqueness of prime factorization for natural numbers greater than 2 (a uniqueness that will be demonstrated later in this course), the equality $a^2 = 2b^2$ is impossible. Therefore, the initial assumption ($\sqrt{2} \in \mathbb{Q}$) is absurd, and we have thus proven (by contradiction) that $\sqrt{2} \notin \mathbb{Q}$.

1.3.3 Proof by Contrapositive

The structure is as follows:

To show that $P \Rightarrow Q$ is a true proposition, it (is necessary and) suffices to show that $\bar{Q} \Rightarrow \bar{P}$ is a true proposition.

Example. Let k and k' be two non-zero natural numbers. Let's prove that $(kk' = 1 \Rightarrow k = k' = 1)$. Assume that $k \neq 1$ or $k' \neq 1$. Then, we have $k \geq 2$ and $k' \geq 1$ or $k \geq 1$ and $k' \geq 2$. In both cases, $kk' \geq 2$, and in particular, $kk' \neq 1$. Therefore, $(k \neq 1 \text{ or } k' \neq 1) \Rightarrow (kk' \neq 1)$.

- By contrapositive, we have shown that $(kk' = 1) \Rightarrow (k = 1 \text{ and } k' = 1)$.

1.4 Mathematical Theories

At the foundation of a mathematical theory are axioms and definitions:

Definition1.2 (Axiom) An axiom is a mathematical statement accepted without proof.

Example.

- Euclid's parallel postulate.
- Pasch's axiom on the intersection of a triangle and a line.

- Hilbert's axioms for Euclidean geometry.
- Archimedes' axiom for real numbers.
- Peano's axioms for natural numbers.
- Zermelo-Fraenkel axioms for set theory.
- Zorn's lemma (also known as the axiom of choice).

Definition1.3 A definition is arbitrarily assigned to designate a mathematical object.

Example.

- Definitions of a number.
- Definitions of a function.
- Definitions of a derivative.

In a mathematical theory, one finds propositions (assertions), predicates, theorems, lemmas, and conjectures:

Definition1.4 (Assertion) An assertion is a mathematical statement to which a truth value can be assigned: true (1) or false (0), but never both simultaneously.

Example.

- The statement "Algiers is the capital of Algeria" is true.
- The statement "24 is a multiple of 2" is true.
- The statement "19 is a multiple of 2" is false.

Definition1.5 (Predicate) A predicate is an assertion that contains variables.

Example.

- The following statement: $P(n)$: "n is a multiple of 2" is a predicate because it becomes an assertion when a value is assigned to n.
- $P(10)$: "10 is a multiple of 2" is a true assertion.

- $P(11)$: "11 is a multiple of 2" is a false assertion.
- $Q(x, A)$: "$x \in A$" is a predicate with two variables; $Q(1, \mathbb{N})$ is true, $Q(\sqrt{2}, \mathbb{Q})$ is false.

Definition1.6 (Lemma) A lemma is a result of minor importance.

Definition1.7 (Theorem) A theorem is a result of major importance.

Definition1.8 (Conjecture) A conjecture is a proposition that has been verified in several cases, but has not yet been proven.

Example.

- Fermat's conjecture on the following Diophantine equation with unknowns x, y, and z: $n \in \mathbb{N}, x^n + y^n = z^n$. It asserts that there is no non-trivial solution if the parameter $n > 2$. But it was not until 1996, with the work of the English mathematician Andrew Wiles, that a definitive answer was found.
- The Riemann conjecture on the non-trivial zeros of the zeta function: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^*}$ (an unresolved conjecture).
- Bertrand's conjecture on prime numbers within the intervals $[n, 2n]$.

1.5 Logical Connectors

Let P and Q be two propositions:

Statement. not P

Notation. $\neg P$

The assertion $\neg P$ is true means that P is false.

Statement. P and Q

Notation. $P \wedge Q$

The assertion $P \wedge Q$ is true if both P and Q are true; $P \wedge Q$ is false otherwise.

Statement. P or Q

Notation. $P \vee Q$

The assertion $P \vee Q$ is true if at least one of the assertions P or Q is true; $P \vee Q$ is false if both P and Q are false.

Statement. $\left\{ \begin{array}{c} \text{if } P\text{, then } Q \\ P \text{ implies } Q \\ P \text{ is a sufficient condition for } Q \\ Q \text{ is a necessary condition for } P \end{array} \right\}$

Notation. $P \Longrightarrow Q, P \longrightarrow Q$

The assertion $P \Longrightarrow Q$ is true means that it is excluded that P is true without Q being true.

Statement. $\left\{ \begin{array}{c} P \text{ is equivalent to } Q \\ P \text{ if and only if } Q \end{array} \right\}$

Notation. $P \Longleftrightarrow Q, P \longleftrightarrow Q, P \equiv Q$

The assertion $P \Longleftrightarrow Q$ is true means that:

$$(P \Longrightarrow Q) \text{ and } (Q \Longrightarrow P) \text{ are true.}$$

This is summarized in the truth tables below:

$\neg P$	P
0	1
1	0

P	Q	$P \wedge Q$	$P \vee Q$	$P \Longrightarrow Q$	$P \Longleftrightarrow Q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Properties1.1

- $P \wedge (Q \vee Q) \equiv (P \wedge Q) \vee (P \wedge Q)$; double distributivity of "and" and "or."
- $P \vee (Q \wedge Q) \equiv (P \vee Q) \wedge (P \vee Q)$.
- $(P \Longrightarrow Q) \equiv (\neg Q \Longrightarrow \neg P)$; contrapositive.
- $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$; De Morgan's law.
- $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$.
- $P \Longrightarrow Q \equiv \neg P \vee Q$.
- $\neg(P \Longrightarrow Q) \equiv P \wedge \neg Q$.

1.6 Logical Quantifiers

Statement. For all or for every.

Notation. $\forall \quad (\forall x P(x))$

Statement. There exists at least one or there exists.

Notation. $\exists \quad (\exists x P(x))$

Example.

- The proposition $\forall x \in [-3, 1], x^2 + 2x - 3 \leq 0$ is true.
- The proposition $\forall n \in \mathbb{N}, (n^2 \text{ even }) \Longrightarrow (n \text{ even })$ is true.
- The proposition $\exists x \in \mathbb{R}, x^2 = 4$ is true.
- The proposition $\exists! x \in \mathbb{R}_+^*, \ln x = 1$ is true.

Remark.

- The proposition $\exists x \in E, P(x)$ means that

$$\exists x((x \in E) \wedge P(x))$$

  and is read as follows: "There exists an element x belonging to E such that $P(x)$ is true."

- The proposition $\forall x \in E, P(x)$ means that

$$\forall x(x \in E \Longrightarrow P(x))$$

  and is read as follows: "If for all (or every) x belonging to E, $P(x)$ is true."

- If there exists exactly one x in E such that $P(x)$ is true, one can write $\exists! x \in E, P(x)$.

- If $\forall x \in E, P(x)$ is true, then $\exists x \in E, P(x)$ is true.

Remark. (Caution) $\exists!$ does not denote a quantifier. Indeed:

$$(\exists! x \in E, P(x)) \equiv (R_1 \wedge R_2)$$

with $R_1 =$ existence and $R_2 =$ uniqueness.

- Two identical quantifiers can be swapped.
- Do not swap two different quantifiers.

1.6.1 Negation Rules

Let $P(x)$ be a predicate on E. Clearly, we have:

- $\neg(\forall x \in E, P(x)) \equiv \exists x \in E, \neg P(x)$.

- $\neg(\exists x \in E, P(x)) \equiv \forall x \in E, \neg P(x)$.

Example.

- The negation of $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}_+, 1 + nx \leq (1 + x)^n$ is $\exists n \in \mathbb{N}, \exists x \in \mathbb{R}_+, 1 + nx > (1 + x)^n$.

- The negation of $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 5$ is $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \neq 5$.

Remark. (Caution) We also verify that:

$$\neg(\exists! x \in E, P(x)) \equiv (\neg R_1 \vee \neg R_2)$$

with R_1 = existence and R_2 = uniqueness.

- Identical quantifiers can be swapped.
- Do not swap different quantifiers.

1.7 Proof Methods

To perform a proof (or reasoning), one follows a process that allows the transition from propositions assumed to be true (as hypotheses) to a proposition called the conclusion, using logical rules.

Chapter 2

Propositional Calculus

2.1 Alphabet and Word

Let A be any set (finite or infinite). The elements of A are called letters, and A itself is called an alphabet.

Definition 2.1. A word over the alphabet A is a finite sequence of elements from A:

$$U = U_1 U_2 \dots U_n$$

where n is the length of the word U.

The set of words over A is denoted by A^*.

On A^*, the concatenation operation is defined as follows:

$$A^* \times A^* \longrightarrow A^*$$

$$(U, V) \longmapsto U \cdot V = U_1 \cdot U_2 \dots U_n \cdot V_1 \cdot V_2 \dots V_m$$

where $U = U_1 \dots U_n$ and $V = V_1 \dots V_m$.

The length of a word defines a function:

$$l : A^* \longrightarrow \mathbb{N}$$

$$U \longmapsto l(U) = n = \text{length of } U$$

Concatenation is an associative operation and has the empty word ε as its neutral element:

$$u \cdot \varepsilon = \varepsilon \cdot u = u$$

In other words, A^* is a monoid.

Definition 2.2. We say that $a \in A$ has an occurrence in the word u if a is a letter of u, i.e., if $u = u_1 u_2 \dots u_n$, then $\exists k \in \{1, 2, \dots, n\}$ such that $a = u_k$.

Remark. There may be multiple occurrences of a in u.

Example.

$$A = \{a, b \dots x, y, z\}$$

$$u = abaab$$

$$l(u) = 5$$

The letter a has three occurrences in u, and b has two.

Properties 2.1.

- $l(uv) = l(u) + l(v)$
- $uv = uw \Rightarrow v = w$
- $uv = vw \Rightarrow u = w$

Definition 2.3. The word u is a prefix of the word v if there exists a word w such that $v = uw$.

The word u is a suffix of v if there exists a word w such that $v = wu$.

2.2 Syntax of Propositional Formulas

Definition 2.4. The propositional connectors are the symbols:

$\neg$: for negation (not)

$\wedge$: for conjunction (and)

$\vee$: for disjunction (or)

$\longrightarrow$: for implication

$\longleftrightarrow$: for equivalence

Let P be a non-empty set of elementary or atomic propositions. The elements of P are denoted by p, q, r, s.

Remark.

1- In elementary logic, a proposition is a statement that communicates facts, e.g., $p =$ "It is raining," $q =$ "The weather is nice."

2- P does not contain the connectors $\neg, \wedge, \vee, \longrightarrow, \longleftrightarrow$; we consider the following alphabet: $A = P \cup \{\neg, \wedge, \vee, \longrightarrow, \longleftrightarrow\} \cup \{()\}$.

Let A^* be the set of words over A:

$$(p \longrightarrow q) \in A^*$$

$$(p \in A^*)$$

$$p \in A^*$$

$$() \in A^*$$

$$(pq\wedge) \in A^*$$

Definition 2.5. The set $\mathcal{F}$ of propositional formulas is the smallest subset of A^* that satisfies:

1- $P \subseteq \mathcal{F}$ (every elementary proposition is a formula).

2- If $F \in \mathcal{F}$, then $\neg F \in \mathcal{F}$.

3- If $F, G \in \mathcal{F}$, then $(F * G) \in \mathcal{F}$ with $* \in \{\wedge, \vee, \longrightarrow, \longleftrightarrow\}$.

Remark.

1- Formulas are sequences of symbols without any inherent meaning. Assigning a meaning, i.e., a truth value ("true" or "false") to a formula constitutes its semantics.

2- The term "smallest" is to be understood in terms of set inclusion. $\mathcal{F}$ is therefore the intersection of all subsets of A^* that satisfy properties 1, 2, and 3. This intersection is non-empty because A^* itself satisfies these properties, so $\mathcal{F} = \bigcap_{Y \subseteq A^*} Y$, where Y satisfies properties 1, 2, and 3.

Examples.

- $(\neg p \longrightarrow q)$ is a formula.

- $(p \wedge q \wedge r)$ is not a formula.
- $(\neg p \longrightarrow q)$ is a formula.
- p is a formula.
- $(p \longrightarrow q \vee r)$ is not a formula.

Definition 2.6. The length of a formula F is the number of letters in F: $l(F) = \#$ letters in F.

Example. $F = (p \wedge q)$, then $l(F) = 5$. If $F = p$, then $l(F) = 1$.

Remark There is no formula of length 0.

- It is possible to give a more explicit description of the set $\mathcal{F}$: we will define, by recursion, a sequence $(\mathcal{F}_n)_{n\in\mathbb{N}}$ of subsets of A^*. We set $\mathcal{F}_0 = P$ and for each n:

$$\mathcal{F}_{n+1} = \mathcal{F}_n \cup \{\neg F \mid F \in \mathcal{F}_n\} \cup \{(F * G) \mid F, G \in \mathcal{F}_n, * \in \{\wedge, \vee, \longrightarrow, \longleftrightarrow\}\}$$

  Note that the sequence $(\mathcal{F}_n)_{n\in\mathbb{N}}$ is increasing, i.e., $\mathcal{F}_n \subseteq \mathcal{F}_{n+1}$ for $n \leq m$, so $\mathcal{F}_n \subseteq \mathcal{F}_m$.

Proposition 2.1. $\mathcal{F} = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n$

Proof. Let $Z = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n$:

Z is a subset of A^* that satisfies properties 1, 2, and 3, so $\mathcal{F} \subseteq Z$ (because $\mathcal{F}$ is the smallest subset of A^* that satisfies properties 1, 2, and 3).

Is $Z \subseteq \mathcal{F}$?

We show by induction that for every integer n, we have $\mathcal{F}_n \subseteq \mathcal{F}$.

If $n = 0$, then $P = \mathcal{F}_0 \subseteq \mathcal{F}$ by definition. We assume (induction hypothesis) that $\mathcal{F}_n \subseteq \mathcal{F}$, then $\mathcal{F}_{n+1} \subseteq \mathcal{F}$ according to the definition of $\mathcal{F}_{n+1}$ and the stability properties of $\mathcal{F}$.

Definition 2.7. The height of a formula $F \in \mathcal{F}$ is the smallest integer n such that $F \in \mathcal{F}$. It is denoted $h[F]$: $h(F) = \min\{n \mid F \in \mathcal{F}_n\}$.

Example.

- $F = p$, then $h(F) = 0$.

- $F = (p \wedge q)$, then $h(F) = 1$.
- $F = \neg p$, then $h(F) = 1$.
- $F = (\neg p \wedge q)$, then $h(F) = 2$.

2.3 Principle of Indication on the Set of Formulas

Suppose we want to demonstrate that a certain proposition $Q(F)$ holds for all $F \in \mathcal{F}$. We can do this by reasoning by induction (in the usual sense) on the height of F: we will then need to show, first, that $Q(F)$ is true for every formula F belonging to $\mathcal{F}_0$, and then that if $Q(F)$ is true for all $F \in \mathcal{F}_n$, then $Q(F)$ is also true for every $F \in \mathcal{F}_{n+1}$ for all $n \in \mathbb{N}$.

Principle. If Q verifies:

1) $Q(p)$ is true $\forall p \in P$ i.e., ($Q(F)$ is true for $F \in \mathcal{F}_n$).

2) $Q(F)$ is true $\Rightarrow Q(\urcorner F)$ is true.

3) $Q(F)$ is true and $Q(G)$ is true $\Rightarrow Q(F * G)$ is true for $* \in \{, , \wedge, \vee, \Rightarrow, \Leftarrow\}$, then $Q(F)$ is true $\forall F \in \mathcal{F}$.

Example. $Q(F)$: "F has an equal number of opening and closing parentheses" i.e., $Q(F) =$ "$O(F) = f(F)$". We show that $Q(F)$ is true, $\forall F \in \mathcal{F}$. For this, let us define: $O(F) = \sharp$ opening parentheses, $f(F) = \sharp$ closing parentheses.

1) Let $F = p \in P$, $O(F) = f(F) = 0$, therefore $Q(p)$ is true.

2) We assume that $Q(F)$ is true $\Rightarrow Q(\urcorner F)$ is true.

$$O(F) = f(F)$$

$$O(\urcorner F) = O(F) = f(F) = f(\urcorner F) \text{ i.e., } O(\urcorner F) = f(\urcorner F) \text{ i.e., } Q(\urcorner F) \text{ is true.}$$

3) Let us assume that:

$$\left.\begin{array}{l} O(F) = f(F) \text{ and } O(G) = f(G) \\ O((F * G)) = O(F) + O(G) + 1 \\ f((F * G)) = f(F) + f(G) + 1 \end{array}\right\} \Rightarrow O((F*G)) = f((F*G)) \text{ hence } Q((F*G)) \text{ is true.}$$

Its Formulas.

We define the set $sf(F)$ of the subformulas of F by:

- If $F = p$, $sf(F) = \{F\}$
- If $F = \rceil G$, $sf(F) = \{sf(G)\} \cup \{F\}$.
- If $F = (G * H)$, $sf(F) = \{sf(G)\} \cup \{sf(H)\} \cup \{F\}$.

Example.

$$F = \rceil((\underbrace{(p \Rightarrow q)}_{G} \wedge r) \Longleftrightarrow \underbrace{s}_{H})$$

$$= \rceil \underbrace{(G \Longleftrightarrow H)}_{K} = \rceil K$$

$$sf(F) = sf(\rceil K) = sf(K) \cup \{F\}$$

$$K = (G \Longleftrightarrow H)$$

$$sf(K) = sf(G) \cup sf(H) \cup \{K\}$$

$$H = s, \, therefore : \, sf(H) = \{s\}$$

$$G = (\underbrace{(p \Rightarrow q)}_{G_1} \wedge \underbrace{r}_{G_2}) = (G_1 \wedge G_2)$$

$$sf(G) = sf(G_1 \wedge G_2) = sf(G_1) \cup sf(G_2) \cup \{G\}$$

$$sf(G_2) = \{r\}$$

$$G_1 = (p \Rightarrow q) \, therefore, \; sf(G_1) = sf(p \Rightarrow q) = \{p \, , \, q\} \cup \{p \Rightarrow q\}$$

$$sf(F) = \{p, \, q, \, r, \, s, \, (p \Rightarrow q), \, (p \Rightarrow q) \wedge r, \, ((p \Rightarrow q) \wedge r) \Longleftrightarrow s, \, F\}$$

2.4 The Interpretation of a Logical Formula

2.4.1 Decomposition Tree of a Formula

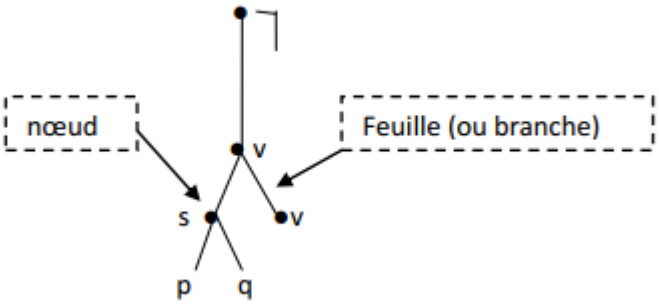
The tree A_F of the formula F is defined by recursion on F.

- • If $F = p$, then $A_F = {}^0p$.

- • If $F = \rceil G$, then $A_F = q_{A_G}^{\neg}$.
- • If $F = (G * H)$, then $A_F = \overset{*}{\underset{A_G \quad A_H}{\wedge}}$

  Where: $*$ can be any of the logical operators: $=, \wedge, \vee, \Rightarrow, \Longleftrightarrow$

Example. $F = \rceil ((p \wedge q) \vee q)$



Example. $M = (((A \wedge (\rceil B \Rightarrow \rceil A)) \wedge (\rceil B \vee \rceil C)) \Rightarrow (C \Rightarrow \rceil A))$

Let us define: $M_0 = ((A \wedge (\rceil B \Rightarrow \rceil A)) \wedge (\rceil B \vee \rceil C))$ *and* $M_1 = (C \Rightarrow \rceil A)$

We first observe that M can be written as $(M_0 \Rightarrow M_1)$

Next, define: $M_{00} = (A \wedge (\rceil B \Rightarrow \rceil A))$, $M_{01} = (\rceil B \vee \rceil C)$, $M_{10} = C$, $M_{11} = \rceil A$

We write $M_0 = (M_{00} \wedge M_{01})$ *and* $M_1 = (M_{10} \Rightarrow M_{11})$ and proceed by successively defining:

- $M_{000} = A$
- $M_{001} = (\rceil B \Rightarrow \rceil A)$
- $M_{010} = \rceil B$
- $M_{011} = \rceil C$
- $M_{110} = A$
- $M_{0010} = \rceil B$
- $M_{0011} = \rceil A$
- $M_{0100} = B$
- $M_{0110} = C$

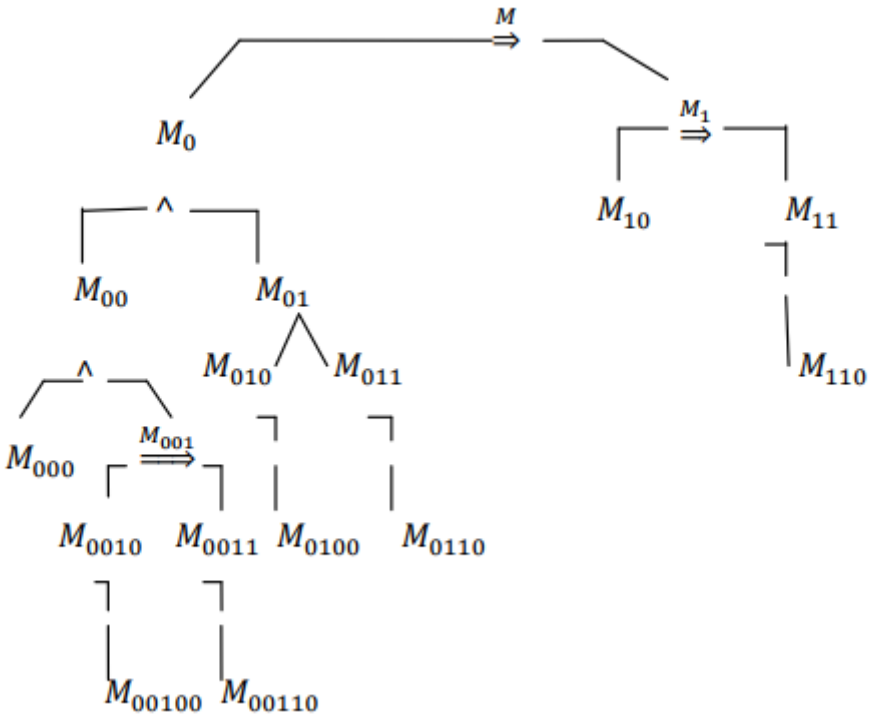
- $M_{00100} = B$
- $M_{00110} = A$

So that:

$M_{00} = (M_{000} \wedge M_{001})$, $M_{01} = (M_{010} \vee M_{011})$, $M_{11} = \rceil M_{110}$, $M_{001} = (M_{0010} \Rightarrow M_{0011})$,

$M_{010} = \rceil M_{0100}$, $M_{011} = \rceil M_{0110}$, $M_{0010} = \rceil M_{00100}$ *and* $M_{0011} = \rceil M_{00110}$

$h(M) = 5$ i.e., $M \in \mathcal{F}_s$.

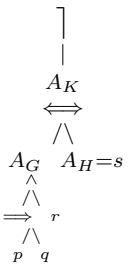


Definition 2.8. The height of a tree is the maximum number of leaf nodes from the root to one end of the tree; in Example 1, $h(F) = 3$.

Example. $F = \rceil (((\underbrace{(p \Rightarrow q)}_{G}) \wedge r) \iff \underbrace{s}_{H})$

$F = \rceil (\underbrace{G \iff H}_{K}) = \rceil K$

$A_F = \underset{A_K}{\rceil}$; $K = (G \iff H)$



$h(F) = 4$

Each node n determines a subtree A_n corresponding to a subformula F. Conversely, the tree of each subformula is a subtree of the tree of the formula. Thus:

Subformulas of F = Subtrees of A_F

2.4.2 Substitution in a Formula

Let F be a formula, and let $p_1, p_2, \ldots, p_n$ be elementary propositions. The notation $F[p_1, p_2, \ldots, p_n]$ means that the propositional variables in F are among the p_i, where $i = 1, 2, \ldots, n$.

Example. If $F = (p \iff (p \wedge q))$, we write $F[p, q]$.

Definition 2.9. We denote $F_{\frac{G_1}{p_1},\frac{G_2}{p_2},\ldots,\frac{G_n}{p_n}}$ as the formula obtained by substituting G_i in place of p_i.

Alternative Notation. $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}} = F[G_1, \ldots, G_n]$

Example. If $F = (p \iff (p \wedge q))$ and $G = (q \Rightarrow p)$, then $F_{\frac{G}{p}} = F(G, q) = ((q \Rightarrow p) \iff ((p \Rightarrow q) \wedge q))$

Proposition. The expression $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}$ is also a formula.

Proof. We proceed by induction on the formula F:

- If $F = p$:
  - If $F = p_K$, then $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}} = G_K$
  - If $F = p \neq p_1, p_2, \ldots, p_n$, then $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}} = F$
- If $F = \neg G$, assume $G_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}$ is a formula. Then $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}} = \neg G_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}$ is also a formula.

- If $F = (G * H)$, where $*$ is $\wedge, \vee, \Rightarrow, \Leftrightarrow$, the reasoning is similar.

Theorem 2.1 (Substitution and Evaluations). Let v be a valuation, $F, G_1, G_2, \ldots, G_n$ be formulas, and $p_1, p_2, \ldots, p_n$ be elementary propositions. Define v' as follows:

$$v'(p) = \begin{cases} v(p) & \text{if } p \neq p_1, p_2, \ldots, p_n, \\ \bar{v}(G_i) & \text{if } p = p_i \text{ for } 1 \leq i \leq n. \end{cases}$$

Then $\bar{v}(F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = \bar{v'}(F)$.

Proof.

- If $F = p$:
  - If $p \neq p_i$, then $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}} = F$ and $\bar{v}(F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = \bar{v}(F) = v(F) = v'(F) = \bar{v'}(F)$.
  - If $p = p_i$, then $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}} = G_i$ and $\bar{v}(F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = \bar{v}(G_i) = v'(p_i) = v'(F) = \bar{v'}(F)$.
- If $F = \neg G$ and $\bar{v}(G_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = \bar{v'}(G)$, then $\bar{v}(F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = \bar{v}(\neg G_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = 1 + \bar{v}(G_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = 1 + \bar{v'}(G) = \bar{v'}(\neg G) = \bar{v'}(F)$.
- If $F = (G * H)$ with $*$ being $\wedge, \vee, \Rightarrow, \Leftrightarrow$, similar reasoning applies.

Corollary. If F is a tautology, then $F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}$ is also a tautology.

Proof. For any valuation v, we have $\bar{v}(F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}}) = \bar{v'}(F_{\frac{G_1}{p_1},\ldots,\frac{G_n}{p_n}})$.

Theorem 2.2. Let F be a formula, G a sub-formula of F, and H a formula equivalent to G. Then $F' = F_{\frac{H}{G}}$ is logically equivalent to F.

Proof. By induction on formulas:

- If $F = p$ and $G = F$, then $F' = H$, and hence $F' \sim F$.
- If $F = \neg F_1$, then $G = F$, and hence $H = F'$, and $F \sim F'$. If G is a sub-formula of F_1, then $F_1' = F_{1\frac{H}{G}} \sim F_1$, so $F' = \neg F_1' \sim F$.
- If $F = F_1 * F_2$, where $* = \wedge, \vee, \Rightarrow, \Leftrightarrow$, there are three possibilities:
  - If $G = F$ and $F' = H$, then $F' \sim F$.

– If G is a sub-formula of F_1, then by induction hypothesis, the formula F_1', resulting from substituting H for G in F_1, is logically equivalent to F_1. The formula F' is then $(F_1' * F_2)$, which is logically equivalent to F, because for any valuation v, $\bar{v}(F') = \bar{v}(F_1') \cdot \bar{v}(F_2) = \bar{v}(F_1) \cdot \bar{v}(F_2) = \bar{v}(F)$. Similar reasoning applies to other cases: $* = \vee, \Rightarrow, \Leftrightarrow$.

2.5 Semantics

Definition 2.10. A truth value distribution or valuation v is a function: $v : P \longrightarrow \{0, 1\}$ where P is the set of elementary propositions. We say that v defines a model $\mathcal{M}$ of propositional calculus. The values 0 and 1 represent "true" and "false" and can also be denoted by v and F, where $1 = v$ and $0 = F$. If P has a cardinality n, the number of different truth values is exactly $2^n = 2^{\sharp P}$.

Example. Let $P = \{p, q\}$, then $2^2 = 4$

1 1

1 0

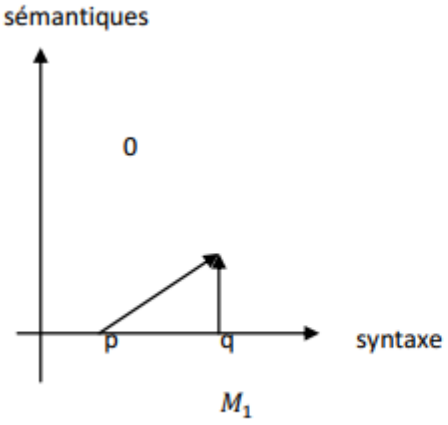
0 1

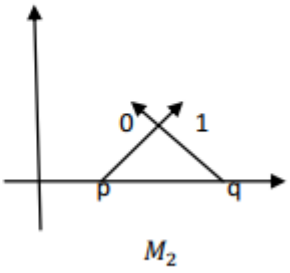
0 0

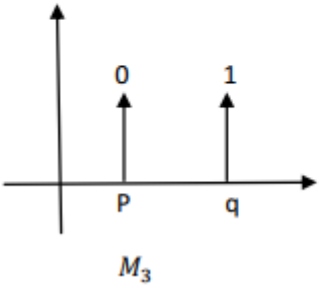
$$v_1 : P \longrightarrow \{0, 1\} \qquad v_2 : P \longrightarrow \{0, 1\}$$
$$p \longrightarrow 1 \qquad p \longrightarrow 1$$
$$q \longrightarrow 1 \qquad q \longrightarrow 0$$

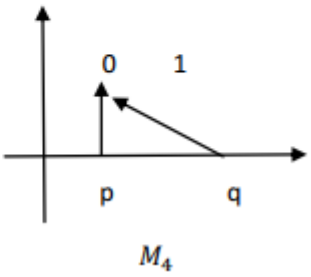
$$v_3 : P \longrightarrow \{0, 1\} \qquad v_4 : P \longrightarrow \{0, 1\}$$
$$p \longrightarrow 0 \qquad p \longrightarrow 0$$
$$q \longrightarrow 1 \qquad q \longrightarrow 0$$

The goal of semantics is to assign truth values to the formulas of propositional calculus for the different valuations defined on the elementary propositions.









Theorem 2.3. For any valuation $v : P \longrightarrow \{0, 1\}$, there exists a unique extension $\bar{v}$: $\mathcal{F} \longrightarrow \{0, 1\}$ $(i.e.\ \bar{v} = v\ on\ P)$ such that:

1) $\bar{v}(\neg F) = 1 \iff \bar{v}(F) = 0.$

2) $\bar{v}((F \wedge G)) = 1 \iff \bar{v}(F) = \bar{v}(G) = 1.$

3) $\bar{v}((F \vee G)) = 0 \iff \bar{v}(F) = \bar{v}(G) = 0.$

4) $\bar{v}((F \Rightarrow G)) = 0 \iff \bar{v}(F) = 1\, and\, \bar{v}(G) = 0.$

5) $\bar{v}((F \Leftrightarrow G)) = 1 \iff \bar{v}(F) = \bar{v}(G).$

Proof. Let $\bar{v}_1$ and $\bar{v}_2$ be two extensions of v, and let $Q(F)$ be the proposition

‘‘$\bar{v}_1(F) = \bar{v}_2(F)$‘‘. We need to show that $Q(F)$ is true for all $F \in \mathcal{F}$

• $If\ F = p : \bar{v_1}(F) = \bar{v_2}(F) = v(F)$ then $Q(F)$ is true.

• *If* $F = \neg G$ *and* $Q(G)$ is true, then:

$$\left.\begin{array}{l} \bar{v_1}(F) = 1 \iff \bar{v_1}(G) = 0 \\ \bar{v_1}(F) = 0 \iff \bar{v_1}(G) = 1 \end{array}\right\} \Longrightarrow \bar{v_1}(F) = \bar{v_2}(F)$$

Hence, $Q(F)$ is also true.

• The same holds for $F = (G * H)$, $* = \wedge, \vee, \Rightarrow, \Leftrightarrow$.

Remark. If we define $+$ *and* $\times$ in $\frac{\mathbb{Z}}{\mathbb{Z}} = \{0\,,\,1\}$ by

$0 + 0 = 0$ $\qquad$ $0 \times 0 = 0$

$0 + 1 = 1$ $\qquad$ $0 \times 1 = 0$

$1 + 0 = 1$ $\qquad$ $1 \times 0 = 0$

$1 + 1 = 0$ $\qquad$ $1 \times 1 = 1$

the conditions 1) *and* 5) become:

1) $\bar{v}(\neg F) = 1 + \bar{v}(F)$.

2) $\bar{v}((F \wedge G)) = \bar{v}(F)\,\bar{v}(G)$.

3) $\bar{v}((F \vee G)) = \bar{v}(F) + \bar{v}(G) + \bar{v}(F)\,\bar{v}(G)$.

4) $\bar{v}((F \Rightarrow G)) = 1 + \bar{v}(F) + \bar{v}(F)\,\bar{v}(G)$.

5) $\bar{v}((F \Leftrightarrow G)) = 1 + \bar{v}(F) + \bar{v}(G)$.

These conditions are often written in truth table form for the connectives $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$.

F	$\neg F$
0	1

F	G	$(F \wedge G)$
1	1	1
1	0	0
0	1	0
0	0	0

F	G	$(F \vee G)$
1	1	1
1	0	1
0	1	1
0	0	0

F	G	$(F \Rightarrow G)$
1	1	1
1	0	0
0	1	1
0	0	1

F	G	$(F \Leftrightarrow G)$
1	1	1
1	0	0
0	1	0
0	0	1

Example. $F = \neg(((p \Leftrightarrow q) \vee (p \Rightarrow q) \wedge (r \Leftrightarrow s)) \Rightarrow (p \Rightarrow q))$

Assume that $P = \{p, q, r, s\}$

$$v : P \longrightarrow \{0, 1\}$$

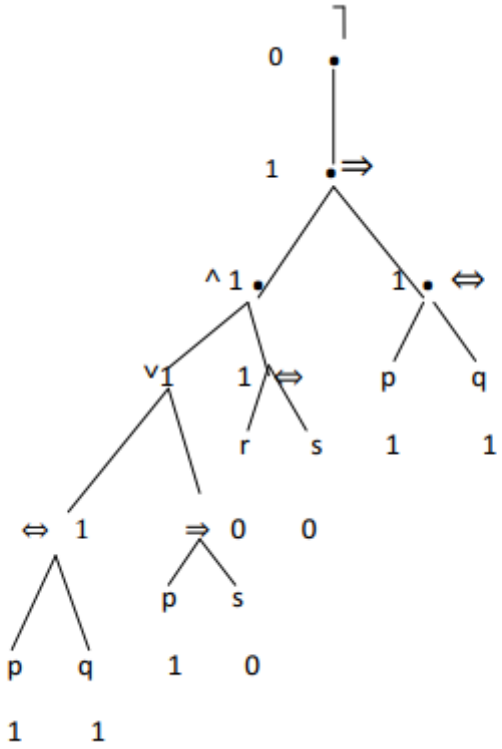
$$p \longrightarrow 1$$

$$q \longrightarrow 1$$

$$r \longrightarrow 0$$

$$s \longrightarrow 0$$

Compute $\bar{v}(F)$, hence: $\bar{v}(F) = 0$



2.6 Tautologies and Logical Equivalences

Let v be a truth value defining a model $\mathcal{M}$ of propositional logic, and let $\bar{v}$ be its extension to formulas.

Definition 2.11.

1) The formula F is said to be satisfied in the model $\mathcal{M}$ if $\bar{v}(F) = 1$, and we denote this as $\mathcal{M} \models F$. Otherwise, it is said to be unsatisfied $\bar{v}(F) = 0$, and we denote this as $\mathcal{M} \not\models F$.

2) F is a tautology if for every model $\mathcal{M}$, we have $\mathcal{M} \models F$, denoted as $\models F$.

Example. $F = (p \vee \neg p)$, $P = \{p\}$. The truth value $\bar{v}_2(F) = 1$. F is an anti-tautology if for every model $\mathcal{M}$, we have $\mathcal{M} \not\models F$, denoted as $\not\models F$.

Example. $F = (p \wedge \neg q)$, $P = \{p\}$, $v_1 : p \longrightarrow 1$, $\bar{v}_1(F) = 0$

, $v_2 : p \longrightarrow 0$, $\bar{v}_2(F) = 0$.

- A tautology is therefore a formula that is always true ($\forall$ valuation).

- An anti-tautology is a formula that is always false.

3) F is logically equivalent to G if $(F \Leftrightarrow G)$ is a tautology, denoted as $F \sim G$. In other words, $\bar{v}(F) = \bar{v}(G)$ for every valuation v.

Example. $F = p,\ F \sim G$, because $(p \Leftrightarrow \neg\neg p)$ is a tautology $G = \neg\neg p$.

Remark.

1) In terms of truth tables, a tautology is a formula that has 1 everywhere in its last column.

- An anti-tautology has 0 everywhere in its last column.

- Two logically equivalent formulas have the same truth tables.

2) $\sim$ defines an equivalence relation on $\mathcal{F}$, with the quotient set $\frac{\mathcal{F}}{\sim} = \{[F], F \in \mathcal{F}\},\ [F] = \{G \in \mathcal{F}/F \sim G\}$ being the equivalence classes of F. When comparing two formulas "for logical equivalence," it means comparing the corresponding classes in $\frac{\mathcal{F}}{\sim}$.

$$\left.\begin{array}{l} F \text{ is a tautology} \iff \forall v,\ \bar{v}(F) = 1 \\ G \text{ is a tautology} \iff \forall v,\ \bar{v}(G) = 1 \end{array}\right\} \iff F \sim G$$

Thus, all tautologies are logically equivalent and form the class 1.

Similarly, all anti-tautologies are logically equivalent and form the class 0.

3) $F = G \Rightarrow F \sim G$.

$F \sim G \not\Rightarrow F = G$.

$F \sim G \Rightarrow [F] = [G]$.

Example. Here are some tautologies in the form of equivalences:

1) Idempotency of conjunction and disjunction

$((p \wedge p) \Leftrightarrow p)$

$((p \vee p) \Leftrightarrow p)$

2) Commutativity of conjunction, disjunction, and equivalence:

$((p \wedge q) \Leftrightarrow (q \wedge p)),\ \ ((p \vee q) \Leftrightarrow (q \vee p)),\ \ ((p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p))$

3) Associativity of conjunction, disjunction, equivalence:

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

$(((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r)))$

4) Distributivity of disjunction/conjunction and vice versa:

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

5) Absorption:

$((p \wedge (p \vee q)) \Leftrightarrow p)$, $((p \vee (p \wedge q)) \Leftrightarrow p)$

6) De Morgan's Laws:

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

7) Contrapositive:

$((p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p))$

8) $(\neg\neg p \Leftrightarrow p)$, $((p \Rightarrow q) \Leftrightarrow (\neg p \vee q))$

Here are non-equivalent formulas:

$(p \wedge p)$ and $(q \wedge q)$ (taking $v(p) = 1$ and $v(q)$)

$(p \Rightarrow p)$ and p (taking $v(p) = 0$)

$(p \Leftrightarrow q)$ and $(p \Rightarrow q)$ (taking $v(p) = 0$, $v(q) = 1$)

$(p \Rightarrow (p \Rightarrow p))$ and $((p \Rightarrow p) \Rightarrow p)$ (taking $v(p) = 0$))

Remark. Thanks to the associativity of $\wedge$ and $\vee$ the following notations can be used: The formula $((F \wedge G) \wedge H)$ will be denoted as $(F \wedge G \wedge H)$.

The formula $((F \vee G) \vee H)$ will be denoted as $(F \vee G \vee H)$. More generally, for any natural number k if F_1, F_2, ..., F_k are formulas, we will represent them as:

$$\underbrace{(F_1 \wedge F_2 \wedge ... \wedge F_k)}_{\bigwedge_{i=1}^{k} F_i} \underset{def}{=} F_1 \wedge (F_2 \wedge (... \wedge F_k...))$$

$$\underbrace{(F_1 \vee F_2 \vee ... \vee F_k)}_{\bigvee_{i=1}^{k} F_i} \underset{def}{=} F_1 \vee (F_2 \vee (... \vee F_k..))$$

In the list below, formulas on the same line are pairwise logically equivalent:

1) $(A \Rightarrow B)$, $(\neg A \vee B)$, $((A \wedge B) \Leftrightarrow A)$, $((A \vee B) \Leftrightarrow B)$.

2) $\neg(A \Rightarrow B)$, $(A \wedge \neg B)$.

3) $(A \Leftrightarrow B)$, $((A \wedge B) \vee (\neg A \wedge \neg B))$, $((\neg A \vee B) \wedge (\neg B \vee A))$.

4) $(A \Leftrightarrow B)$, $((A \Rightarrow B) \wedge (B \Rightarrow A))$, $(\neg A \Leftrightarrow \neg B)$, $(B \Leftrightarrow A)$.

5) $(A \Leftrightarrow B)$, $((A \vee B) \Rightarrow (A \wedge B))$.

6) $\neg(A \Leftrightarrow B)$, $(A \Leftrightarrow \neg B)$, $(\neg A \Leftrightarrow B)$.

7) A, $(A \wedge T)$, $(A \vee T)$, $(A \Leftrightarrow T)$, $(T \Rightarrow A)$.

8) $\neg A$, $(A \Rightarrow \neg A)$, $((A \Rightarrow B) \wedge (A \Rightarrow \neg B))$.

9) $\neg A$, $(A \Rightarrow \bot)$, $(A \Leftrightarrow \bot)$

10) $\bot$, $(A \wedge \bot)$, $(A \Leftrightarrow \neg A)$.

11) T, $(A \vee T)$, $(A \Rightarrow T)$, $(\bot \Rightarrow A)$.

12) $(A \Rightarrow (B \wedge C))$, $((A \Rightarrow B) \wedge (A \Rightarrow C))$.

13) $(A \Rightarrow (B \vee C))$, $((A \Rightarrow B) \vee (A \Rightarrow C))$.

14) $((A \wedge B) \Rightarrow C)$, $((A \Rightarrow C) \vee (B \Rightarrow C))$.

15) $((A \vee B) \Rightarrow C)$, $((A \Rightarrow C) \wedge (B \Rightarrow C))$.

Note. From lines 12) to 15) it can be observed that there is no distributivity of implication with respect to conjunction or disjunction. However, distributivity is present on the left side in 12) and 13), i.e., when the "$\wedge$" or "$\vee$" is on the right side of the $\Rightarrow$. In cases 14) and 15), there is a sort of false distributivity where "$\wedge$" (or $\vee$) is transformed into "$\vee$" (or $\wedge$).

Theorem 2.4 (Substitutions and Evaluation) Let v be an evaluation, F, G_1, G_2, ..., G_n be formulas, and p_1, p_2, ..., p_n be elementary propositions.

Let v' be the evaluation defined by:

$$v' = \begin{cases} v(p) \text{ if } p \neq p_1, p_2, ..., p_n. \\ \bar{v}(G_i) \text{ if } p = p_i \ (1 \leq i \leq n) \end{cases}$$

Then: $\bar{v}(F_{\frac{G_1}{p_1} \cdots \frac{G_n}{p_n}}) = \bar{v'}(F)$.

Proof. We proceed by induction on formulas:

* If $F = p$,

  - If $p \neq p_i$ then $F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}} = F$ and $\bar{v}(F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v}(F) = v(F) = v'(F) = \bar{v'}(F)$.

  - If $p = p_i$ then $F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}} = G_i$ and $\bar{v}(F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v}(G_i) = v'(p_i) = v'(F) = \bar{v'}(F)$.

* If $F = \neg G$,

  $\bar{v}(G_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v'}(G)$
  $\bar{v}(F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v}(\neg G_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = 1 + \bar{v}(G_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = 1 + \bar{v'}(G) = \bar{v'}(\neg G) = \bar{v'}(F)$.

* If $F = G \wedge H$,

  $\bar{v}(G_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v'}(G)$ and $\bar{v}(H_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v'}(H)$
  $\bar{v}(F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v}((G_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) \wedge (H_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}})) = \bar{v}(G) \cdot \bar{v}(H) = \bar{v'}(G) \cdot \bar{v'}(H) = \bar{v'}(G \wedge H) = \bar{v'}(F)$.

* Similar reasoning applies to other cases.

Corollary. If F is a tautology, then the formula $F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}$ is also a tautology.

Proof: For any evaluation v we have: $\bar{v}(F_{\frac{G_1}{p_1}\cdots\frac{G_n}{p_n}}) = \bar{v'}(F) = 1$.

2.6.1 Normal Forms

2.7 Complete Systems of Connectors

Definition 2.12.

1) For any n-tuple $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in \{0, 1\}^n$, we denote by $V_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$ the valuation defined by $V^{(p_i=\varepsilon_i)}_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$ for all $i \in \{1, 2, ..., n\}$

2) For each propositional variable p and each element $\varepsilon \in \{0, 1\}$, we denote by ε_p the formula:

$$\varepsilon_p = \begin{cases} p \text{ if } \varepsilon = 1 \\ \neg p \text{ if } \varepsilon = 0 \end{cases}$$

3) For any formula F we denote by $\Delta(F) = \{v \in \{0\,,\,1\}^P \,|\, \bar{v}(F) = 1\}$ the set of valuations such that the formula F defines a function:

$$\varnothing_F : \{0\,,\,1\}^n \longrightarrow \{0\,,\,1\}$$
$$(\varepsilon_1,\, \varepsilon_2,\, ...,\, \varepsilon_n) \longmapsto \bar{v}_{\varepsilon_1,\,\varepsilon_2,\,...,\,\varepsilon_n}(F)$$

$\varnothing_F$ is compatible with the logical equivalence relation. In other words, $F \sim G \Leftrightarrow \varnothing_F = \varnothing_G$. Thus, $\varnothing_F$ defines, by quotienting, a function:

$$\varnothing : \frac{\mathcal{F}}{\sim} \longrightarrow \{0\,,\,1\}^{(0\,,\,1)^n}$$
$$.[F] \longmapsto \varnothing_F$$

where $[F]$ is the equivalence class of the formula F with respect to the relation $\sim$.

Theorem 2.5 $\varnothing$ is a bijection.

Proof.

1) $\oslash$ **Injectivity:** Let $[F]$, $[G]$ be two classes of formulas

$\varnothing([F]) = \varnothing([G]) \Rightarrow \varnothing_F = \varnothing_G \Leftrightarrow F \sim G \Leftrightarrow [F] = [G]$.

Thus: $\varnothing$ is injective.

2) $\varnothing$ **Surjectivity:** Let $\varnothing : \{0\,,\,1\}^n \longrightarrow \{0\,,\,1\}$. We need to find if there exists an $F \in \mathcal{F}$ such that $\varnothing = \varnothing_F$?

$*$ If $\varnothing$ takes only the value 0, then any anti-tautology F satisfies $\varnothing = \varnothing_F$, for example, $F = (p_1 \wedge \neg p_1)$

$*$ Otherwise, the set $x = \varnothing^{-1}(\{1\}) = \{(\varepsilon_1,\, \varepsilon_2, ..., \varepsilon_n) \in \{0,1\}^n \,|\, \varnothing(\varepsilon_1,\, \varepsilon_2, ..., \varepsilon_n) = 1\}$ is non-empty.

Let $F_x = \bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in X} \left(\bigwedge_{1\leq i\leq n} \varepsilon_i\, p_i\right)$, then $\Delta(F_x) = \{\bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in X},\, (\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X\}$ $\circledast$ i.e., $\bar{v}_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}(F_x) = 1 \Leftrightarrow \varnothing(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) = 1$, thus: $\varnothing = \varnothing_{F_x}$

for, $\circledast$ for all $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n)$, $\bigtriangleup \left(\bigwedge_k \varepsilon_k\, p_k\right) = \bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in x}, \bigtriangleup \left(\bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in x} \left(\bigwedge_i \varepsilon_i\, p_i\right)\right) = \{v_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n},\, (\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in x\}$, $\bar{v}\left(\bigwedge_k \varepsilon_k\, p_k\right) = 1 \Leftrightarrow \bar{v}\left(\bigwedge_k \varepsilon_k\, p_k\right) = 1 \Leftrightarrow v(p_k) = v_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}(p_k)$.

Corollary. If $\sharp p = n$ then there are exactly 2^{2^n} classes of formulas, each corresponding to a function $\varnothing : \{0\,,\,1\}^n \longrightarrow \{0\,,\,1\}$

Definition 2.12. A function $\varnothing : \{0\,,\,1\}^n \longrightarrow \{0\,,\,1\}$ is called a propositional connector with n places.

Example. We have already seen the connector

1) According to the previous definition, it corresponds to the 2-place connectors.

$$\begin{aligned} \varnothing : \{0\,,\,1\}^2 &\longrightarrow \{0\,,\,1\} \\ (0\,,\,0) &\longmapsto 0 \\ (0\,,\,1) &\longmapsto 0 \\ (1\,,\,0) &\longmapsto 0 \\ (1\,,\,1) &\longmapsto 1 \end{aligned}$$

Or equivalently, to the class of the formula $p_1 \wedge p_2$.

2) An example of a 1-place connector is:

$$\begin{aligned} \varnothing : \{0\,,\,1\} &\longrightarrow \{0\,,\,1\} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 0 \end{aligned}$$

It corresponds to the class of $\neg p_1$ and is thus the usual connector $\neg$.

3) The following 2-place connector is called the "NAND" connector:

$$\begin{aligned} \varnothing : \{0\,,\,1\}^2 &\longrightarrow \{0\,,\,1\} \\ (0\,,\,0) &\longmapsto 1 \\ (0\,,\,1) &\longmapsto 0 \\ (1\,,\,0) &\longmapsto 0 \\ (1\,,\,1) &\longmapsto 0 \end{aligned}$$

which corresponds to the formula $\neg(p_1 \wedge p_2)$.

2.7.1 Normal Forms

Definition 2.13. A formula F is said to be in canonical disjunctive normal form (CDNF) if there exists a non-empty subset $X \subseteq \{0\,,\,1\}^n$ such that $F = \bigvee_{(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n)\in X} \left(\bigwedge_{1\leq i\leq n} \varepsilon_i\, p_i \right)$.

It is said to be in disjunctive normal form (DNF) if there exist:

$*$ An integer $m \geq 1$

$*$ Integers $k_1, ..., k_m \geq 1$

$*$ For $1 \leq i \leq m$, variables $p_{i_1}, p_{i_2}, ..., p_{ik_i}$ and k_i elements $\varepsilon_{i_1}, ..., \varepsilon_{k_i}$ from $\{0\,,\,1\}$ such that:

$$F = \bigvee_{1 \leq i \leq m} (\varepsilon_{i_1} p_{i_1} \wedge \varepsilon_{i_2} p_{i_2} \wedge ... \wedge \varepsilon_{ik_i} p_{ik_i})$$

Similarly, conjunctive normal forms (CNF) and canonical conjunctive normal forms (CCNF) are defined (by swapping the symbols for disjunction and conjunction).

Remark. A CDNF is a DNF. Similarly, a CCNF is a CNF

$(n = k_i, \forall\, i, p_{ij} = p_j)$

Theorem 2.6 Every formula F is logically equivalent to a CNF and a DNF. The NAND connector: "or" $\rceil\,(p_1 \vee p_2) = (p_1 \vee p_2)$ $\vee$: NAND connector "or".

p_1	p_2	F
1	1	0
1	0	0
0	1	0
0	0	1

$\varnothing_F : \{0\,,\,1\}^2 \longrightarrow \{0\,,\,1\}$

$\{0\,,\,1\}^2 = \{(0,0)\,,\,(0,1)\,,\,(1,0)\,,\,(1,1)\}$

$(0,0) \longmapsto 1,\ (0,1) \longmapsto 0$

$F = \rceil\,(p_1 \wedge p_2) \underset{def}{=} (p_1\ p_2)$

$\wedge$: NAND connector "and"

$$\varnothing = \varnothing_F : \{0\,,\,1\}^2 \longrightarrow \{0\,,\,1\}$$
$$(0,0) \longmapsto 1$$
$$(0,1) \longmapsto 1$$

An n-place connector is a function $\varnothing\,\{0\,,\,1\}^n \longrightarrow \{0\,,\,1\}$.

p_1	p_2	$\rceil(p_1 \wedge p_2)$
1	1	0
1	0	1
0	1	1
0	0	1

Example. $F = ((p_1 \wedge p_2) \Rightarrow p_3)$

$\varnothing\,\{0\,,\,1\}^3 \longrightarrow \{0\,,\,1\}$

$(0,0,0) \longmapsto 1$

$(0,0,1) \longmapsto 1$

$(1,1,0) \longmapsto 0$

$\varnothing$ is a 3-place connector.

Theorem 2.7 (Normal Form) Every formula F is logically equivalent to at least one formula in disjunctive normal form (DNF) and at least one formula in conjunctive normal form (CNF).

Proof. $*$ If F is a tautology, it is logically equivalent to $p_1 \wedge \rceil\, p_1$ which is both a DNF and a CNF. $*$ If F is neither a tautology nor an anti-tautology, then by the previous theorem, there exists $x \neq \varnothing/\varnothing_F = \varnothing_{F_x}$, $x \in \{0\,,\,1\}^n$ i.e.: $F \sim F_x$ which is a CDNF and hence also a DNF. For $\rceil\, F$, there also exists $x'/\rceil\, F \sim F_{x'}$, so: $F = \rceil\rceil\, F \sim \rceil(\vee(\wedge)) = \wedge(\vee) \sim CCNF$ (according to De Morgan's law).

Example. $G = (A \Rightarrow (((B \wedge \rceil\, A) \vee (\rceil\, C \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \rceil\, B))))$ Let $H = (B \wedge \rceil\, A)$, $I = (\rceil\, C \wedge A)$, $J = (A \Rightarrow \rceil\, B)$, $K = (H \vee I)$, $L = (A \vee J)$ and $M = (K \Leftrightarrow L)$. Then we have $G = (A \Rightarrow M)$. The truth table for G is:

A	B	C	$\rceil A$	$\rceil B$	$\rceil C$	H	I	J	K	L	M	G
1	1	1	0	0	0	0	0	0	0	1	0	0
1	1	0	0	0	1	0	1	0	1	1	1	1
1	0	1	0	1	0	0	0	1	0	1	0	0
1	0	0	0	1	1	1	1	1	1	1	1	1
0	1	1	1	0	0	1	0	0	1	1	1	1
0	1	0	1	0	1	1	1	0	1	1	1	1
0	0	1	1	1	0	0	0	1	0	1	0	1
0	0	0	1	1	1	0	1	1	1	1	1	1

According to the truth table, G is satisfied by the valuations

$(0,0,0)$, $(0,0,1)$, $(0,1,1)$, $(1,0,0)$, $(1,1,0)$, while $\rceil G$ is satisfied by $(1,0,1)$ and $(1,1,1)$.

We derive the CDNF of G:

$(\lceil A \wedge \rceil B \wedge \rceil C) \vee (\lceil A \wedge \rceil B \wedge C) \vee (\lceil A \wedge B \wedge C) \vee (A \wedge \rceil B \wedge \rceil C) \vee (A \wedge B \wedge \rceil C)$.

Next, the CDNF of $\rceil G$: $(A \wedge \rceil B \wedge C) \vee (A \wedge B \wedge C)$.

Finally, the CCNF of G: $(\lceil A \wedge B \wedge \rceil C) \wedge (\lceil A \wedge \rceil B \wedge \rceil C)$.

Example. $F = \rceil((\lceil p \Rightarrow q) \Rightarrow \rceil(q \Leftrightarrow p))$ We use the equivalences:

$(p \Rightarrow q) \Leftrightarrow (\lceil p \vee q)$

$(p \Leftrightarrow q) \Leftrightarrow ((\lceil p \vee q) \wedge (\lceil q \vee p))$

$$F \sim \rceil(\lceil(\lceil p \Rightarrow q) \vee \rceil(q \Leftrightarrow p))$$
$$\sim \rceil(\lceil(\lceil\rceil p \vee q) \vee \rceil((\lceil q \vee p) \wedge (\lceil p \vee q)))$$
$$\sim \rceil(\lceil(p \vee q) \vee \rceil((\lceil q \vee p) \wedge (\lceil p \vee q)))$$

We then use De Morgan's laws:

$\rceil(p \vee q) \Leftrightarrow (\lceil p \wedge \rceil q)$

$\rceil(p \vee q) \Leftrightarrow (\lceil p \vee \rceil q)$

Therefore:

$$F \sim \rceil\rceil(p \vee q) \wedge \rceil\rceil((\lceil q \vee p) \wedge (\lceil p \vee q))$$
$$\sim (p \vee q) \wedge (\lceil q \vee p) \wedge (\lceil p \vee q)$$
$$\sim (p \vee q) \wedge (\lceil q \vee p) \wedge (\lceil p \vee q)$$

2.8 Complete Systems of Connectives

Definition 2.14.

1) Let $\alpha_1, \alpha_2, ..., \alpha_k$ be a set of connectives of arbitrary arity. The set $\alpha_1, \alpha_2, ..., \alpha_k$ is a complete system if and only if: for any formula $F \in \mathcal{F}$, there exists a formula G based on the alphabet $P \cup \{\alpha_1, ..., \alpha_k\} \cup \{(,)\}$ such that $F \sim G$.

2) $\alpha_1, \alpha_2, ..., \alpha_k$ is a minimal complete system if no subset $A \underset{\neq}{\subset} \{\alpha_1, ..., \alpha_k\}$ is a complete system.

Example: $\{\rceil, \vee, \wedge\}$ is a complete system of connectives.

Proposition:

1) The system $\{\rceil, \vee, \wedge\}$ is not minimal.

2) The system $\{\rceil, \vee\}$ is minimally complete.

3) The system $\{\rceil, \wedge\}$ is minimally complete.

Proof.

1) $(p \wedge q) \sim \rceil(\rceil p \vee \rceil q)$, hence $(p \wedge q)$ can be expressed in terms of $\rceil$ and $\vee$.

2) Suppose $\vee$ can be expressed in terms of $\rceil$. Then, every formula is $\sim \rceil\rceil....\rceil p$ and therefore either p or $\rceil p$, which is not the case for $(p \wedge q)$.

2.8.1 Theories

Definition 2.15. A theory $\mathcal{Z}$ of propositional calculus is a set of formulas $T \subseteq \mathcal{F}$.

Let $\mathcal{M}$ be a model defined by the valuation v. We say that:

1) T is satisfied in m if $\mathcal{M} \vDash F$ for all $F \in T$. We write $\mathcal{M} \vDash T$.

2) T is consistent or non-contradictory or satisfiable if there exists a model $\mathcal{M} \vDash T$.

3) T is finitely satisfiable if and only if every finite sub-theory $T' \subseteq T$ is satisfiable (this definition is of interest only for infinite T).

4) T is contradictory if and only if it is not satisfiable, i.e., it has no model.

5) The formula F is a consequence of T if and only if every model of T is a model of F, i.e., $\mathcal{M} \vDash T \Rightarrow \mathcal{M} \vDash F$. We denote this as $T \vDash F$ or $(T \underset{\vdash}{*} F)$.

6) T and T' are two equivalent theories if and only if they have exactly the same models (or every formula in T is a consequence of T' and every formula in T' is a consequence of T).

Examples. Consider distinct propositional variables p, q, p_1, p_2, ..., p_m ...: the set $\{p, q, (\urcorner p \vee q)\}$ is satisfiable; $\{p, \urcorner q\}$ is contradictory; the empty set is satisfied by any valuation. $\{p, q\} \vDash (p \wedge q)$, $\{p, (p \Rightarrow q)\} \vDash q$, the set $\{p, q\}$ and $\{(p \wedge q)\}$ are equivalent, as well as $\{p_1, p_2, ..., p_m, ..\}$ and $\{p_1 \wedge p_2 \wedge ...p_m \wedge ...\}$.

Lemma. For any theories T *and* T', integers $p \geq 1$, formulas G, H, F_1, F_2, ...F_m, and G_1, G_2, ...G_p, the following properties are verified:

$*T \vDash G$ if and only if $T \cup \{\urcorner G\}$ is contradictory.

$*$ If T is satisfiable and $T' \subseteq T$, then T' is satisfiable.

$*$ If T is satisfiable, then T is finitely satisfiable.

$*$ If T is contradictory and $T \subseteq T'$, then T' is contradictory.

$*$ If $T \vDash G$ and $T \subseteq T'$, then $T' \vDash G$.

$*T \cup \{G\} \vDash H$ if and only if $T \vDash (G \Rightarrow H)$.

$*T \vDash (G \wedge H)$ if and only if $T \vDash G$ *and* $T \vDash H$.

$*\{F_1, F_2, ..., F_m\} \vDash G$ if and only if $\vDash ((F_1 \wedge F_2 \wedge ... \wedge F_m) \Rightarrow G)$.

$*G$ is a tautology if and only if G is a consequence of the empty set.

$*G$ is a tautology if and only if G is a consequence of any set of formulas.

$*G$ is contradictory if and only if $T \vDash (G \wedge \urcorner G)$.

$*G$ is contradictory if and only if every anti-tautology is a consequence.

Chapter 3

Predicate Calculus

Definition 3.1 A "predicate" is a statement concerning objects within a mathematical theory that can be either true or false depending on the objects involved.

Example.

1) "Being an even number" is true for 2 but false for other numbers.

2) "Being smaller than" is true for (2,3) but false for (3,2).

Predicate calculus allows the construction of complex statements from predicates by using special symbols to represent variables, functions on these variables, and the relationships between them. Certain variables never change; these are constants.

In this sense, predicate calculus is richer than propositional calculus.

3.1 Syntax of Predicate Calculus

3.1.1 First-Order Alphabet

Let $v = \{x_0, x_1, x_2, ...\}$ be a set whose elements are called variables.

$*\mathcal{C} = \{c_0, c_1, c_2, ..\}$ is a set whose elements are constants.

$*\mathcal{F} = \bigcup_{n>0} \mathcal{F}_n$ represents functions of arity n.

$*\mathcal{R} = \bigcup_{n>0} \mathcal{R}_n$ represents a union of sets $\mathcal{R}_n$ whose elements are relations of arity n.

(It is assumed that $\mathcal{R}_2$ contains a particular element of equality)

$*$ The symbols $\forall$ and $\exists$ (for all, there exists).

Definition 3.2 A first-order alphabet is an alphabet A of the form:

$A = \cup \cup \{(,), \rceil, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists\} \cup \mathcal{C} \cup \mathcal{F} \cup \mathcal{R}$.

- The part $\cup \cup \{(,), \rceil, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists\}$ is the logical part of the alphabet or language.

- The part $\sum = \mathcal{C} \cup \mathcal{R} \cup \mathcal{F}.$ is called the signature of the language.

- The logical part is common to all languages, so what characterizes a language is its non-logical part or signature.

Example. Signature of elementary arithmetic

$\sum = \{+, ., <, 0, 1\}$

$\mathcal{C} = \{0, 1\}$

$\mathcal{F} = \{+, .\} = \mathcal{F}_2$

$\mathcal{R} = \{<, =\} = \mathcal{R}_2$

3.1.2 Terms

Let A^* be the set of words formed from the alphabet A.

Definition 3.3 The set of terms T constructed from A is the smallest set of $A^*/$ such that

$1) \cup \cup \mathcal{C} \subseteq T.$

$2) t_1, t_2, ..., t_n \in T \Rightarrow f\, t_1, ..., t_n \in T, \forall\, f \in \mathcal{F}_n\, \forall\, n \geq 1.$

Example. In the theory of real numbers, the constants are $\mathbb{R}$, the variables are x,y,..., the functions $=$ are real functions: $\cos, \sin, +, ., ..$

$*\, \sin x$ is a term.

$*\, .xx$ is a term usually represented by x^2.

$*\, + xy$ is a term usually represented by $x + y$.

$*$ The expression $\sin(x + \sin(y^2 + x))$ is represented by the term: $\sin + x \sin + x.yy$

Note. As a word, each term has a unique representation.

The Height of a Term

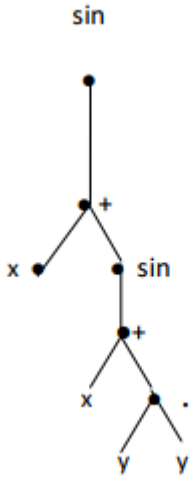
$T = \bigcup_{n \geq 0} T_n$ *with* $T_0 = v \cup \mathcal{C}$ and $T_{n+1} = T_n \cup \{f t_1, ..., t_k,\ f \in \mathcal{F}_k$ *and* $t_1, ..., t_k \in T_n\}$

$h(t) = min\{n/t \in T_n\}$

$*$ We can also refer to the decomposition tree of a term. The height of a term is the height of its decomposition tree:

Example. The term: $\sin + x \sin + x.yy$

$h = 5$



3.1.3 Formula

An atomic formula is a word in A^* that is $Rt_1...t_n$ where R is a relation of arity n $(R \in \mathcal{R})$ and $t_1....t_n$ are terms (we write $= t_1t_2$ for $t_1 = t_2$).

Definition3.4 The set of first-order formulas is the smallest subset $\mathcal{F}$ of $A^*/$

$*1)$ Any atomic formula $\in \mathcal{F}$.

$*2)$ $F, G, \in \mathcal{F} \Rightarrow \rceil F, (F \wedge G), (F \vee G), (F \Rightarrow G), (F \Leftrightarrow G) \in \mathcal{F}$.

$*3)$ $F, \in \mathcal{F} \Rightarrow \forall v_n F$ and $\exists v_n F \in \mathcal{F}, \forall n$.

Note.

1) We have $\mathcal{F} = \bigcup_{n\geq 0} \mathcal{F}_n$, $\mathcal{F}_0 =$atomic formula,
$\mathcal{F}_{n+1} = \mathcal{F} \cup \{\rceil F, F \in \mathcal{F}\} \cup \{(F * G), F, G \in \mathcal{F}_n, * =\} \cup \{\forall v_k F, F \in \mathcal{F}_n, k \in \mathcal{N}\} \cup \{\exists v_k F, F \in \mathcal{F}\ and\ h(F) = min\{n/\ F \in \mathcal{F}_n\}$.

2) As a word, every formula has a unique writing.

3) A formula also has a decomposition tree, with the leaves being the atomic formulas.

Example. Let the signature $\sum = \{p, Q, R, f, g, T\}$

$*\forall x\,(Rxy \Rightarrow Qxfy)$.

$* \rceil \exists x(Rxy \vee Qxgyx)$.

$* \forall x\,(px \wedge \exists y(Tyx \Rightarrow sxy))$ are formulas.

The subformulas of F are defined as follows: $*$ If F is atomic, then $sf(F) = \{F\}$.

$* F = \rceil G$, $sf(F) = \{F\} \cup sf\{G\}$.

$*$ If $F = (G_1 * G_2)$, $sf(F) \cup sf\{G_1\} \cup sf\{G_2\}$.

$*$ If $F = \forall x_k G$, $sf(F) = \{F\} \cup sf(G)$.

$F = \exists x_k G$.

3.2 Free and Bound Variables

A variable v_n can appear multiple times in a formula F. We say it has multiple occurrences. These occurrences are of two types: free and bound.

Definition3.5 We define by indication the free occurrences of v_n :

$\star$ If F is atomic, all occurrences of v_n in F are free.

$\star$ If $F = \rceil G$, the free occurrences of v_n in F are those of v_n in G.

$\star$ If $F = (G \alpha H)$, the free occurrences of v_n are those of v_n in G and those of v_n in H.

$\star$ If $F = \forall v_k G$ or $F = \exists v_k G$ with $k \neq n$, the free occurrences of v_n in F are those of v_n in G.

$\star$ If we say that x_n is quantified in F as $F = \forall v_n G$ or $F = \exists v_n G$ no occurrence of v_n in F is free.

Example. $\sum = \{R, c, f\}$

R: Relation, c: constant, f: function

$F = \forall x_0(\exists x_1 \forall x_0(Rx_1x_0 \Rightarrow \rceil x_0 \simeq x_3) \wedge \forall x_2(\exists x_2(Rx_1x_2 \vee fx_0 \simeq c) \wedge x_2 \simeq x_2)$

All occurrences of x_0 and x_2 are bound. The first two occurrences of x_1 are bound, but the third is free. x_3 is free.

Definition3.6 A variable in F is free if it has at least one free occurrence. A closed formula is a formula with no free variables. In the previous example, F is not closed ($(x_1 \, and \, x_3)$

are free). A closure of a variable in F is a formula of the form $\forall\, v_{i_1},\, v_{i_2}, ..., v_{i_n}\, F$ where $v_{i_1},\, ..., v_{i_n}$ are the free variables of F. An inverse closure is closed.

3.2.1 Scope of a Quantifier

Let $\ominus = \exists$ or $\forall$. In any formula F containing Ox, the term Ox is followed by a unique subformula G in which the variable x is free under Ox.

Definition 3.7 G is the scope of the quantifier O. The occurrences of x that fall within the domain of O are the free occurrences of x in G.

Example: $F = \exists\, x((px \vee \underset{8}{Qy} \wedge \underset{12}{gy} = z) \Rightarrow (\exists x \forall^{\swarrow 21} \underset{22}{y}\, \underset{25}{Rxy} \wedge fxz =)\, y$ where y is free at positions $8\, and\, 12$, and bound at positions 22 and 25, quantified at 22 and 25 within the domain of 21.

3.2.2 Substitution in Terms

Notation

$t = t[x_{i_1},\, x_{i_2}, ..., x_{i_n}]$ indicates that the variables with at least one occurrence in the term t are among $x_{i_1},\, ..., x_{i_n}$. If $m = \underset{j}{max}\, x_j$ we can also write $t = t[x_0,\, x_1, ..., x_m]$.

Definition 3.8 Let $y_1, ..., y_k$ be variables and $t,\, u_1, ..., u_k$ be terms. The term $t\frac{u_1}{x_1},...,\frac{u_k}{x_k}$ is obtained by substituting the terms $u_1, u_2, ..., u_k$ for the variables $y_1, ..., y_k$ in all occurrences of y_i in t. More precisely:

$\star t =$ constant or variable $\neq y_i$ then $t\frac{u_1}{y_1},...,\frac{u_k}{y_k} = t$.

$\star t = y_i\, (1 \leq i \leq k)\, t\frac{u_1}{y_1},...,\frac{u_k}{y_k} = u_i$.

$\star t = ft_1t_2...t_n\ t\frac{u_1}{y_1},...,\frac{u_k}{y_k} = ft_1\frac{u_1}{y_1},...,\frac{u_k}{y_k}....t_n\frac{u_1}{y_1},...,\frac{u_k}{y_k}$

Proposition 3.1 $t\frac{u_1}{y_1},...,\frac{u_k}{y_k}$ is a term.

Proof. By induction on the term t.

3.2.3 Substitution in Formulas

Notation

$F = F[x_{i_1}, ..., x_{i_n}]$ means that the free variables in F are among x_{i_1}. We will substitute terms for free variables in a formula.

Definition 3.9 Let F be a formula, and $y_1, ..., y_k$ be terms. The expression $F_{\frac{u_1}{y_1}...\frac{u_k}{y_k}}$ obtained by substituting the terms $u_1, ..., u_k$ for the variables $y_1, ..., y_k$ is defined as follows:

$\star$ *If* $F = Rt_1....t_n$ is atomic, then $F_{\frac{u_1}{y_1}...\frac{u_k}{y_k}} = Rt_1\frac{u_1}{y_1}...\frac{u_k}{y_k}.....t_n\frac{u_1}{y_1}...\frac{u_k}{y_k}$.

$\star$ *If* $F = \rceil G$ then $F_{\frac{u_1}{y_1}...\frac{u_k}{y_k}} = \rceil G_{\frac{u_1}{y_1}...\frac{u_k}{y_k}}$.

$\star$ *If* $F = (G \alpha H)$, $F_{\frac{u_1}{y_1}...\frac{u_k}{y_k}} = (G_{\frac{u_1}{y_1}...\frac{u_k}{y_k}} \alpha H_{\frac{u_1}{y_1}...\frac{u_k}{y_k}})$.

$\star$ *If* $F = OxG(x \neq y_i)$, $F_{\frac{u_1}{y_1}...\frac{u_k}{y_k}} = OxG_{\frac{u_1}{y_1}...\frac{u_k}{y_k}}$, $O = \exists$ *or* $\forall$.

$\star$ *If* $F = Oy_iG(i = 1, 2, ..., k)$, $F_{\frac{u_1}{y_1}...\frac{u_k}{y_k}} = Oy_iG_{\frac{u_1}{y_1}...\frac{u_{i-1}}{y_{i-1}},\frac{u_{i+1}}{y_{i+1}}...\frac{u_k}{y_k}}$

Example. $F = \forall x_0(\exists x_1 \forall x_0(Rx_1x_0 \Rightarrow \rceil x_0 = x_3) \wedge \forall x_2(\exists x_2(Rx_1x_2 \vee fx_0 = c) \wedge v_2 = v_2))$

$t = ffc$

$F_{\frac{t}{x_1}} = \forall x_0(\exists x_1 \forall x_0(Rx_1x_0 \Rightarrow \rceil x_0 = x_3) \wedge \forall x_2(\exists x_2(\exists x_2(Rffcx_0 \vee fx_0 = c) \wedge x_2 = x_0))$

3.3 Semantics of Predicate Calculus

We aim to assign truth values to formulas of predicate calculus. To do so, it is necessary to specify a domain in which variables take values, and where the symbols of relation and function have meaning.

Example 1. Consider the formula $\exists y \forall x\, Ryx$. To assign a truth value to this formula, we must assign values to the variables x, y and specify the definition of the "relation" R. Thus, it depends on the set in which the variables x, y take their values and on the definition of R in that set.

$\star$ If $R = \leqslant$ over $\mathbb{N}$, then the formula is true.

$\star$ If $R = <$ over $\mathbb{N}$, the formula is false.

⋆ If $R = \leqslant$ or $<$ over $\mathbb{Z}$, the formula is false.

Therefore, we need to specify a set in which the variables take values and in which the symbols of relations and functions become true relations and functions. This set will be a structure (or a realization of the language or alphabet A of the predicate calculus considered).

Example 2. *Rcx*

⋆ True for $\mathbb{N}$, $c = 0$, $x = 1$, $R = \leqslant$.

⋆ False for $\mathbb{N}$, $c = 0$, $x = -1$, $R = \leqslant$.

3.3.1 Definition of a Structure

Let A be an alphabet of first-order.

Definition 3.10 An A-structure is given by a set S such that:

⋆ Every constant symbol c in A is associated with an element $\bar{c}$ in S.

⋆ Each function symbol f of arity n is associated with a function $\bar{f} : S^n \longrightarrow S$.

⋆ Each relation symbol R of arity n is associated with a relation $\bar{R}$ of arity n on S ($\bar{R} \subseteq S^n$) (the equality relation corresponds to equality in S).

Example. Let the signature language be $\Sigma = \{R, f, c_0, c_1\}$. A possible structure is $S = \mathbb{N}, \bar{R} = \leqslant, \bar{f} = +, \bar{c_0} = 0, \bar{c_1} = 1$. Another possible structure is $S = \mathbb{R}, \bar{R} = <, \bar{f} = x, \bar{c_0} = e, \bar{c_1} = T$.

Remark. When considering multiple structures associated with the same language, and for any arbitrary structure, we write $\bar{c_s}, \bar{f_s}$, and $\bar{R_s}$.

Definition 3.11 Let S and S' be two structures of the same language (alphabet). We say that S is a substructure of S' if:

⋆ $S \subseteq S'$.

⋆ $\bar{c_s} = \bar{c_{s'}}$ for every constant c.

⋆ $\bar{f_s} = \bar{f_{s'}}$ for every function symbol f of arity n.

⋆ $\bar{R_s} = \bar{R_{s'}} \cap S^n$ for every relation R of arity n.

Example. $\Sigma = \{R, f, g, c_0, c_1\}$

$\star$ $S' = \mathbb{Z}, \bar{R_{s'}} = \leqslant, \bar{f_{s'}} = +, \bar{g_{s'}} = +, \bar{c_{0_{s'}}} = 0, \bar{c_{1_{s'}}} = 1$

$\star$ $S = \mathbb{N}, \bar{R_s} = \leqslant, \bar{f_s} = +, \bar{g_s} = +, \bar{c_{0_s}} = 0, \bar{c_{1_s}}$

Let S and S' be two structures of the same alphabet. A structure morphism between S and S' is a function $\varnothing : S \longrightarrow S'$.

$\star$ $\varnothing(\bar{c_s}) = \bar{c_{s'}}$ for all constants c

$\star$ $\varnothing(\bar{f_{a_1,...,a_n}}) = \bar{f_{s'}}(\varnothing(a_1), ..., \varnothing(a_n))$

for every function symbol f of arity n, for all $a_i \in S, \star(a_1), ..., a_n) \in \bar{R_s^n} \Rightarrow (\varnothing(a_1), ..., \varnothing(a_n) \in \bar{R_{s'}^n})$

for all $a_1, ..., a_n \in S$, and for all relation symbols R of arity n.

Example. $\Sigma = \{f, c\}$

$S =< \mathbb{R}_+^*, 1, x >$; $S' =< \mathbb{R}, 0, + >$

$$\varnothing : \mathbb{R}_+^* \longrightarrow \mathbb{R}$$
$$x \longmapsto \log x$$

Definition 3.12 A structure morphism $\varnothing : S \longrightarrow S'$ is a monomorphism if, for every relation R of arity n, if $a_1, \ldots, a_n \in S$, then $(a_1, a_2, \ldots, a_n) \in \bar{R_s} \Leftrightarrow (\varnothing(a_1), \ldots, \varnothing(a_n) \in \bar{R_{s'}}$.

Example. Every substructure defines a monomorphism (every injection $S \circlearrowleft S'$); the converse is also true.

Proposition 3.2 Every monomorphism is injective.

Proof. Among the relation symbols, we have the equality relation $=$, which defines equality on S and S': "=S" = "=s", "==". Therefore, if $a_1, a_2 \in S$ and $\varnothing(a_1) = \varnothing(a_2)$, since $\varnothing$ is a monomorphism, we have: $\varnothing(a_1) = \varnothing(a_2) \Leftrightarrow a_1 = a_2$, thus $\varnothing$ is injective.

Definition 3.13 An isomorphism of structures $\varnothing : S \longrightarrow S'$ is a surjective monomorphism; in particular, $\varnothing$ must be a bijection. An automorphism is an isomorphism $\varnothing : S \longrightarrow S$.

Example. $S =< \mathbb{R}_+^*, 1, \times >$ and $S' =< \mathbb{R}, 0, + >$.

$\varnothing : \mathbb{R}_+^* \longrightarrow \mathbb{R}, x \longmapsto \log x$ is an automorphism.

The next step is the interpretation of terms.

Definition 3.14 Let $t = t[x_0, \ldots, x_{n-1}]$ be a term and S a structure of first-order logic. Let $a_0, \ldots, a_{n-1}$ be elements of S.

The interpretation $\bar{t_s}$ of t in S when $x_i = a_i$, $0 \leq i \leq n$, is defined as follows:

$\star$ If $t = x_i$, then $\bar{t_s} = a_i$.

$\star$ If $t = c$, then $\bar{t_s} = \bar{c_s}$.

$\star$ If $t = ft_1 \cdots t_k$, then $\bar{t_s} = \bar{f_s}(\bar{t_{1_s}}, \ldots, \bar{t_{k_s}})$.

Example. $\Sigma = \{f, g, c_0, c_1\}$.

$S = \mathbb{N}, \bar{f} = +, \bar{g} = \times, \bar{c_0} = 0, \bar{c_1} = 1$.

$t = gyfxc_1 = t[x, y]$

$$\begin{pmatrix} x = x_0 \\ y = x_1 \end{pmatrix}$$

Let $a_0 = 2, a_1 = 3$.

$\bar{t_s} = \bar{g}(3, \bar{f}(2, 1)) = 3 \times (2 + 1) = 3 \times 3 = 9$

Proposition 3.3 Let $t = t[x_0, \ldots, x_{n-1}]$ and $t' = t'[y, x_0, \ldots, x_{n-1}]$ be two terms, and let $a_0, \ldots, a_{n-1}$ be elements of the structure S. Then we have $\bar{u_s} = \bar{t_{s'}}$, with $u = t'_{\frac{t}{y}}$ and $y \rightsquigarrow \bar{t_s} = b \in S$.

Proof. By induction on the term t'

$$\star t' = c, u = t' = c$$

$$\bar{u_s} = \bar{c_s} = \bar{t'_s}$$

$$\star t' = x_i, u = t' = x_i$$

$$\bar{u_s} = a_i = \bar{t'_s}$$

$$\star t' = y, u = t$$

$$\bar{u_s} = \bar{t_s} = \bar{t'_s}$$

$$\star t' = ft_1 \cdots t_k, \text{ then } u = fu_1 \cdots u_k \text{ with } u_i = t_{i\frac{t}{y}}$$

By the hypothesis $\bar{u_{i_s}} = \bar{t_{i_s}}$

Thus: $\bar{u_s} = \bar{f}(\bar{u_{1_s}}, \ldots, \bar{u_{k_s}}) = f(\bar{t_{1_s}}, \ldots, \bar{t_{k_s}}) = \bar{t'_s}$

3.3.2 Satisfaction of a Formula in a Structure

Let A be a first-order alphabet and S an A-structure. Let $F = F[x_0, ..., x_{n-1}]$ be a formula (this notation means that the free variables of F are among the x_i).

The satisfaction of a formula F in S is defined when the variables x_i are interpreted by the elements $a_0, a_1, \ldots, a_{n-1}$ of S.

This is written as:

$$S \models F[a_0, a_1, \ldots, a_{n-1}]$$

Definition 3.15 $\star$ If F is the atomic formula $Rt_1t_2 \ldots t_k$ with $t_i = t_i[x_0, \ldots, x_{n-1}]$, then

$$S \models F[a_0, \ldots, a_{n-1}] \Leftrightarrow (\bar{t_{1s}}, \ldots, \bar{t_{ks}}) \in \bar{R}_s$$

$\star$ If $F = \neg G$

$$S \models F[a_0, \ldots, a_{n-1}] \Leftrightarrow S \not\models G[a_0, \ldots, a_{n-1}]$$

$\star$ If $F = (G \wedge H)$, then

$$S \models F \Leftrightarrow S \models G \text{ and } S \models H$$

$\star$ If $F = (G \Rightarrow H)$, then

$$S \models F \Leftrightarrow S \not\models G \text{ or } S \models H$$

$\star$ If $F = (G \vee H)$, then

$$S \models F \Leftrightarrow S \models G \text{ or } S \models H$$

$\star$ If $F = (G \Leftrightarrow H)$, then

$$S \models F \Leftrightarrow (S \models G \text{ and } S \models H) \text{ or } (S \not\models G \text{ and } S \models H)$$

$\star$ If $F = \forall x G$ (where $x \neq x_i$), then

$$S \models F[a_0, \ldots, a_{n-1}] \Leftrightarrow S \models G[a, a_0, \ldots, a_{n-1}] \text{ for all } a \text{ where } x \text{ is interpreted by } a$$

$\star$ If $F = \exists x G$ (where $x \neq x_i$), then

$$S \models F[a_0, \ldots, a_{n-1}] \Leftrightarrow \text{ if there exists } a \in S \text{ such that } S \models G[a, a_0, \ldots, a_{n-1}] \text{ with } x \mapsto a$$

$\star$ If $F = \forall x_i G$, then

$$S \models F[a_0, \ldots, a_{n-1}] \Leftrightarrow S \models G[a_0, \ldots, a_{i-1}, x_i \mapsto a, a_{i+1}, \ldots, a_{n-1}] \text{ for all } a \in S$$

$\star$ If $F = \exists x_i G$, then

$$S \models F[a_0, \ldots, a_{n-1}] \Leftrightarrow \text{ there exists } a \in S \text{ such that } S \models G[a_0, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_{n-1}]$$

Remark If F is closed (without free variables), we write $S \models F$; F is satisfied in S.

Example Let $\sum = \{\underset{\uparrow 2}{R}, \underset{\uparrow 1}{f}, c\}$ be the structure, and $S = \mathbb{R}, \bar{R}_s = \leqslant, \bar{f}_s = \cos, \bar{c_s} = \pi$.

$\star$ $F = Rcx\,(= Rt_1t_2)$

$$\begin{aligned} S \models F[a] &\Leftrightarrow \bar{t_{1s}}, \bar{t_{2s}} \in \bar{R}_s \\ &\Leftrightarrow \bar{t_{1s}} \leqslant \bar{t_{2s}} \\ &\Leftrightarrow \pi \leqslant a \end{aligned}$$

Thus: $S \models F[a] \Leftrightarrow a \in [\pi, +\infty[$

$\star$ $F = \text{``}fx_0 = c\text{''} = cfx_0$

$$S \models F[a] \Leftrightarrow \bar{c_s} = f\bar{x_{0_s}} \Leftrightarrow \pi = \cos a$$

Thus: $\forall a \in \mathbb{R}, S \not\models F[a]$

$\exists x_1 \underbrace{fx_1}_{G} = x_0$, free variable x_0.

$$\begin{aligned} S \models F[a_0] &\Leftrightarrow S \models G[a_0, a_1] \text{ for some } a_1 \\ &\Leftrightarrow \exists a_1 / \cos a_1 = a_0 \\ &\Leftrightarrow a_0 \in [-1, 1] \end{aligned}$$

$\star$ $\forall x_1 \underbrace{Rx_0fx_1}_{G}$, free variable x_0

$$\begin{aligned} S \models F[a_0] &\Leftrightarrow S \models G[a_0, a_1]/\forall a_1 \\ &\Leftrightarrow \forall a_1 / a_0 \leqslant \cos a_1 \\ &\Leftrightarrow a_0 \in]-\infty, -1] \end{aligned}$$

$\star$ $\forall x_1 \underbrace{\exists x_2 (Rx_1x_2 \wedge fx_2 = x_0)}_{G}$, free variable x_0

$$S \models F[a_0] \Leftrightarrow \forall a_1 \exists a_2 / S \models G[a_0, a_1, a_2]$$
$$\Leftrightarrow \forall a_1 / \exists a_2 / a_1 \leqslant a_2 \text{ and } a_0 = \cos a_2$$
$$\Leftrightarrow a_0 \in [-1, 1]$$

$\star$ $x_0 \exists x_1 \underbrace{fx_1 = x_0}_{G}$ closed formula

$$\forall a_0, \exists a_1 / \cos a_1 = a_0 \quad S \models F$$

$\star$ $\exists x_1 \forall x_2 \underset{G}{Rfx_2x_1}$ closed formula

$$\exists a_1 / \forall a_2, \cos a_2 \leqslant a_1 \quad S \models F$$

Proposition 3.4 Let $t = t[x_0, \ldots, x_{n-1}]$ be a term and $F = F[z, x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1}]$ a formula such that no occurrence of z is within the scope of $\forall x_i$ or $\exists x_i$. Then, for any structure S and $\forall a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1} \in S$, we have:

$$S \models F_{\frac{t}{z}}[a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1}] \Leftrightarrow S \models F[\bar{t_s}, a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1}]$$

Proof By induction on the formula F

$\star$ $F = Rt_1t_2 \ldots t_k \quad t_i = t_i[z, x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1}]$

$$F_{\frac{t}{z}} = Rt_{1\,\frac{t}{z}} \ldots t_{k\,\frac{t}{z}} = Rr_1 \ldots r_k$$
$$S \models F_{\frac{t}{z}} \Leftrightarrow (\bar{r_{1_s}}, \ldots, \bar{r_{k_s}}) \in \bar{R}_s$$

Let $c_i = \bar{t_{i_s}}[\bar{t}, a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1}]$

Then $\bar{r_{i_s}} = c_i$, so $S \vDash F_{\frac{t}{z}} \Leftrightarrow (\bar{t_{i_s}}[\bar{t_s}, a_0, ..., a_{n-1}, b_0, ..., b_{m-1}]) \in \bar{R}_s$, $i = 1, .., k \Leftrightarrow S \vDash F[\bar{t_s}, a_0, ..., a_{n-1}, b_0, ..., b_{m-1}]$

Consequence and Universal Equivalence

Let A be a first-order alphabet:

$\star$ A closed formula F is universally valid if $S \models F$ for every A-structure S. We denote this by

$\models F$.

$\star$ A closed formula F is contradictory if and only if $\neg F$ is universally valid.

$\star$ A formula F with free variables is universally valid if its universal closure is.

$\star$ F is universally equivalent to G (denoted $F \sim G$) if and only if $(F \Leftrightarrow G)$ is universally valid.

$\star$ A theory T over A is a set of closed formulas.

$\star$ The structure S is a model of the theory T if and only if $S \models F$ for all $F \in T$ (we also say that S and T satisfy $S \models T$).

$\star$ A theory T is consistent if it has at least one model; otherwise, it is contradictory.

$\star$ A theory is finitely consistent if every finite subset is consistent.

$\star$ A closed formula F is a consequence of T if every model of T satisfies F. We denote this by $T \models F$.

(If F is not closed, consider its universal closure.)

$\star$ T_1 is equivalent to T_2 if and only if every model of T_1 is a model of T_2 and vice versa.

Proposition 3.5

1) If $F \sim F'$ and $G \sim G'$, then $\neg F \sim \neg F'$, $(F \alpha G) \sim (F' \alpha G')$, where α is $\wedge, \vee, \Rightarrow, \Leftrightarrow$

$\forall x\, F \sim \forall x\, F'$

$\exists x\, F \sim \exists x\, F'$

2) Let F be a formula, G a subformula of F, and $G' \sim G$. Then $F' = F_{\frac{G'}{G}} \sim F$.

Proof.

1) Consider the closed formula $\forall$. We need to show that the closure of $(\forall x\, F \Leftrightarrow \forall x\, F')$ is satisfied in any structure S. Write

$$F = F[x_0, ..., x_{n-1}, x]$$

$$F' = F'[x_0, ..., x_{n-1}, x]$$

Let $x \to a$

$$\begin{aligned} S \models \forall x\, F[a_0, ..., a_{n-1}] &\Leftrightarrow \forall a\, S \models F[a_0, ..., a_{n-1}, a] \\ &\Leftrightarrow \forall a\, S \models F'[a_0, ..., a_{n-1}, a] \\ &\Leftrightarrow S \models \forall x\, F'[a_0, ..., a_{n-1}] \\ &\Leftrightarrow S \models (\forall x\, F \Leftrightarrow \forall x\, F') \end{aligned}$$

2) By induction on the formula F.

Example.

$$\left.\begin{array}{c} \neg\forall x\, F \sim \exists x\, \neg F \\ \forall x(F \wedge G) \sim (\forall x\, F \wedge \forall x\, G) \\ \exists x(F \vee G) \sim (\exists x\, F \vee \exists x\, G) \\ \exists x(F \Rightarrow G) \sim (\forall x\, F \Rightarrow \exists x\, G) \\ \forall x\, \forall y\, F \sim \forall y\, \forall x\, F \\ \exists x\, \exists y\, F \sim \exists y\, \exists x\, F \end{array}\right\} \text{Equivalent formulas}$$

$$\left.\begin{array}{c} \exists x(F \wedge G) \Rightarrow (\exists x\, F \wedge \exists x\, G) \\ (\forall x\, F \vee \forall x\, G) \Rightarrow \forall x(F \vee G) \\ \exists x\, \forall y\, F \Rightarrow \forall y\, \exists x\, F \end{array}\right\} \text{Universally valid formulas}$$

If x is not free in F, we have: $\forall x\, F \sim \exists x\, F \sim F$.

Corollary. Every first-order formula is equivalent to a formula using only $\neg, \wedge, \vee$.

Proof. $\{\neg, \vee\}$ is complete for logical connectives, and $\exists$ can be expressed in terms of $\neg$ and $\forall$.

Chapter 4

Axiomatic of Z F and AC

4.1 Paradoxes, Naive Set Theory

The basic idea of naive set theory is a very powerful concept, that of a set. A set is a collection of objects, which can themselves be sets. These objects are called elements of the set. (We can distinguish one element from another by their properties, which are assertions that will be true for some elements and false for others.) Two "naive" sets are very intuitive: the empty set and the set Ω of all sets. Unfortunately, the naive concept of a set turns out to be too broad; it can lead to paradoxes. The most important of these paradoxes is based on a theorem proven by Georg Cantor in 1891, which states that the set $\mathcal{P}(E)$ of all subsets of a set E is always larger than E itself; this means that the elements of $\mathcal{P}(E)$ cannot be put into a one-to-one correspondence with those of the set E.

For example, if $E = \{1, 2, 3\}$, a set containing three elements,

$$\mathcal{P}(E) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

contains eight elements, and we have $8 > 3$. Similarly, for a finite set E, $\mathcal{P}(E)$ is larger than E because a one-to-one correspondence cannot be established between the elements of E and those of $\mathcal{P}(E)$. We say that E and $\mathcal{P}(E)$ do not have the same cardinality. The paradox arises when we consider the set Ω of all sets: Cantor's theorem tells us that $\mathcal{P}(\Omega)$ is a "larger" set than Ω, which is supposed to contain all sets! Here are now some other classic paradoxes (or antinomies):

4.1.1 Russell's Paradox

Russell's paradox is a very simple paradox in set theory (Russell himself played a significant role in its formalization, in an equivalent sense), which Bertrand Russell discovered and published in 1903. It was actually known to Zermelo, independently, at the same time, but the latter did not publish it.

Statement of the Paradox

The paradox can be formulated as follows: does the set of all sets that do not contain themselves contain itself? If we answer yes, then, by definition, the members of this set do not contain themselves, so it does not contain itself: contradiction. But if we answer no, then it has the required property to belong to itself: contradiction again. Thus, there is a contradiction in both cases, making the existence of such a set paradoxical.

More formally, if we set $y = \{x \mid x \notin x\}$, we immediately have $y \in y \Leftrightarrow y \notin y$, so each of the two possibilities, $y \in y$ and $y \notin y$, leads to a contradiction.

Solutions to the Paradox

The main solutions proposed to evade this paradox were:

1. Restriction of the comprehension axiom, due to Zermelo (1908):

A predicate does not define a set but what is called a class, and its intersection with a set gives a subset of that set. It is possible to write the predicate " $x \notin x$", but it no longer defines a set. It can define a subset of a given set, but this does not necessarily lead to a paradox. It became necessary for the development of mathematics to introduce several other instances of the comprehension principle as particular axioms (pairing, union, set of subsets, etc.). Later, Abraham Fraenkel and Thoralf Skolem independently introduced the schema of replacement axioms, which is still a restriction of the general comprehension principle but extends the schema of comprehension axioms introduced by Zermelo. They also clarified the notion of a predicate, and particularly Skolem, the logical context (first-order predicate calculus).

2. Russell's Theory of Types:

Outlined in an appendix of the aforementioned 1903 work, Russell developed it in a 1908 paper (see references). He continued, with Whitehead, with the Principia Mathematica published in 1910. According to this theory, sets are hierarchically ordered by type. A set can only contain objects that are of strictly lower types than the type of the initial set, so the paradoxical statement (the self-membership predicate " $x \in x$") can no longer be written. Russell did not immediately develop the theory of types after 1903. He first considered alternative solutions, such as the "no-class" theory, which he attempts to outline in his 1906 paper. In this same paper, Russell does not even mention the theory of types among the solutions he explored.

4.1.2 The Barber Paradox

The barber paradox is a didactic illustration of Russell's paradox, attributed to Bertrand Russell himself. Therefore, one should not give excessive importance to this "paradox," which the logician E. W. Beth qualifies as a "supposed antinomy" or a "pseudo-antinomy."

Statement of the Paradox

The paradox can be stated as follows:

The town council of a village issues an ordinance requiring its barber (male) to shave all the male inhabitants of the village who do not shave themselves, and to refrain from shaving those who do.

The barber, who is indeed a resident of the village, cannot adhere to this rule because:

- If he shaves himself, he violates the rule, as the barber can only shave men who do not shave themselves.
- If he does not shave himself—whether he allows himself to be shaved or keeps his beard—he is also in the wrong, as he is responsible for shaving men who do not shave themselves.

Thus, the rule is inapplicable. Does this constitute a paradox? There is no reason to believe that a village council or any other authority cannot issue an absurd ordinance. In fact, rather than

being a logical antinomy, this "paradox" simply demonstrates that a barber complying with this rule cannot exist. It illustrates that if R is any binary relation (in this case, " ...shaves..."), the following statement, written in formal language: $\neg\exists y\forall x(yRx \Leftrightarrow \neg xRx)$, is a universally valid formula in first-order predicate calculus. Refer to the article on Russell's paradox to see why this can lead, in the case of membership relation in a naive set theory, to a genuine antinomy, i.e., a demonstrated contradiction within the theory.

4.1.3 The Liar Paradox

The Liar Paradox is derived from the Cretan Paradox (or Epimenides Paradox). This paradox is attributed to Euclid, an opponent of Aristotle. In its most concise form, it is stated as follows: "A man says: I am lying. If it is true, then it is false. If it is false, then it is true." This can be interpreted in two ways:

- As a statement, this phrase says: "This statement is false.";
- As a proposition, it should be understood as: "I am lying now."

Statement of the Paradox

The Liar Paradox is attributed to Epimenides the Cretan (7th century BCE), although it appears that this early formulation of the Liar Paradox was considered paradoxical only much later; when in the 4th century BCE, Euclid of Miletus stated: "A man said that he was lying. Is what the man said true or false?"

This paradox can be extended with the statement: "The next sentence is false. The previous sentence is true."

Assigning to Epimenides the proposition: "All Cretans are liars," this was considered by ancient philosophers as a paradox because it defied the principle of non-contradiction. Indeed, if Epimenides is telling the truth, then he is lying (since he is a Cretan), thus his statement is false (since all Cretans lie). Conversely, if Epimenides is lying when he says this, then there exists at least one Cretan who tells the truth, and hence his statement is false. In all cases, his statement is false, which is not contradictory; this is the resolution of the paradox.

Solution to the Paradox

Aristotle seems to allude to this paradox in "Sophistical Refutations" and provides this solution: one can lie in general while telling the truth about a specific point. The contradiction disappears once the proposition is understood as: "I am telling the truth when I say that I am lying": the truth in question is no longer absolute, but relative to a specific content. An ambiguity thus arises from the confusion between language and metalanguage (the language talking about the language in which it is spoken).

Modern interpreters have resolved this paradox by extending it in time. Indeed, all that can be deduced from Epimenides' statement is that it is false; in particular, not all Cretans are liars, but Epimenides is. Thus, the paradox is resolved by extending it in space. However, the statement in the present tense would require an analysis in the same temporal context, with all the immediacy necessary for the resolution of Epimenides' assertion.

In fact, the negation of "All Cretans are liars" is not "All Cretans tell the truth," but: "There exists at least one Cretan who tells the truth" (and one should even say, in the sense that liar has been used so far, "There exists at least one Cretan who sometimes tells the truth"). Thus, there may be one or more Cretan liars, but it is true that Epimenides could be one.

Similarly, the paradox "I always lie" ceases to be a paradox when extended over time: at the moment I say "I always lie," I am necessarily lying (otherwise, we have the same problem as with Epimenides), which implies that I do not always lie. There is no logical contradiction: I sometimes lie, but not always!

The Liar Paradox becomes more interesting when considering the following version: "I am lying right now." If this becomes true!

This indicates that when a statement can refer to itself, it can lead to an unstable situation.

This statement performs an action by virtue of its utterance; it is a performative contradiction. Another example: "I am dead" (if I am speaking, it means I am still alive).

4.1.4 Cantor's Paradox

Cantor's Paradox, or the paradox of the largest cardinal, is a paradox in set theory whose argument was discovered by Georg Cantor in the 1890s (it is found in a letter to David Hilbert dated 1897). It was named by Bertrand Russell in his "Principles of Mathematics" published in 1903. The paradox states that the existence of a largest cardinal leads to a contradiction. In a naive set theory that assumes any property defines a set, this paradox is indeed an antinomy, a contradiction derived from the theory, since the cardinality of the class of all sets would then be the largest cardinal. However, it is not a paradox for Cantor, who never referred to it as such. For him, it shows that the largest cardinal, if it can be defined in some way, is not a set: reformulated in modern terms and in an axiomatic set theory that Cantor was unaware of, the class of cardinals is not a set.

Statement of the Paradox

The paradox can be derived in two ways. Both use the fact that every set has a cardinality, and thus implicitly the Axiom of Choice.

- It is shown that the class of cardinals is equipotent to the class of ordinals, thereby reducing Cantor's paradox to the Burali-Forti paradox. This requires a form of the Replacement Schema.
- Cantor's theorem on the cardinality of the power set is used: if the largest cardinal is a set, then it has a power set, which has a cardinality strictly greater than that largest cardinal.

Cantor's Paradox and Russell's Paradox

Cantor can eliminate any appeal to the notion of cardinality, and thus to the Axiom of Choice, in the second reasoning. Consider the class of all sets (whose cardinality would naturally be the largest cardinal).

For Cantor, every set could be well-ordered and had a cardinality. However, any appeal to the notion of cardinality, and thus to the Axiom of Choice, can be eliminated in the second reasoning. Let V be the class of all sets (whose cardinality would naturally be the largest

cardinal). If V is a set, then its power set $\mathcal{P}(V)$ is also a set. Thus, $\mathcal{P}(V) \subset V$, and the identity defines an injection from $\mathcal{P}(V)$ into V, contradicting Cantor's theorem. It has thus been shown that the class of all sets is not a set.

Cantor himself stated that Russell's paradox, and in this case the proof of Cantor's theorem, were related. By adapting the proof of Cantor's theorem to this specific case, one constructs a left inverse to the identity from $\mathcal{P}(V)$ into V, and considers the set $\{x \in V \mid x \notin f(x)\}$, whose intersection with $\mathcal{P}(V)$ is $\{x \in \mathcal{P}(V) \mid x \notin x\}$.

Russell's paradox has the advantage of being simpler and not involving the power set of a set; the only set-theoretic property used is unrestricted comprehension, which is used only once and is exactly the reason for the paradox. Cantor's paradox also uses unrestricted comprehension, in an analogous way to Russell's paradox, which is not valid in standard set theories such as ZFC, but is permissible when it asserts that the power set of a set is a set, which is indeed allowed (this is the Axiom of the Power Set).

4.1.5 Richard's Paradox

Richard's Paradox appears in a set theory that is not sufficiently formalized. It played an important role in research on the foundations of mathematics, particularly in the early 20th century, and has since its publication in 1905 generated numerous comments. Its author, the French mathematician Jules Richard, a professor at the Lycée de Dijon, described it in a letter to the editor of the Revue générale des Sciences Pures et Appliquées. The editor decided to publish it, in the form of a short article, in the June 30, 1905 issue of that journal.

Statement of the Paradox

If we enumerate all real numbers definable in a finite number of words, then we can construct, using Cantor's diagonal argument, a real number not on this list. Yet, this number has been defined in a finite number of words.

Here are some details about the construction:

1. Real numbers definable with a finite number of words form, by this very fact, a countable

set, denoted E.

2. A real number N not in E can be constructed using the following diagonalization procedure: enumerate the elements of E, then choose each digit of N so that the n-th digit of N differs from the n-th digit of the n-th element, and ensure it is not 9 (to avoid double representation of decimals). Thus, for each n, the n-th element differs from N in at least one digit, so n does indeed differ from N (all reals, aside from decimals, have a unique decimal representation).

3. However, in describing this construction process, N has been defined in a finite number of words: this is a contradiction.

This paradox, which is formulated very simply, like Russell's paradox, raises a different kind of problem, which is that of the permissible language for mathematical statements, as Giuseppe Peano noted as early as 1906. Like Russell's paradox, it played an important role in the crisis of the foundations of mathematics at the beginning of the 20th century, a crisis that the Hilbert program aimed to resolve definitively. It is mentioned by Kurt Gödel in the introduction to his 1931 paper on incompleteness theorems: when summarizing the argument for constructing an undecidable proposition, he states that "The analogy between this reasoning and Richard's antinomy is striking." The statement Gödel constructs is inspired by the liar paradox, in a form—a proposition that states itself as not being provable (or false, to truly reflect the liar paradox)—which poses the same kind of questions as Richard's paradox.

Richard's paradox also had many reformulations, including Berry's paradox about the smallest number not definable in fewer than a specified number of words (100 or any number greater than the non-'i' elements used to define this number), sometimes also referred to as Richard's paradox.

Solution to the Paradox

Most often, this paradox is resolved by distinguishing between two levels of language: the language of the theory being described, sometimes called the object language, and the language, often not formalized, used to describe this theory, the metalanguage. When defining the count-

able set of reals definable in a finite number of words, it can only be done in a specific language. The description of the real number N is made in a finite number of words in the metalanguage. Its construction simply shows that it cannot be described in a finite number of words in the original language. To reflect the paradox in the object language, one would need to encode the metalanguage in the object language, as Gödel does for the liar paradox. Then there is no paradox.

This solution (distinguishing two levels of language) was not exactly the one proposed by Richard in his paper. For him, the paradox arises from the very definition of N invoking the set E, while E is not yet completely defined. According to Richard, when constructing the enumeration, at the moment when the statement defining N (and hence the letter E appears) is enumerated, it has no meaning yet. This was systematized by Henri Poincaré, who was greatly interested in Richard's paradox, under the name of "non-predicative definitions." He saw the rejection of these definitions as the "true solution" to the paradoxes. Non-predicative theories have since been shown to be consistent (non-paradoxical), but predicativity remains a good principle for constructing consistent theories. Predicativity is also a principle sought by some, such as Quine, who sees it as a way to avoid an "ontological commitment" that only makes sense if one supports the philosophical position of mathematical Platonism.

4.1.6 Grelling's Paradox

The Grelling-Nelson paradox is a semantic paradox formulated in 1908 by Kurt Grelling and Leonard Nelson, and is sometimes mistakenly attributed to the German philosopher and mathematician Hermann Weyl. It is then referred to as Weyl's paradox, but is also known as Grelling's paradox.

Statement of the Paradox

The Grelling paradox can be stated as follows: some adjectives describe properties that apply to themselves, such as "polysyllabic," "French." Such adjectives can be termed autological. Other adjectives, conversely, describe properties that do not apply to themselves. For example,

"long," "monosyllabic." Such words can be termed heterological. This leads to a classification of words into two categories:

(a) autological;

(b) heterological.

However, such a distinction leads to a paradox. Given the previous definitions, the paradox arises when considering the status of the heterological predicate itself. Thus, is "heterological" autological or heterological? For if "heterological" is heterological, then by definition, "heterological" is autological. Conversely, if "heterological" is autological, then it results in it being heterological. The conclusion is paradoxical, as it implies that "heterological" is heterological if and only if it is autological.

The paradox arises because if the word heterological does not apply to itself, then it is heterological while not being so, and if it applies to itself, it is not heterological while being so. The reasoning leading to the Grelling paradox can be presented in more detail as follows: It is noted that the proposition $P(X) =$ "the word X is heterological" is a proposition for which the truth value is undefined if X is the word heterological. However, it is also evident that the word heterological is not autological either. Therefore, the proposition $P(X)$ has three ranges of values, one of which is undefined, as X ranges over the set of words in the language.

Solution to the Paradox

Among the solutions proposed to resolve the Grelling paradox, one observes that the structure of the paradox is very similar to that of Russell's paradox. Thus, both paradoxes would have a common structure and lead to similar conclusions.

One approach is to reject the definitions of all predicates that present self-referential structures. However, such a solution proves to be unsatisfactory. Indeed, it appears to be too restrictive, as it is quite possible to validly determine the status of many self-referential predicates, such as "polysyllabic." Proscribing all predicates with self-referential structures would be paying too high a price for merely eliminating the paradox.

4.2 Zermelo-Fraenkel Axioms (ZF)

We will discuss the axiom of choice, specifically in mathematical logic, within the usual axiomatization of sets called ZF (for Zermelo-Fraenkel theory). We will first present this axiomatization and provide all the necessary reminders for a precise statement of the axiom of choice.

The Zermelo-Fraenkel axiomatic theory is a theory based on first-order logic with identity and a single non-logical symbol. It is a first-order axiomatic theory constructed over the language $\{\in, =\}$. The objects discussed in this theory, i.e., the elements of a model of ZF, are sets: every variable represents a set, and there are no other types of objects.

Here are the axioms of the ZF theory:

4.2.1 Axiom of Extensionality

Two sets are identical if they have the same elements.

$$\forall A \forall B[(\forall x(x \in A) \Leftrightarrow (x \in B)) \Rightarrow A = B]$$

It stipulates that if A and B are two sets with exactly the same elements, then they are equal; thus, to define a set A, it is sufficient to define its elements.

4.2.2 Axioms of Construction

Axiom of Pairing

$$\forall x \forall y \exists A \forall z((z \in A) \Leftrightarrow (z = x \vee z = y))$$

It means that given two sets x and y, there exists a set A that has as elements only x and y; this set is unique by the axiom of extensionality and will be denoted $\{x, y\}$. By the axiom of extensionality, this set is unique, and one can define the pair $\{a, b\}$ by the unique c such that $\forall z((z \in c) \Leftrightarrow (z = a \vee z = b))$. One can also define the singleton $\{a\}$ as the set $\{a, a\}$. Since $\{a, b\} = \{b, a\}$, the ordered pair (a, b) is also defined by $(a, b) = \{\{a\}, \{a, b\}\}$.

Axiom of Union

$$\forall E \exists A(\forall z(z \in A) \Leftrightarrow (\exists y \in E, z \in y)).$$

This means that the elements of A are exactly the elements of the elements of E. Again, such a set is unique. We denote it by $\cup E$ (read as "union of E"). Informally, this corresponds to an indexed union by the index set E, where the sets being united are precisely the elements of E. For example, if we know that $\{\{1,2\},\{3,4,5\}\}$ is a set (with two elements), we deduce the existence of the set $\{1,2,3,4,5\}$.

This axiom thus allows us to define the union of two arbitrary sets by $x \cup y = \cup\{x,y\}$. This definition illustrates the "naïve" set-theoretic union because it is possible to prove $\forall x \forall y \forall z \quad ((z \in x \cup y) \Leftrightarrow (z \in x \vee z \in y))$ from the axioms established so far.

Axiom of Power Sets

If x is a set, there exists a set y whose elements are the subsets of x.

$$\forall x \exists y \forall t((t \in y) \Leftrightarrow (\forall v(v \in t) \Rightarrow (v \in x))).$$

Let a and b be two sets. The statement $\forall x(x \in a) \Rightarrow (x \in b)$ expresses set inclusion. We abbreviate statements by replacing this formula with $a \subset b$. The axiom of power sets can then be written more concisely as:

$$\forall x \exists y \forall t((t \in y) \Leftrightarrow (t \subset x)).$$

This axiom states that if x is a set, there exists a set, denoted $\mathcal{P}(x)$, the power set of x, whose elements are exactly the subsets of x.

Axiom Schema of Comprehension

If $\mathfrak{P}(x)$ is a property and E is a set, then the collection of objects x in E that satisfy the property $\mathfrak{P}(x)$ is also a set. Note that this axiom allows for the definition of a set from a property, but only if the elements already belong to another set: this avoids the definition of too large sets and avoids both Russell's and Cantor's paradoxes. Hence, the naïve set of all sets is not a set in the ZF theory!

The comprehension schema can be formally stated as:

$$\forall a_1 \ldots \forall a_n \forall A \exists B \forall x \left[x \in B \Leftrightarrow \left((x \in A) \wedge P\left(x, a_1, \ldots, a_n\right)\right)\right]$$

for any formula P containing no free variables other than $x, a_1, \ldots, a_n$ (in particular, B cannot appear in P). The $a_1, \ldots, a_n$ are parameters of the formula P.

This schema particularly implies the existence of a set with no elements. Indeed, the set Y defined by:

$$\forall x (x \in Y) \Leftrightarrow ((x \in X) \wedge (x \neq x))$$

exists precisely by the comprehension axiom and is empty. Such a set is unique by extensionality, and it will be denoted $\emptyset$ subsequently.

This schema also allows for the definition of the intersection of two sets, say A and B. It is simply the set X defined by:

$$\forall z (z \in X) \Leftrightarrow ((z \in A) \wedge (z \in B))$$

(considering it here as a subset of A). Once again, extensionality proves the uniqueness of such a set, and it will be denoted $A \cap B$.

Axiom of Replacement

The previous axioms do not allow for the discussion of all the sets one might want. We need to add the following:

We say that $F\left(x, y, a_1, \ldots, a_n\right)$, a formula with $(n+2)$ free variables, is a functional relation (or functional class) in x and y if it satisfies the following condition:

$$\forall x \forall y \forall y' \forall a_1, \ldots, \forall a_n$$

$$\left(\left(F\left(x, y, a_1, \ldots, a_n\right) \wedge F\left(x, y', a_1, \ldots, a_n\right)\right) \Rightarrow (y = y')\right).$$

This means exactly that given $x, a_1, \ldots, a_n$, there is at most one y that satisfies $F\left(x, y, a_1, \ldots, a_n\right)$; it is the image of x under the functional F.

The replacement schema states that for any functional F, if A is a set, so is $F(A)$. Therefore, we would like to index the axioms by functionals. However, this is not possible because the

property of being a functional heavily depends on the considered universe, and we would like the axioms to be independent of this. In practice, the axioms are indexed by all formulas, and we proceed as follows:

$$F(x, y, a_1, \ldots, a_n) \text{ functional } \Rightarrow$$

$$\forall a_1 \ldots \forall a_n \forall A \exists B \forall y$$

$$((y \in B) \Leftrightarrow (\exists x \in A \wedge F(x, y, a_1, \ldots, a_n))).$$

The set B will be denoted $F(A)$.

A variant of the replacement schema as stated above is to assume that in addition to being functional, the relation defined by F (with the above notations) is defined everywhere on the universe, so we add the hypothesis:

$$\forall a_1 \ldots \forall a_n \forall x \exists y F(x, y, a_1, \ldots, a_n).$$

In this case, we can use the notation $y = \phi(x)$ for the functional $F(x, y, a_1, \ldots, a_n)$. If A is a set, then the set obtained by replacement, using the functional relation F, is denoted $\{\phi(x) \mid x \in A\}$.

When f is a function (in the sense of a set of pairs) defined on A, we also denote:

$$\{f(x) \mid x \in A\} = \{y \mid \exists x \in A \text{ such that } y = f(x)\}$$

the set whose existence is justified by the comprehension schema.

Axiom of Infinity

There exists an infinite set, that is, by definition, a set that contains a subset different from itself and as large as itself. There are many ways to formulate this, for example:

$$\exists X((\exists x \in X) \wedge (\forall x \in X, x \cup \{x\} \in X))$$

where $\{x\}$ is the set containing only x, which exists by virtue of the pair axiom.

Axiom of Foundation

There are no infinite descending chains of sets (x_n) such that x_{n+1} belongs to x_n, which belongs to... x_1, which belongs to x_0. In particular, this axiom avoids the existence of a set x that

belongs to x. More precisely, the axiom of foundation states that every non-empty set contains another set whose intersection with the first set is empty. The simplest way to write this as an axiom is probably:

$$\forall x(x \neq \emptyset) \Rightarrow (\exists y \in x, (x \cap y) = \emptyset).$$

4.2.3 Zermelo's Set Theory

Zermelo's set theory is a modern presentation of the theory published by him in 1908, explicitly or implicitly presented within the framework of first-order logic with equality. It includes the following axioms:

- Axiom of Extensionality;
- Axioms of Construction:
  - Axiom of Pairing;
  - Axiom of Union;
  - Axiom of Power Sets;
  - Axiom of Infinity;
  - Schema of Comprehension Axioms.

Remark. The axiom of the empty set, sometimes introduced separately, is deduced from the schema of comprehension axioms (in first-order logic).

4.2.4 Zermelo-Fraenkel Set Theory

It includes additionally:

- Schema of Replacement Axioms;
- Axiom of Foundation.

The schema of replacement axioms particularly allows for the development of ordinal set theory.

- The schema of comprehension axioms is deduced from the schema of replacement axioms (and hence particularly the existence of the empty set, assuming that every set theory universe has at least one element).

- The axiom of pairing is deduced from the axiom of power sets and the schema of replacement.

4.3 Axiom of Choice (AC)

We denote by ZFC the axiomatic system obtained by adding the axiom of choice (AC) to the Zermelo-Fraenkel system (ZF).

4.3.1 Axiom of Choice

Let E be a non-empty set. There exists a function f from $P(E)\backslash\{\emptyset\}$ to E that assigns to each non-empty subset A of E an element of that subset. More formally, this is written as:

$$\forall E \exists f (f \text{ is a function from } P(E)\backslash\{\emptyset\} \text{ to } E)$$

and

$$[\forall A \in P(E)\backslash\{\emptyset\}(A, a) \in f \Rightarrow a \in A]$$

A function f satisfying this property is called a choice function on E. The axiom of choice states exactly that every set admits a choice function.

For example, if $E = \{\{1, 2, 3\}, \{a, b\}, \{x, y\}\}$, then one can form the set

$$f = \{(\{1, 2, 3\}, 1), (\{a, b\}, b), (\{x, y\}, x)\}$$

.

4.3.2 Some Equivalent Forms

The axiom of choice is equivalent to many other statements:

1. Cartesian Product of Sets: equivalently and more compactly, it says that a non-empty product (i.e., indexed by a non-empty set) of non-empty sets is non-empty.

2. Zermelo's Theorem: Every set has a well-ordering.

3. Zorn's Lemma: Every partially ordered set in which every non-empty totally ordered subset has an upper bound has at least one maximal element.

4. Hausdorff's Maximality Principle: Every partially ordered set has a maximal totally ordered subset.

5. Every surjection has a right inverse: Let X and Y be two sets and $f : X \to Y$ be a surjective function, then there exists a function $g : Y \to X$ such that $g \circ f = \mathrm{Id}_Y$.

4.3.3 Zorn's Lemma

Definition 4.1 Let E be a set equipped with a binary relation denoted by $\leq$. We say that this relation is an order if it satisfies the following three properties:

- **(reflexivity):** $\forall x \in E, x \leq x$
- **(transitivity):** $\forall x \in E \forall y \in E \forall z \in E((x \leq y \wedge y \leq z) \Rightarrow (x \leq z))$
- **(antisymmetry):** $\forall x \in E \forall y \in E((x \leq y \wedge y \leq x) \Rightarrow (x = y))$.

A relation on E that satisfies only the first two conditions is called a preorder.

Definition 4.2 We say that the order is total, or that E is totally ordered, if the relation $\leq$ additionally satisfies:

$$\forall x \in E \forall y \in E(x \leq y \vee y \leq x)$$

Remark. We often say that E is a partially ordered set if it is equipped with an order relation. The term "partially" does not imply that the order relation is not total; it simply indicates that it is not necessarily total.

Definition 4.3 Let E be a partially ordered set. What is called a greatest element of E is an element x of E that is greater than all other elements, i.e., satisfying $y \leq x$ for all y in E.

Remark. • The property of antisymmetry directly shows that if a greatest element exists, then it is unique.

- It is important not to confuse this notion with that of a maximal element. A maximal element of E is an element x of E such that there is no strictly greater (i.e., greater and different) element than x.

Example. To illustrate the distinction, it is interesting to note that if E is a set equipped with the relation "equality" (i.e., $x \leq y$ if and only if $x = y$) which is an order relation, then

every element of E is a maximal element, but E does not have a greatest element if its cardinality is greater than 2. It is also interesting to note that this example shows that a maximal element is not necessarily unique.

Remark. However, it is true that if E is totally ordered, then a maximal element is necessarily unique, and the notions of maximal element and greatest element coincide. It is also true that if E is a partially ordered set that admits a greatest element x, then it admits a unique maximal element which is precisely x.

Definition 4.4 Now consider E as a partially ordered set. Let A be a subset of E. The order relation $\leq$ restricted to A (formally, this is the intersection of the relation $\leq$ with the set $A \times A$) is denoted by $\leq_A$.

- We say that A is bounded in E if there exists an element x in E that is greater than all elements of A, i.e., such that $y \leq x$ for all y in A.
- We say that A is a chain if the order induced on A is total.
- We say that E is inductive if every chain in E is bounded.
- Finally, we say that E is well-ordered if every non-empty subset A has a least element.

Hausdorff's Maximality Principle (PM): Every partially ordered set admits a maximal chain.

Another more common formulation of this statement is the Kuratowski-Zorn lemma, better known as Zorn's lemma.

Zorn's Lemma: Every inductive preorder has a maximal element.

Equivalence of these two statements: Assume initially Hausdorff's maximality principle and let E be an inductive partially ordered set. We need to prove that E has a maximal element. Consider a maximal chain A in E. By hypothesis, it is bounded. Let x be a bound. If there existed in E an element y strictly greater than x, then the set $A \cup \{y\}$ would be a chain in E strictly containing A, which is excluded. This proves that x is a maximal element of E.

Conversely, assume Zorn's lemma. Let E be a partially ordered set. Consider X as the

subset of $P(E)$ consisting of chains of E, ordered by inclusion. We claim that this set is inductive. Indeed, given a subset $\boldsymbol{X}^n$ of X, it is immediate to observe that the union of $\boldsymbol{X}^*$ (which is a subset of E) bounds $\boldsymbol{X}'$. Applying Zorn's lemma to X provides exactly what we seek.

4.3.4 Applications of the Axiom of Choice

The Axiom of Choice is a central tool in applied mathematics. One of the earliest explicit mentions of this axiom is due to Peano in 1890, in his proof of the existence of a solution for a system of differential equations. Among the classical proofs in mathematics that use the Axiom of Choice, we can mention:

- In general topology: Tychonoff's theorem.

Theorem 4.1 The product of compact topological spaces is compact.

- In algebra: The Axiom of Choice is often used in algebra in a different form: Zorn's Lemma.

Theorem 4.2 Every vector space has a basis.

Theorem 4.3 Every proper ideal of a ring is contained in a maximal proper ideal.

Theorem 4.4 Every field has a unique algebraic closure.

- In functional analysis: The Hahn-Banach theorem (geometric form).

Theorem 4.5 Let E be a topological vector space, A and B two non-empty convex, disjoint sets, with one of them open. Then there exists a hyperplane H that separates A and B.

- **In game theory:** The Axiom of Choice implies that there exists a set A of integer sequences such that neither player has a winning strategy in the following game: they alternately choose an integer, and the first player wins if and only if the sequence formed belongs to A.
- **In measure theory:** The Axiom of Choice allows us to assert the existence of non-measurable subsets of $\mathbb{R}$ in the sense of Lebesgue.

The Axiom of Choice is thus very useful in mathematics. This is why it is accepted by mathematicians despite its paradoxical consequences, such as the famous Banach-Tarski paradox. This paradox states that it is possible to cut a ball of radius r into pieces that can be rearranged to form two balls of radius r.

4.3.5 Independence of the Axiom of Choice

Two logical results indicate that the Axiom of Choice is independent of the other axioms of set theory.

Theorem 4.6 (Gödel, 1938) ZFC is consistent if ZFC is.

Here, consistency means that no contradiction can be found from these axioms. It is known that if it is consistent, the ZF system does not refute the Axiom of Choice, i.e., there is no proof of the negation of AC from the axioms of the ZF system.

Theorem 4.7 (Cohen, 1963) $ZF + \neg AC$ is consistent if ZF is.

If it is consistent, the ZF system does not prove the Axiom of Choice, i.e., there is no proof of AC from the axioms of the ZF system.

The proof uses the technique of forcing, which is difficult. Another approach, based on Boolean algebras, is said to be simpler. For more details,

4.4 Exercises

Exercise 1. Show that if $(a, b) = (c, d)$, then $a = c$ and $b = d$.

Exercise 2. Let $y = \{\{a, b, c\}, \{\{a, b\}\}, \{a\}, \{\{d\}\}\}$. What are the elements of vy?

Exercise 3. Show that if a, b, and c are sets, we can define a set d whose elements are exactly a, b, and c. We denote this set by $d = \{a, b, c\}$.

Exercise 4. Let a and b be sets. Show that $a \times b$ is a set.

Exercise 5. Show that the Axiom of Pairing is a consequence of the Schema of Substitution and the Axiom of Power Sets.

Exercise 6. Show that the Separation Schema is a consequence of the Replacement Schema.

Exercise 7. Let A and B be classes. We define the class $A \triangle B$, the symmetric difference of A and B, by:

$$A \Delta B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

- Show that if a and b are sets, the class $a \Delta b$ is a set.

Exercise 8. The Axiom of Foundation is defined by the following formula:

$$\forall x(x \neq \emptyset \Rightarrow \exists y[(y \in x) \wedge (y \cap x = \emptyset)])$$

- Show that the Axiom of Foundation implies:
  1. that a set x cannot contain itself, i.e., for any set x, $x \notin x$;
  2. that for any sets $x_1, \ldots, x_n$ such that for all $i \geq 1$ and $i \leq n-1$, we have $x_i \in x_{i+1}$, it follows that $x_n \notin x_1$;
  3. (with the Axiom of Infinity) that there does not exist a sequence $x_1, \ldots, x_n, \ldots$ of sets such that for all $i \geq 1$, $x_{i+1} \in x_i$.

Exercise 9. Show that the Axiom of Pairing is a consequence of the Schema of Substitution and the Axiom of Power Sets.

Exercise 10. Consider the theory ZFC_{fin}, which is the theory ZFC (Replacement Schema, Axiom of Power Sets, Axiom of Union, Axiom of Extensionality) with the Axiom of Choice and the Axiom of Foundation. The goal of this exercise is to provide a model of ZFC_{fin} that does not satisfy the Axiom of Infinity. For any integer q, define $[q]$ as the unique set of integers $\{p_1, \ldots, p_n\}$ such that $q = \sum_{i=1}^{n} 2^{p_i}$ (consider the binary representation of q). Define the binary relation E on $\mathbb{N}$ by: $pEq \iff p \in [q]$; show that:

1. The structure $(\mathbb{N}, E)$ satisfies the Axiom of Extensionality;
2. For any integer q, the set $[q]$ of E-elements of q is finite;
3. For any finite set of integers $\{p_1, \ldots, p_n\}$, there exists a unique integer q such that $[q] = \{p_1, \ldots, p_n\}$;
4. The structure $(\mathbb{N}, E)$ is a model of ZFC_{fin}, and the Axiom of Infinity is not satisfied in this structure.

Chapter 5

Well-Ordering and Proof by Induction

5.1 Proof by Induction

5.1.1 Simple Induction Proof

Theorem 5.1 Let $\mathcal{P}(n)$ be a predicate dependent on an element n of $\mathbb{N}$.

Assume that $\mathcal{P}(0)$ is true. (Base Case)

Also assume that for every integer n, the implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ is true. (Inductive Step)

1. Then the proposition $\mathcal{P}(n)$ is true for all integers n.

Proof. We use proof by contradiction.

Let $E = \{n \in \mathbb{N} \mid \mathcal{P}(n) \text{ is false}\}$.

As a non-empty subset of $\mathbb{N}$, the set E has a smallest element n_0.

n_0 is different from 0 because we assumed $\mathcal{P}(0)$ is true. Since $0 < n_0$, we know that $n_0 - 1 \in \mathbb{N}$.

$\mathcal{P}(n_0 - 1)$ is true because $n_0 - 1 \notin E$.

By the induction hypothesis $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$, it follows that $\mathcal{P}(n_0)$ is true, which contradicts the fact that $n_0 \in E$.

This method of proof uses the principle known as the "well-ordering principle."

Example. Consider the sequence defined by the recurrence relation:

$$\begin{cases} u_0 = \frac{1}{2} \\ u_{n+1} = \frac{1+u_n^2}{2}, \forall n \geq 0 \end{cases}$$

We will show by induction that $(u_n)_{n\in\mathbb{N}}$ is bounded above by 1.

For $n = 0$, we have $u_0 = \frac{1}{2} \leq 1$.

Assume now that the proposition is true for n and show it for $n + 1$.

Note that the terms of the sequence are positive.

$$0 \leq u_n \leq 1 \Rightarrow u_n^2 \leq 1 \Rightarrow u_n^2 + 1 \leq 1 + 1 \Rightarrow \frac{1 + u_n^2}{2} \leq \frac{2}{2} = 1$$

5.1.2 Proof Schema Using the Well-Ordering Principle

1. Define the set $E = \{n \in \mathbb{N} \mid \mathcal{P}(n) \text{ is false}\}$.

2. Assume that E is non-empty as the basis for a proof by contradiction.

3. Since $\mathbb{N}$ is well-ordered, there is a smallest element n_0 in E.

4. The smallest element cannot be the starting proposition. Use the inductive step to reach a contradiction.

Example.

Consider the sequence defined by the recurrence relation:

$$\begin{cases} u_0 = \frac{1}{2} \\ u_{n+1} = \frac{1+u_n^2}{2}, \forall n \geq 0 \end{cases}$$

We will show by the well-ordering principle that $(u_n)_{n\in\mathbb{N}}$ is bounded above by 1. We use proof by contradiction.

Let $E = \{n \in \mathbb{N} \mid u_n > 1\}$.

As a non-empty subset of $\mathbb{N}$, the set E has a smallest element n_0. Since n_0 is different from 0, because $u_0 = \frac{1}{2} \leq 1$.

Since $0 < n_0$, we know that $n_0 - 1 \in \mathbb{N}$ and $n_0 - 1 \notin E$.

$0 \leq u_{n_0-1} \leq 1 \Rightarrow u_{n_0-1}^2 \leq 1 \Rightarrow u_{n_0-1}^2+1 \leq 1+1 \Rightarrow \frac{1+u_{n_0-1}^2}{2} \leq \frac{2}{2} = 1 \Rightarrow u_{n_0} \leq 1 \Rightarrow u_{n_0} \notin E.$

This contradicts the fact that $n_0 \in E$.

Example (Importance of Base Case)

Is $3^{2n+4} - 2^n$ a multiple of 7?

Assume that $3^{2n+4} - 2^n$ is a multiple of 7.

We will show that $3^{2(n+1)+4} - 2^{n+1}$ is a multiple of 7.

We have

$$3^{2n+6} - 2^{n+1} = 9 \times 3^{2n+4} - 2 \times 2^n = (7+2) \times 3^{2n+4} - 2 \times 2^n$$

$$= 7 \times 3^{2n+4} + 2 \times 3^{2n+4} - 2 \times 2^n$$

Therefore, we have the sum of two multiples of 7, which is also a multiple of 7.

Here, the base case fails for $n = 0$ because $3^4 - 2^0 = 80$, which is not divisible by 7.

We can demonstrate using congruences that $3^{2n+4} - 2^n$ is not a multiple of 7.

Indeed, we have:

$3^2 \equiv 2 \pmod 7 \Rightarrow 3^{2n} \equiv 2^n \pmod 7$, and $3^4 \equiv 4 \pmod 7$, thus $3^{2n+4} \equiv 4 \cdot 2^n \pmod 7$.

Also, $2^n \equiv 2^n \pmod 7$, so $3^{2n+4} - 2^n \equiv 3 \cdot 2^n \pmod 7$.

Since 7 does not divide 3 or 2, it follows that 7 does not divide $3^{2n+4} - 2^n$.

Remark. To show that a proposition $\mathcal{P}(n)$ is true for all integers $n \geq n_0$, replace the base case assumption with $\mathcal{P}(n_0)$ is true.

Example. Simple Induction Proof (with a step greater than 1)

The Fibonacci sequence is given by

$$\begin{cases} F_0 = 0. \\ F_1 = 1. \\ \forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n. \end{cases}$$

Let $\varphi = \frac{1+\sqrt{5}}{2}$ and $\varphi' = \frac{1-\sqrt{5}}{2}$ (where φ is called the golden ratio). We have φ and φ' as solutions of the equation $x^2 - x - 1 = 0$.

Question : Show that for all $n \geq 1$, we have $F_n \leq \varphi^{n-1}$.

Answer : For $n = 1$, we have $F_1 = 1 \leq 1 = \varphi^0$.

For $n = 2$, we have $F_2 = F_1 + F_0 = 1 \leq \frac{1+\sqrt{5}}{2} = \varphi^1$.

We need to prove that :

$\forall n \geq 1 : \mathcal{P}(n) \wedge \mathcal{P}(n+1) \Rightarrow \mathcal{P}(n+2)$

By definition

$\forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^n + \varphi^{n-1}$ (By induction hypotheses)

$\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi + 1) \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi^2) \quad (\text{since } \varphi^2 - \varphi - 1 = 0)$

Therefore, $\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n+1}$

5.1.3 Generalized Proof by Induction

Theorem 5.2 Let $\mathcal{P}(n)$ be a proposition depending on an element n of $\mathbb{N}$.

Assume that $\mathcal{P}(0)$ is true. (Initialization)

Assume also that for every integer n, the implication $(\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \ldots \wedge \mathcal{P}(n)) \Rightarrow \mathcal{P}(n+1)$ is true. (Inductive Step)

Then the proposition $\mathcal{P}(n)$ is true for all integers n.

Proof. Let $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \ldots \wedge \mathcal{P}(n) = Q(n)$.

We will show that $Q(n)$ is true for all values of $\mathbb{N}$ if and only if $\mathcal{P}(n)$ is true for all values of $\mathbb{N}$.

Here, we need to show an equivalence, so we must demonstrate two implications.

Implication n°1

We will show that if $Q(n)$ is true for all values of $\mathbb{N}$, then $\mathcal{P}(n)$ is true for all values of $\mathbb{N}$.

Since $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \ldots \wedge \mathcal{P}(n)$ is true, it follows that $\mathcal{P}(0)$ is true and $\mathcal{P}(1)$ is true ... and $\mathcal{P}(n)$ is true, so $\mathcal{P}(n)$ is true.

Implication n°2

We will show that if $\mathcal{P}(n)$ is true for all values of $\mathbb{N}$, then $Q(n)$ is true for all values of $\mathbb{N}$.

Since $\mathcal{P}(n)$ is true for all values of $\mathbb{N}$, it follows that $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \ldots \wedge \mathcal{P}(n)$ is also true, and thus $Q(n)$ is true for all values of $\mathbb{N}$.

Example. Demonstrate that every integer $n \geq 2$ can be uniquely factored into a product of prime factors.

Proof.

Let $P(n)$ be the property: every integer k in $\{2, 3, 4, \ldots, n-1, n\}$ can be factored into a product of prime factors.

i) $P(2)$ is true because $2 = 2$.

ii) Assume that $P(k)$ is true for all natural numbers $2 \leq k \leq n$. We need to prove that $P(n+1)$ is true.

- If $n+1$ is prime, it can be written as $n+1 = n+1$.
- If $n+1$ is not prime, it has a prime divisor p, and we have $n+1 = q \cdot p$. We must have $q \leq n$, and by assumption (ii), q can be factored into a product of prime factors.

Therefore, $P(n+1)$ is true.

5.1.4 Strong Induction

Theorem 5.3 Let $\mathcal{P}$ be a proposition depending on an element n of $\mathbb{N}$.

If for every n we have: $\forall k < n : \mathcal{P}(k) \Rightarrow \mathcal{P}(n)$

Then the proposition $\mathcal{P}(n)$ is true for all integers n.

Proof. We perform a generalized proof by induction on n.

For $n = 0$:

$\forall k < 0 : \mathcal{P}(k)$ This proposition is true because k belongs to the empty set.

Assume that the proposition $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \ldots \wedge \mathcal{P}(n)$ is true and show that $\mathcal{P}(n+1)$.

Since $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \ldots \wedge \mathcal{P}(n)$ is true, it follows that $\forall k < n+1 : \mathcal{P}(k)$ is true.

Hence, $\mathcal{P}(n+1)$ is true.

5.1.5 Special Case of Proof by Induction (Cauchy's Induction)

Proposition 5.1 Let $P(n)$ be a predicate that satisfies:

$$\begin{cases} (i) : P(1) \text{ is true.} \\ (ii) : \forall n \in \mathbb{N} : P(n) \Rightarrow P(2n) \\ (iii) : \forall n \in \mathbb{N} : P(n+1) \Rightarrow P(n) \end{cases}$$

Then $P(n)$ is true for all values of n.

5.1.6 Proof of the Cauchy-Schwarz Inequality by Induction

Theorem 5.4 Harmonic, geometric, and arithmetic means.

Let $a_1, a_2, \ldots, a_n$ be positive real numbers. Then:

$$\frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 \cdot a_2 \cdots a_n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}$$

Equality holds if and only if all the a_i are equal.

Proof. For $n = 2$, it must be shown that $a_1 a_2 \leq \left(\frac{a_1+a_2}{2}\right)^2$, which is equivalent to $(a_1 - a_2)^2 \geq 0$, and this is true.

We will show $P(n) \Rightarrow P(n-1)$. Let $A = \sum_{k=1}^{n-1} \frac{a_k}{n-1}$, then:

$$\left(\prod_{k=1}^{n-1} a_k\right) A \overset{P(n)}{\leq} \left(\sum_{k=1}^{n-1} \frac{a_k + A}{n}\right)^n = \left(\frac{(n-1)A + A}{n}\right)^n = A^n$$

5.2 Well-Founded Order

5.2.1 Order and Strict Order

Definition 5.1 Let $\mathcal{R}$ be a binary relation on E.

- We say that $\mathcal{R}$ is reflexive if: $\forall x \in E, x\mathcal{R}x$.
- We say that $\mathcal{R}$ is symmetric if: $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- We say that $\mathcal{R}$ is antisymmetric if: $\forall (x, y) \in E^2, x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$.
- We say that $\mathcal{R}$ is transitive if: $\forall (x, y, z) \in E^3, x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Definition 5.2 A binary relation is an order relation if it is reflexive, antisymmetric, and transitive.

Example. The set $\mathbb{R}$ with the usual order relation ($\leq$).

Thus $\prod_{k=1}^{n-1} a_k \leq A^{n-1} = \left(\sum_{k=1}^{n-1} \frac{a_k}{n-1}\right)^{n-1}$

We now prove that $P(n) \Rightarrow P(2n)$:

$$\prod_{k=1}^{2n} a_k = \left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=n+1}^{2n} a_k\right) \overset{P(n)}{\leq} \left(\sum_{k=1}^{n} \frac{a_k}{n}\right)^n \left(\sum_{k=n+1}^{2n} \frac{a_k}{n}\right)^n$$
$$\overset{P(2)}{\leq} \left(\frac{\sum_{k=1}^{2n} \frac{a_k}{n}}{2}\right)^{2n} = \left(\frac{\sum_{k=1}^{2n} a_k}{2n}\right)^{2n}$$

The left inequality follows from the previous one by considering $\frac{1}{a_1}, \ldots, \frac{1}{a_n}$.

Example. On the set of subsets of a set, the relation $\subset$ is an order relation.

Definition 5.3 A binary relation is a strict order relation if it is transitive and anti-reflexive.

$$\mathcal{R} \text{ anti-reflexive } : \forall x \in E : x \not\mathcal{R} x$$

Example. The set $\mathbb{R}$ with the relation $<$.

Proposition 5.2 A strict order relation is antisymmetric.

Proof. $\mathcal{R}$ is by definition transitive and anti-reflexive.

A relation is antisymmetric if it satisfies:

$$\forall (x, y) \in E^2, \quad (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$$

We will show that in a strict order relation, the proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ is always false.

We use proof by contradiction.

Assume there exists $(x, y) \in E^2$ such that the proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ is true. Then by transitivity, we get $x\mathcal{R}x$, which contradicts the fact that $\mathcal{R}$ is anti-reflexive.

Therefore, the proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ is always false, and thus the logical implication $(x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$ is always true.

Definition 5.4 Let $(E, \mathcal{R})$ be an ordered set. Two elements x and y are said to be comparable if $x\mathcal{R}y$ or $y\mathcal{R}x$. Otherwise, x and y are said to be incomparable.

Example. Let $\mathcal{P}(\{a, b, c\})$ - the power set of $\{a, b, c\}$ - with the order relation $\subset$.

The elements $\{a, b\}$ and $\{b, c\}$ are incomparable.

Definition 5.5 An order $\mathcal{R}$ on E is said to be total if any two elements are always comparable: $\forall (x, y) \in E, x\mathcal{R}y$ or $y\mathcal{R}x$.

An order that is not total is said to be partial.

Definition 5.6 A strict order is said to be total if any two distinct elements are always comparable:

$$\forall (x, y) \in E, x \neq y \Rightarrow x\mathcal{R}y \text{ or } y\mathcal{R}x$$

Remark. In what follows, we will denote an order relation by $\preceq$ and a strict order relation by $\prec$.

5.2.2 Minorants, Majorants, Minimizers, and Maximizers

Definition 5.7 Let $(E, \preceq)$ be an ordered set and F a non-empty subset of E.

We say that $x \in E$ is a lower bound of F if:

$$\forall y \in F, x \preceq y$$

If the lower bound of F is an element of F, it is called the smallest element or the minimum of F.

We say that $x \in E$ is an upper bound of F if:

$$\forall y \in F, y \preceq x$$

If the upper bound of F is an element of F, it is called the largest element or the maximum of F.

Definition 5.8 Let $(E, \preceq)$ be an ordered set and F a non-empty subset of E.

- An element x is a minimal element of F when no element of F is strictly smaller than x:

$$\forall y \in F, y \preceq x \Rightarrow x = y$$

- An element x is a maximal element of F when no element of F is strictly larger than x:

$$\forall y \in F, x \preceq y \Rightarrow x = y$$

Remark. If the relation is a total order, then the notions of minimal element and minimum coincide (the same remark applies to the notions of maximal element and maximum).

Example. 0 is a minimal element of $(\mathbb{N}, \leq)$ and is also its minimum.

Example. Consider the set $\mathcal{P}(\{a, b, c\})\backslash\{\varnothing\}$ with the partial order $\subset$. The elements $\{a\}, \{b\}, \{c\}$ are minimal elements, but there is no minimum.

Bibliography

[1] P. Franceschi. *Introduction à la philosophie analytique: paradoxes, arguments et problèmes contemporains*. Paul Franceschi, 2015.

[2] S. Fratani *et al.* *Cours Logique et Calculabilité*, L3 Informatique, 2015. Available at: https://pageperso.lislab.fr/luigi.santocanale/teaching/1415teaching/LC/DOCS/old/cours_2303-2015.pdf.

[3] C. Huayi. *Notes du cours: Introduction aux raisonnements mathématiques*, 2008. Available at: http://www-fourier.ujf-grenoble.fr/huayi/Enseignments/ParisVIII/2007_2008/logique.pdf.

[4] T. Seiller. *Théorie des Ensembles*, 2010. Available at: http://www.pps.univ-paris-diderot.fr/seiller/documents/thens.pdf.

[5] O. Simon. *Nombres réels*, 2005. Available at: http://capes-math.univ-rennes1.fr/cours-pdf/reels.pdf.

[6] F. Sturm. *Cours de mathématiques - ASINSA-1: Introduction à la logique mathématique*, 2013. Available at: http://maths.insalyon.fr/fsturm/TELECHARGEMENT/COURSASINSA1/che_cours_ASINSA1_logique.pdf.

[7] A. Torres. *Introduction à la logique*, 2003. Available at: http://www.adelino-torres.com/metodologia/INTRODU%C3%87%C3%83O.pdf.

[8] J. Vélu. *Méthodes mathématiques pour Informaticiens*. Dunod, 2003.

[9] Wikipedia. *Logique intuitionniste*. Available at: https://fr.wikipedia.org/wiki/Logique_intuitionniste.

[10] Wikipedia. *Paradoxe de Russell*. Available at: https://fr.wikipedia.org/wiki/Paradoxe_de_Russell.

[11] Wikipedia. *Paradoxe du barbier*. Available at: https://fr.wikipedia.org/wiki/Paradoxe_du_barbier.

[12] Wikipedia. *Paradoxe du menteur*. Available at: https://fr.wikipedia.org/wiki/Paradoxe_du_menteur.

[**13**] Wikipedia. *Paradoxe de Cantor*. Available at: https://fr.wikipedia.org/wiki/Paradoxe_de_Cantor.

[**14**] Wikipedia. *Paradoxe de Richard*. Available at: https://fr.wikipedia.org/wiki/Paradoxe_de_Richard.

[**15**] Wikipedia. *Paradoxe de Grelling-Nelson*. Available at: https://fr.wikipedia.org/wiki/Paradoxe_de_Grelling-Nelson.