Foundations of Computer Science
Logic, models, and computations

Chapter: Propositional calculus

Course CSC_41012_EP

of l'Ecole Polytechnique

Olivier Bournez

bournez@lix.polytechnique.fr

Version of August 20, 2024

Propositional calculus

The *propositional logic* provides means to discuss logical grammatical connectors such as *negation*, *disjunction* or *negation*, by composition starting some Boolean propositions. These connectors are sometimes called *Aristotelian* as they have been pointed out by Aristotle.

The *propositional logic* permits essentially to talk about *Boolean functions*, that is to say about functions from $\{0,1\}^n \to \{0,1\}$. Indeed, the variables, that is to say the *propositions* can only take two values, *true* or *false*.

The propositional calculus has an important position in computer science. A first reason is because today's computers are digital and working in *binary*. This has the consequence that our processors are essentially made of binary gates of the type that we will study in this chapter.

From a point of view of expressive power, propositional calculus remains very limited. For example, one cannot express in propositional calculus the existence of an object with a given property. The predicate calculus, more general, that we will study in Chapter 5, provides means to express some properties of objects and relations between objects, and more generally to formalise the mathematical reasoning.

Since the propositional calculus provides anyway the common basis to numerous logical systems, we will take some time on it in this chapter.

1 Syntax

To define formally and properly this language, we must distinguish the *syntax* from the *semantic*: The *syntax* describes how formulas are written. The *semantic* describes their meaning.

Fix a finite or denumerable set $\mathscr{P} = \{p_0, p_1, \cdots\}$ of symbols that are called *propositional variables*.

Definition 1 (Propositional formulas) *The set of propositional formulas $\mathscr{F}$ over $\mathscr{P}$ is the language over the alphabet $\mathscr{P} \cup \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, (,)\}$ defined inductively by the following rules: ,,,,*

(*B*) *it contains $\mathscr{P}$: Every propositional variable is a propositional formula;*

(*I*) *If $F \in \mathscr{F}$ then $\neg F \in \mathscr{F}$;*

(*I*) *If* $F,G \in \mathscr{F}$ *then* $(F \wedge G) \in \mathscr{F}$, $(F \vee G) \in \mathscr{F}$, $(F \Rightarrow G) \in \mathscr{F}$, *and* $(F \Leftrightarrow G) \in \mathscr{F}$.

It is an inductive definition that is valid by the considerations of the previous chapter: It is a non-unambiguous definition. This can be reformulated by the following proposition, that is sometimes called *unique reading theorem of propositional calculus*.

Remark 1 *The non-ambiguity comes essentially from the explicit parentheses. We use here the trick in the previous chapter that was considering* $Arith'$ *instead of* $Arith$ *to allow to write some expressions without any reading ambiguity.*

Proposition 1 (Decomposition / Uniqueness reading) *Let* F *be a propositional formula. Then* F *is of one, and exactly one of the following forms:*

1. *a propositional formula* $p \in \mathscr{P}$;
2. $\neg G$, *where* G *is a propositional formula;*
3. $(G \wedge H)$ *where* G *and* H *are some propositional formulas;*
4. $(G \vee H)$ *where* G *and* H *are some propositional formulas;*
5. $(G \Rightarrow H)$ *where* G *and* H *are some propositional formulas;*
6. $(G \Leftrightarrow H)$ *where* G *and* H *are some propositional formulas.*

Moreover, in the cases 2., 3., 4., 5. and 6., there is unicity of the formula G *and unicity of the formula* H *with these properties.*

The fact that a formula can always be decomposed into one of the 6 cases above is easy to establish inductively. The unicity of the decomposition follows from the following exercise:

p	$\neg p$	q	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	1	0	0	0	1	1
1	0	0	1	0	0	0
0	1	1	1	0	1	0
1	0	1	1	1	1	1

Figure 1: Truth value.

Exercise 1 *Prove that the previous inductive definition is* non-ambiguous, *that is that G and H are uniquely defined in each of the cases above.*
We can proceed in the following way.

- *Prove that in any formula F the number of open parentheses is equal to the number of closing parentheses.*
- *Prove that in any word M prefix of the word F, we have $o(M) \geq f(M)$, where $o(M)$ is the number of open parentheses, and $f(M)$ the number of closing parentheses.*
- *Prove that in any formula F whose first symbol is some open parenthesis, and for any word M proper prefix of F, we have $o(M) > f(M)$.*
- *Prove that any word M proper prefix of F is not a formula.*
- *Deduce the result.*

We call *subformula* of F a formula that appears in the recursive decomposition of F.

2 Semantic

We are going now to define the *semantic* of a propositional formula, that is to say, the meaning that is assigned to such a formula.

The *truth value* of a formula is defined as the interpretation of this formula, after having fixed the truth value of the propositional variables: The principle is to interpret the symbols $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$ by the logic $negation$, the logical or (also called disjunction), the logical and (also called conjunction), the implication and the *double implication* (also called *equivalence*)).

Formally,

Definition 2 (Valuation) *A* valuation *is a distribution of truth value to the propositional variables, that is to say a function from $\mathscr{P}$ to* $\{0,1\}$.

In all what follows, 0 represents false, and 1 represents true.

The conditions in the following definition are often represented as a *truth value*: See Figure 1.

Proposition 2 *Let v be a valuation.*
By Theorem 2.5, there exists a unique function $\overline{v}$ defined on all $\mathscr{F}$ that satisfies the following conditions:

- (B) *$\overline{v}$ extends v: for every propositional variable $p \in \mathscr{P}$, $\overline{v}(p) = v(p)$;*
- (I) *the negation is interpreted by logic negation: if F is of the form $\neg G$, then $\overline{v}(F) = 1$ if and only if $\overline{v}(G) = 0$;*
- (I) *$\wedge$ is interpreted as the logical and: if F is of the form $G \wedge H$, then $\overline{v}(F) = 1$ if and only if $\overline{v}(G) = 1$ and $\overline{v}(H) = 1$;*
- (I) *$\vee$ is interpreted as the logical or: if F is of the form $G \vee H$, then $\overline{v}(F) = 1$ if and only if $\overline{v}(G) = 1$ or $\overline{v}(H) = 1$;*
- (I) *$\Rightarrow$ is interpreted as the logical implication: if F is of the form $G \Rightarrow H$, then $\overline{v}(F) = 1$ if and only if $\overline{v}(H) = 1$ or $\overline{v}(G) = 0$;*
- (I) *$\Leftrightarrow$ is interpreted as the logical equivalence: if F is of the form $G \Leftrightarrow H$, then $\overline{v}(F) = 1$ if and only if $\overline{v}(G) = \overline{v}(H)$.*

We write $v \models F$ for $\overline{v}(F) = 1$, and we say that v is *a model* of F, or that v satisfies F. We write $v \not\models F$ otherwise. The value of $\overline{v}(F)$ for the valuation v is called the *truth value of F on v*.

3 Tautologies, equivalent formulas

We would like to classify the formulas according to their interpretations. A particular class of formulas are those that are always trues, and that are called the *tautologies*.

Definition 3 (Tautology) *A* tautology *is a formula F that is satisfied by any valuation. We write in this case $\models F$.*

Definition 4 (Equivalence) *Two formulas F and G are said to be* equivalent *if for every valuation v, $\overline{v}(F) = \overline{v}(G)$. We write in this case $F \equiv G$.*

Example 1 *The formula $p \vee \neg p$ is a tautology. The formulas p and $\neg\neg p$ are equivalent.*

Remark 2 *It is important to understand that $\equiv$ is a symbol that is used to write a relation between formulas, but that $F \equiv G$ is not a propositional formula.*

Exercise 2 *Prove that $\equiv$ is some equivalence relation on the formulas.*

4 Some elementary facts

Exercise 3 *Prove that for any formulas F and G, the following formulas are tautologies:*

$$(F \Rightarrow F),$$

$$(F \Rightarrow (G \Rightarrow F)),$$

$$(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H)).$$

Exercise 4 *[Idempotence] Prove that for any formula F we have the equivalences:*

$$(F \vee F) \equiv F,$$

$$(F \wedge F) \equiv F.$$

Exercise 5 *[Associativity] Prove that for any formulas F, G, H we have the equivalences:*

$$(F \wedge (G \wedge H)) \equiv ((F \wedge G) \wedge H),$$

$$(F \vee (G \vee H)) \equiv ((F \vee G) \vee H).$$

Because of associativity, one often denotes $F_1 \vee F_2 \vee \cdots \vee F_k$ for $(((F_1 \vee F_2) \vee F_3) \cdots \vee F_k)$, and $F_1 \wedge F_2 \wedge \cdots \wedge F_k$ for $(((F_1 \wedge F_2) \wedge F_3) \cdots \wedge F_k)$.

Remark 3 *Exactly as we do for arithmetic expression: We write $1+2+3$ for $((1+2)+3)$ as well as for $(1+(2+3))$. See all the discussions on $Arith$ and $Arith'$ in the previous chapter.*

Exercise 6 *[Commutativity] Prove that for any formulas F and G we have the equivalences:*

$$(F \wedge G) \equiv (G \wedge F),$$

$$(F \vee G) \equiv (G \vee F).$$

Exercise 7 *[Distributivity] Prove that for any formulas F, G, H we have the equivalences:*

$$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H)),$$

$$(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H)).$$

Exercise 8 *[Morgan's law] Prove that for any formulas F and G we have the equivalences:*

$$\neg(F \wedge G) \equiv (\neg F \vee \neg G),$$

$$\neg(F \vee G) \equiv (\neg F \wedge \neg G).$$

Exercise 9 *[Absorption] Prove that for any formulas F and G we have the equivalences:*

$$(F \wedge (F \vee G)) \equiv F,$$

$$(F \vee (F \wedge G)) \equiv F.$$

5 Replacement of a formula by some equivalent formula

We know now some *equivalences* between formulas, but we are going to convince ourselves that one can use these equivalences in a *compositional* way: If one replaces in some formula some subformula by some equivalent formula, then one obtains an equivalent formula.

5.1 A simple remark

Observe first that the truth value of a formula is depending only on the propositional formulas that appear in the formula: When F is a formula, we will write $F(p_1, \cdots, p_n)$ to say that the formula F is written with the propositional formulas $p_1, \cdots, p_n$ only.

Proposition 3 *Let $F(p_1,\cdots,p_n)$ be a formula. Let v be some valuation. The truth value of F on v is depending only on the value of v on $\{p_1,p_2,\cdots,p_n\}$.*

Proof: The property can be established easily by structural induction. □

5.2 Substitutions

We have to defined what means replacing p by G in a formula F, denoted by $F(G/p)$.

This provides the rather pedantic definition, but we have to go through this:

Definition 5 (Substitution of p by G in F) *The formula $F(G/p)$ is defined by induction on the formula F:*

(*B*) *If F is the propositional formula p, then $F(G/p)$ is the formula G;*

(*B*) *If F is a propositional formula q, with $q \neq p$, then $F(G/p)$ is the formula F;*

(*I*) *If F is of the form $\neg H$, then $F(G/p)$ is the formula $\neg H(G/p)$;*

(*I*) *If F is of the form $(F_1 \vee F_2)$, then $F(G/p)$ is the formula $(F_1(G/p) \vee F_2(G/p))$;*

(*I*) *If F is of the form $(F_1 \wedge F_2)$, then $F(G/p)$ is the formula $(F_1(G/p) \wedge F_2(G/p))$;*

(*I*) *If F is of the form $(F_1 \Rightarrow F_2)$, then $F(G/p)$ is the formula $(F_1(G/p) \Rightarrow F_2(G/p))$;*

(*I*) *If F is of the form $(F_1 \Leftrightarrow F_2)$, then $F(G/p)$ is the formula $(F_1(G/p) \Leftrightarrow F_2(G/p))$.*

5.3 Compositionality

We obtain the promised result: If one replaces in a formula some subformula by some equivalent formula, then one obtains an equivalent formula;

Proposition 4 *Let F, F', G and G' be formulas. Let p be a propositional variable.*

- *If F is a tautology, then $F(G/p)$ is also a tautology.*
- *If $F \equiv F'$, then $F(G/p) \equiv F'(G/p)$.*
- *If $G \equiv G'$ then $F(G/p) \equiv F(G'/p)$.*

Exercise 10 *Prove the result by structural induction.*

6 Complete systems of connectors

Proposition 5 *Every propositional formula is equivalent to a propositional formula that is built only with the connectors $\neg$ and $\wedge$.*

Proof: This results from a proof by induction on the formula. This is true for the formulas that correspond to some propositional variable. Suppose the property true for the formulas G and H, that is to say suppose that G (respectively H) is equivalent to some formula G' (respectively H') built only with the connectors $\neg$ and $\wedge$.

If F is of the form $\neg G$, then F is equivalent to $\neg G'$, and the induction hypothesis is preserved.

If F is of the form $(G \wedge H)$, then F is equivalent to $(G' \wedge H')$, and the induction hypothesis is preserved.

If F is of the form $(G \vee H)$, by using the second Morgan's law, and the fact that $K \equiv \neg\neg K$ to eliminate the double negations, we obtain that $F \equiv \neg(\neg G' \wedge \neg H')$, which is indeed built using only the connectors $\neg$ and $\wedge$.

If F is of the form $(G \Rightarrow H)$, then F is equivalent to $(\neg G' \vee H')$ that is equivalent to a formula build uniquely with the connectors $\neg$ and $\wedge$ by the previous cases.

If F is of the form $(G \Leftrightarrow H)$, then F is equivalent to $(G' \Rightarrow H') \wedge (H' \Rightarrow G')$ that is equivalent to a formula build uniquely with the connectors $\neg$ and $\wedge$ by the previous cases. □

A set of connectors with the above property for $\{\neg, \wedge\}$ is called a complete system of connectors.

Exercise 11 *Prove that $\{\neg, \vee\}$ is also a complete system of connectors.*

Exercise 12 *Give a binary logic connector that, alone, constitutes a complete system of connectors.*

7 Functional completeness

Suppose that $\mathscr{P} = \{p_1, p_2, \cdots, p_n\}$ is finite. Let V be the set of valuations on $\mathscr{P}$. Since a valuation is a function from $\{1, 2, \ldots, n\}$ to $\{0, 1\}$, V contains 2^n elements.

Each formula F over $\mathscr{P}$ can be seen as a function from V to $\{0, 1\}$, that is called its *truth value of F*: This function is the function that, to a valuation v associates the truth value of this formula on the valuation.

There are 2^{2^n} functions from V to $\{0, 1\}$. The question that one may ask is to know if all these functions can be written as formulas. The answer is positive:

Theorem 1 (Functional completeness) *Suppose $\mathscr{P} = \{p_1, p_2, \cdots, p_n\}$ is finite. Let V be the set of valuations over $\mathscr{P}$. Every function f from V to $\{0, 1\}$ is the truth value of some formula F over $\mathscr{P}$.*

Proof: The proof is done by recurrence on the number of propositional variables n.

For $n = 1$, there are four functions from $\{0,1\}^1$ to $\{0,1\}$, that are represented by the formulas p, $\neg p$, $p \vee \neg p$, $p \wedge \neg p$.

Suppose that the property is true for $n-1$ propositional variables. Consider $\mathscr{P} = \{p_1, \cdots, p_n\}$ and let f be a function from $\{0,1\}^n$ to $\{0,1\}$. Each valuation v' over $\{p_1, p_2, \cdots, p_{n-1}\}$ can be seen as the restriction of a valuation on $\{p_1, \cdots, p_n\}$. Let f_0 (respectively f_1) the restriction of f to the valuation v such that $v(p_n) = 0$ (resp. $v(p_n) = 1$). The functions f_0 and f_1 are some functions defined on valuations over $\{p_1, \cdots, p_{n-1}\}$ to $\{0,1\}$ and can be represented by formulas $G(p_1, \cdots, p_{n-1})$ and $H(p_1, \cdots, p_{n-1})$ respectively by recurrence hypothesis. The function f can then be represented by the formula

$$(\neg p_n \wedge G(p_1, \cdots, p_{n-1})) \vee (p_n \wedge H(p_1, \cdots, p_{n-1}))$$

which proves the recurrence hypothesis at rank n. □

Remark 4 *Our attentive reader will have observed that the Proposition 5 can be seen as a consequence of this proof.*

8 Normal forms

8.1 Conjunctive and disjunctive normal forms

One often seeks to transform the formulas into some equivalent form as simple as possible.

Definition 6 *A* literal *is a propositional formula or its negations, i.e. of the form p, or $\neg p$, for $p \in \mathscr{P}$.*

Definition 7 *A* disjunctive normal form *is a disjunction $F_1 \vee F_2 \cdots \vee F_k$ of k formulas, $k \geq 1$ where each formula F_i, $1 \leq i \leq k$ is a conjunction $G_1 \wedge G_2 \cdots \wedge G_\ell$ of ℓ literals (ℓ can possibly depend on i).*

Example 2 *The following formulas are in disjunctive normal form*

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

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

$$(p \wedge \neg q)$$

Definition 8 *A* conjunctive normal form *is a conjunction $F_1 \wedge F_2 \cdots \wedge F_k$ of k formulas, $k \geq 1$ where each formula F_i, $1 \leq i \leq k$ is a disjunction $G_1 \vee G_2 \cdots \vee G_\ell$ of ℓ literals (ℓ can possibly depend on i).*

Example 3 *The following formulas are in conjunctive normal form*

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

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

$$(\neg p \vee q)$$

Theorem 2 *Every formula on a finite number of propositional variables is equivalent to some formula in conjunctive normal form.*

Theorem 3 *Every formula on a finite number of propositional variables is equivalent to some formula in disjunctive normal form.*

Proof: These two theorems are proved by recurrence on the number n of propositional formulas.

In the case where $n = 1$, we have already considered in the previous proofs some formulas covering all the possible cases, and which are actually both in conjunctive normal form and disjunctive normal form.

We suppose the property true for $n-1$ propositional variables. Let f be the truth value associated to the formula $F(p_1, \cdots, p_n)$. As in the previous proof, we can build some formula that represents f, by writing a formula of the form

$$(\neg p_n \wedge G(p_1, \cdots, p_{n-1})) \vee (p_n \wedge H(p_1, \cdots, p_{n-1})).$$

By recurrence hypothesis, G and H are equivalent to formulas in disjunctive normal form

$$G \equiv (G_1 \vee G_2 \vee \cdots \vee G_k)$$

$$H \equiv (H_1 \vee H_2 \vee \cdots \vee H_\ell)$$

We can then write

$$(\neg p_n \wedge G) \equiv (\neg p_n \wedge G_1) \vee (\neg p_n \wedge G_2) \vee \cdots \vee (\neg p_n \wedge G_k)$$

which is in disjunctive normal form and

$$(p_n \wedge H) \equiv (p_n \wedge H_1) \vee (p_n \wedge H_2) \vee \cdots \vee (p_n \wedge H_k)$$

which is also in disjunctive normal form. The function f is hence represented by the disjunction of these two formulas, and hence by a formula in disjunctive normal form.

If we want to obtain F in conjunctive normal form, then the hypothesis induction produces two conjunctive normal form G and H. The equivalence that is used is then

$$F \equiv ((\neg p_n \vee H) \wedge (p_n \vee G)).$$

□

Remark 5 *Our attentive reader would have observed that the previous theorem, as well as Proposition 5 can also be seen as the consequences of this proof.*

8.2 Transformation methods

In practise, there exist two main methods to determine the disjunctive normal form, or the conjunctive normal form of a given formula. The first method consists in transforming the formula by successive equivalence by using the following rules applied in this order:

1. elimination of connectors $\Rightarrow$ by

$$(F \Rightarrow G) \equiv (\neg F \vee G)$$

2. entering the negation in the innermost position:

$$\neg(F \wedge G) \equiv (\neg F \vee \neg G)$$

$$\neg(F \vee G) \equiv (\neg F \wedge \neg G)$$

3. distributivity of $\vee$ and $\wedge$ one with respect to the other

$$F \wedge (G \vee H)) \equiv ((F \wedge H) \vee (F \wedge H))$$

$$F \vee (G \wedge H)) \equiv ((F \vee H) \wedge (F \vee H))$$

Example 4 *Put the formula $\neg(p \Rightarrow (q \Rightarrow r)) \vee (r \Rightarrow q)$ in disjunctive and conjunctive normal form.*

We use the successive equivalences

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

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

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

that is a disjunctive normal form.

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

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

The other method consists in determining the valuations v such that $\overline{v}(F) = 1$, and to write a disjunction of conjunctions, each conjunction corresponding to a valuation for which $\overline{v}(F) = 1$.

The determination of a conjunctive normal form follows the same principle, by exchanging the valuations that value 1 with the valuations giving the value 0, by exchanging conjunctions and disjunctions.

Exercise 13 *Prove that the conjunctive and disjunctive normal form of a formula can be exponentially longer than the size of the formula. The* size of a formula *is defined as the length of the formula seen as a word.*

9 Compactness theorem

9.1 Satisfaction of a set of formulas

We are given this times a set Σ of formulas. One wants to know when it is possible to satisfy all the formulas of Σ.

Let's start by fix the terminology.

Definition 9 *Let Σ be a set of formulas.*

- *A valuation* satisfies Σ *if it satisfies each formula of Σ. One also says in that case that this valuation is* a model *of Σ.*
- *Σ is said* consistent *(this is also called* satisfiable*) if it has a model. In other words, if there exists some valuation that satisfies Σ.*
- *Σ is said* inconsistent*, or* contradictory*, in the opposite case*

Definition 10 (Consequence) *Let F be a formula. The formula F is said to a* consequence *of Σ if every model of Σ is a model of F. We then write $\Sigma \models F$.*

Example 5 *The formula q is a consequence of the set of formulas $\{p, p \Rightarrow q\}$. The set of formulas $\{p, p \Rightarrow q, \neg q\}$ is inconsistent.*

We can get convinced first of the following results, that follows from a game on definitions.

Proposition 6 *Every formula F is a consequence of a set Σ of formulas if and only if $\Sigma \cup \{\neg F\}$ is inconsistent.*

Proof: If every valuation that satisfies Σ satisfies F, there there is no valuation satisfying $\Sigma \cup \{\neg F\}$. Conversely, by contradiction: If there is a valuation that satisfies Σ and not satisfying F, then this valuation satisfies Σ and $\neg F$. □

Exercise 14 *Prove that for any formulas F and F', $\{F\} \models F'$ if and only if $F \Rightarrow F'$ is a tautology.*

More fundamentally, we ave the following rather surprising and fundamental result.

Theorem 4 (Compactness theorem (first version)) *Let Σ be a set of formulas built on a denumerable set $\mathscr{P}$ of propositional variables.*
Then Σ is consistent if and only if every finite subset of Σ is consistent.

Remark 6 *Observe that the hypothesis $\mathscr{P}$ countable is not necessary, if we accept to use Zorn hypothesis (the axiom of choice). We will restrict to the case where $\mathscr{P}$ is denumerable in all the proofs that follow.*

Actually, this theorem can be reformulated as follows:

Theorem 5 (Compactness theorem (second version)) *Let Σ be a set of formulas built on a denumerable set $\mathscr{P}$ of propositional variables.*
Then Σ is inconsistent if and only if Σ has some finite inconsistent subset.

Or even under the following form:

Theorem 6 (Compactness theorem (third version)) *For every set Σ of propositional formulas, and for every propositional formula F built on a denumerable set $\mathscr{P}$ of propositional variables, F is a consequence of Σ if and only if F is a consequence of a finite subset of Σ.*

The equivalence of the three formulations is a simple exercise of manipulations of definitions. We will prove the first version of the theorem.

One of the implication is trivial: If Σ is consistent, then every subset of Σ is consistent, and in particular the finite subsets.

We will provide two proofs of the other implication.

A first proof that makes references to notions of topologies, in particular compactness, and that is addressed to readers who know theses notion, and who like topological arguments.

Proof:[Topological proof] The topological space $\{0,1\}^{\mathscr{P}}$ (with the product topology) is a compact space, since it is obtained as the product of compact spaces (Tychonoff theorem).

For every propositional formula $F \in \Sigma$, the set $\overline{F}$ of the valuations which satisfy it is open in $\{0,1\}^{\mathscr{P}}$, as the truth value of a formula is depending only from a finite number of propositional variables, namely those appearing in the formula. It is also closed, since those that are not satisfying F are those satisfying t $\neg F$.

The hypothesis of the theorem implies that any finite intersection of $\overline{F}$ for $F \in \Sigma$ is non-empty. Since $\{0,1\}^{\mathscr{P}}$ is compact, the intersection of all the $\overline{F}$ for $F \in \Sigma$ is hence non-empty. □

Here is a proof that avoid topology.

Proof:[Direct proof] Consider $\mathscr{P} = \{p_1, p_2, \cdots, p_k, \cdots\}$ an enumeration of $\mathscr{P}$.

We will prove the following lemma: Suppose that there exists some application v from $\{p_1, p_2, \cdots, p_n\}$ to $\{0,1\}$ such that any finite subset of Σ has a model in which $p_1, \cdots, p_n$ take the values $v(p_1)$, ..., $v(p_n)$. Then v can be extended to $\{p_1, p_2, \cdots, p_{n+1}\}$ with the same property.

Indeed, if $v(p_{n+1}) = 0$ does not fit, then there exists some finite set U_0 of Σ that cannot be satisfied when $p_1, \cdots, p_n, p_{n+1}$ take respective values $v(p_1), \ldots, v(p_n)$ and 0. If U is any finite subset of Σ, then from the hypothesis made on v, $U_0 \cup U$ has a model in which $p_1, \cdots, p_n$ take the values $v(p_1), \cdots, v(p_n)$. In this model, the proposition p_{n+1} takes the value 1. In other words, every finite subset U of Σ has a model in which $p_1, \cdots, p_n, p_{n+1}$ take the respective values $v(p_1)$, ..., $v(p_n)$ and 1. Stated in another way, either $v(p_{n+1}) = 0$ is fine with the property, in which case, we can fix $v(p_{n+1}) = 0$, or $v(p_{n+1}) = 0$ is not fine, in which case, we can set $v(p_{n+1}) = 1$ which is fine with the property.

By using this lemma, we hence define some valuation v such that, by recurrence over n, for every n, every finite set of Σ has a model in which $p_1, \cdots, p_n$ take the values $v(p_1), \ldots, v(p_n)$.

It follows that v satisfies Σ: Indeed, let F be a formula of Σ. F is depending only a finite set of propositional formulas $p_{i_1}, p_{i_2}, \cdots, p_{i_k}$ (the one appearing in F). By considering $n = \max(i_1, i_2, \cdots, i_k)$, each of these propositional variables p_{i_j} is among $\{p_1, \cdots, p_n\}$. We then know that the finite subset $\{F\}$ reduced to the formula F admits a model in which $p_1, \cdots, p_n$ take the value $v(p_1), \ldots, v(p_n)$, i.e. F is satisfied by v.

□

10 Exercises

Exercise 15 *Relate the equivalent propositions:*

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

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

Exercise 16 *By adding two numbers whose binary expression uses at most two digits, say ab and cd, we obtain a number of at most three digits pqr. For example, $11+01=100$. Give an expression of p, q and r as a function of a, b, c and d using the usual connectors.*

Exercise 17 *(solution on page 205) Let F and G two formulas with no propositional variable in common. Prove that the two following properties are equivalent:*

- *The formula $(F \Rightarrow G)$ is a tautology;*
- *At least one of $\neg F$ and G is a tautology.*

***Exercise 1** *[Interpolation theorem] Let F and F' such that $F \Rightarrow F'$ is a tautology. Prove that there exists some propositional formula C, whose propositional variables appear in F and F', such that $F \Rightarrow C$ and $C \Rightarrow F'$ are two tautologies (one can reason on recurrence on the number of variables that have at least one occurrence in F without any in F').*

Exercise 18 *(solution on page 205) [Application of compactness to graph colouring] A graph $G = (V, E)$ is k-colorable if there exists some function f from V in $\{1, 2, \ldots, k\}$ such that for all $(x, y) \in E$, $f(x) \neq f(y)$. Prove that a graph is k-colorable if and only if any of its finite sub-graphs is k-colorable .*

***Exercise 2** *[Applications of compactness to group theory] A group G is said to be totally ordered if we have on G some total order relation such that $a \leq b$ implies $ac \leq bc$ and $ca \leq cb$ for all $a, b, c \in G$. Prove that for some Abelian group G can be ordered, it is sufficient and necessary that any subgroup of G spanned by a finite set elements of G can be ordered.*

11 Bibliographic notes

Suggested readings To go further on the notions of this chapter, we suggest [Cori & Lascar, 1993] and [Lassaigne & de Rougemont, 2004].

Bibliography This chapter has been written by using essentially the books [Cori & Lascar, 1993] and [Lassaigne & de Rougemont, 2004].

Index

Bibliography

[Cori & Lascar, 1993] Cori, R. & Lascar, D. (1993). *Logique mathématique. Volume I*. Masson.

[Kreisel & Krivine, 1967] Kreisel, G. & Krivine, J., editors (1967). *Eléments de logique mathématique. Théorie des modèles*. Monographique de la société mathématique de France. Dunod Paris.

[Lassaigne & de Rougemont, 2004] Lassaigne, R. & de Rougemont, M. (2004). *Logic and complexity*. Discrete Mathematics and Theoretical Computer Science. Springer. https://doi.org/10.1007/978-0-85729-392-3