Foundations of Computer Science
Logic, models, and computations

Chapter: Predicate calculus

Course INF412

of l'Ecole Polytechnique

Olivier Bournez

bournez@lix.polytechnique.fr

Version of July 16, 2023

Predicate calculus

Propositional calculus remains very limited, and permits essentially only to talk about Boolean operations on propositions.

If we want to reason about mathematical assertions, we need some richer constructions. For example, one may want to talk about statements like

$$\forall x((Prime(x) \wedge x > \mathbf{1}+\mathbf{1}) \Rightarrow Odd(x)). \tag{1}$$

Such a statement is not captured by propositional logic. First of all, since it uses some *predicates*, such as $Prime(x)$, whose truth value is depending on some variable x, which is not possible in propositional logic. Furthermore, we use here some *quantifiers*, such as $\exists$, $\forall$ which are not present in propositional logic.

The previous statement is an example of a formula from predicate calculus of *first order*. In this course, we will only talk about *first order logic*. The terminology *first order* makes reference to the fact that the existential and universal quantifiers are authorized only on variables.

A statement of *second order* (and one talks more generally of *higher order logic*) would be a statement where quantifications over functions or relations would be authorized. For example, we may want to write $\neg\exists f(\forall x(f(x) > f(x+\mathbf{1})))$ to mean that there does not exist some infinitely decreasing sequence. We will not attempt to understand the theory under this type of statements in this document, as we will see, the problems and difficulties with first order are already sufficiently numerous.

The objective of this chapter is then to define first order logic. As for propositional logic, we will do it by talking of the *syntax*, that is to say the way formulas are written, and then of their *semantic*, that is to say, their meanings.

The *predicate calculus*, remains the most usual formalism to express mathematical properties. This is also a formalism very often used in computer science to describe objects. For example, the request languages in data bases are essentially based on this formalism, applied to some finite objects, representing data.

1 Syntax

To write a *formula* of a first order language, we will use certain symbols that are common to all the languages, and certain symbols that change from a language to the other. The symbols that are common to all the languages are:

- the connectors $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$;
- the parentheses (and) and the comma ,;
- the universal quantifier $\forall$ and the existential quantifier $\exists$;
- an infinite denumerable set of symbols $\mathcal{V}$, called variables.

The symbols that may vary from a language to the other are captured by the notion of *signature*. A signature fixes the symbols of constants, the symbols of functions and the symbols of relations that are authorized.

Formally:

Definition 1 (Signature of a first order language) *The* signature

$$\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$$

of a first order language is given by:

- *a first set $\mathcal{C}$ of symbols, called* constant symbols*;*
- *a second set $\mathcal{F}$ of symbols, called* function symbols*; To each symbol of this set is associated a strictly positive integer, that is called its* arity.
- *a third set $\mathcal{R}$ of symbols, called* relation symbols. *To each symbol of this set is associated a strictly positive integer, that is called its* arity.

We suppose that $\mathcal{V}$, $\mathcal{C}$, $\mathcal{F}$, $\mathcal{R}$ are pairwise disjoint sets.

A formula of first order will then be some particular word on the alphabet

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

Remark 1 *In what follows, we will use the following conventions: We consider that x, y, z, u and v denotes some variables, that is to say some elements of $\mathcal{V}$. a, b, c, d will denote some constants, that is to say some elements of $\mathcal{C}$.*

The intuition is that the constant, functions and relation symbols will be interpreted (in what we will call *structures*). The *arity* of a function symbol or relation symbol will correspond to its number of arguments.

Example 1 *For example, we can consider the signature*

$$\Sigma = (\{\mathbf{0}, \mathbf{1}\}, \{s, +\}, \{Odd, Prime, =, <\})$$

that has the constant symbols $\mathbf{0}$ and $\mathbf{1}$, the function symbol $+$ of arity 2, the function symbol s of arity 1, the relation symbols Odd and $Prime$ of arity 1, the relation symbols $=$ and $<$ of arity 2.

Example 2 *We can also consider the signature* $\mathscr{L}_2 = (\{c, d\}, \{f, g, h\}, \{R\})$ *with* c, d *two constant symbols,* f *a function symbol of arity* 1*,* g *and* h *two function symbols of arity* 2*,* R *a relation symbol of arity* 2*.*

We will define by successive steps, first the *terms*, that intend to represent objects, then the *atomic formulas* that intend to represent some relations between objects, and then the formulas.

1.1 Terms

We have already defined the terms in Chapter 2: What we call here *terms over a signature* Σ, is a term built on the union of function and constant symbols of the signature, and of the variables.

To be more clear, let's express again our definition:

Definition 2 (Termes sur une signature) *Let* $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$ *be a signature.*

The set T *of* terms *on the signature* Σ *is the language over alphabet* $\mathscr{A}(\Sigma)$ *inductively defined by:*

- (B) *every variable is a term:* $\mathscr{V} \subset T$*;*
- (B) *every constant is a term:* $\mathscr{C} \subset T$*;*
- (I) *if* f *is a function symbol of arity* n *and if* $t_1, t_2, \cdots, t_n$ *are terms, then* $f(t_1, \cdots, t_n)$ *is a term*

Definition 3 *A* closed term *is a term without any variable.*

Example 3 $+(x, s(+(\mathbf{1}, \mathbf{1})))$ *is a term built over the signature of Example 1 that is not closed.* $+(+(s(\mathbf{1}), +(\mathbf{1}, \mathbf{1})), s(s(\mathbf{0})))$ *is a closed term.*

Example 4 $h(c, x)$*,* $h(y, z)$*,* $g(d, h(y, z))$ *and* $f(g(d, h(y, z)))$ *are terms over the signature* $\mathscr{L}_2$ *of Example 2.*

1.2 Atomic formulas

Definition 4 (Atomic formulas) *Let* $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$ *be a signature.*

An atomic formula *on the signature* Σ *is a word on the alphabet* $\mathscr{A}(\Sigma)$ *of the form* $R(t_1, t_2, \cdots, t_n)$*, where* $R \in \mathscr{R}$ *is a relation symbol of arity* n*, and where* $t_1, t_2, \cdots, t_n$ *are terms over* Σ*.*

Example 5 $>(x, +(\mathbf{1}, \mathbf{0}))$ *is some atomic formula on the signature of Example 1. So is* $= (x, s(y))$.

Example 6 $R(f(x), g(c, f(d)))$ *is some atomic formula over* $\mathcal{L}_2$.

Remark 2 *We will agree to write sometimes* $t_1 R t_2$ *for some binary symbols, such as* $=, <, +$ *to avoid too heavy notations: For example, we will write* $x > \mathbf{1} + \mathbf{1}$ *for* $>(x, +(\mathbf{1}, \mathbf{1}))$.

1.3 Formulas

Definition 5 (Formules) *Let* $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$ *be a signature.*

The set of (of first order) formulas on the signature Σ *is the language over alphabet* $\mathscr{A}(\Sigma)$ *inductively defined by:*

(B) *every atomic formula is a formula;*

(I) *if* F *is a formula, then* $\neg F$ *is a formula;*

(I) *if* F *and* G *are two formulas, then* $(F \wedge G)$, $(F \vee G)$, $(F \Rightarrow G)$, *and* $(F \Leftrightarrow G)$ *are formulas;*

(I) *if* F *is a formula, and if* $x \in \mathscr{V}$ *is a variable, then* $\forall x F$ *is a formula, and* $\exists x F$ *is a formula.*

Example 7 *The statement* $\forall x((Prime(x) \wedge x > \mathbf{1} + \mathbf{1}) \Rightarrow Odd(x))$ *is a formula on the signature of Example 1.*

Example 8 *So does* $\exists x(s(x) = \mathbf{1} + \mathbf{0} \vee \forall y\ x + y > s(x))$

Example 9 *Examples of formulas over the signature* $\mathcal{L}_2$*:*

- $\forall x \forall y \forall z((R(x, y) \wedge R(y, z) \Rightarrow R(x, z))$
- $\forall x \exists y(g(x, y) = c \wedge g(y, x) = c)$*;*
- $\forall x \neg f(x) = c$*;*
- $\forall x \exists y \neg f(x) = c$.

2 First properties and definitions

2.1 Decomposition / Uniqueness reading

As for the propositional formulas, one can always decompose a formula, and in a unique way.

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

1. *an atomic formula;*
2. $\neg G$*, where G is a formula;*
3. $(G \wedge H)$ *where G and H are formulas;*
4. $(G \vee H)$ *where G and H are formulas ;*
5. $(G \Rightarrow H)$ *where G and H are formulas;*
6. $(G \Leftrightarrow H)$ *where G and H are formulas;*
7. $\forall x G$ *where G is a formula and x is a variable;*
8. $\exists x G$ *where G is a formula and x is a variable.*

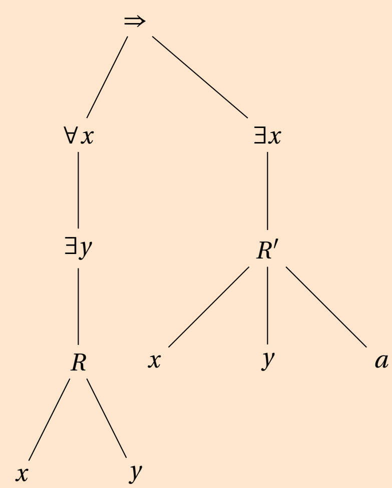
Furthermore, in the first case there is a unique way to "read"' the atomic formula. In all the other cases, there is unicity of the formula G and of the formula H with this property.

One can then represent each formula by a tree (its *decomposition tree*), that is in immediate correspondence with its derivation tree in the sense of Chapter 2): Each vertex is labeled by some constant, function or relation symbol, or by the symbols $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ or a quantifier or universal quantifier.

Example 10 *For example, the formula*

$$(\forall x \exists y R(x,y) \Rightarrow \exists x R'(x,y,a)) \tag{2}$$

is represented by the following tree



Each subtree of such a tree represents a *subformula* of F. If one prefers:

Definition 6 (Subformula) *A formula G is a subformula of a formula F if it appears in the decomposition of F.*

Exercise 1 *(solution on page 233) Let us fix a signature containing the relation symbols R_1, R_2 or respective arity 1 and 2. Let us fix the set of variables $\mathcal{V} = \{x_1, x_2, x_3\}$. Which of the following words are formulas?*

- $(R_1(x_1) \wedge R_2(x_1, x_2, x_3))$
- $\forall x_1 (R_1(x_1) \wedge R_2(x_1, x_2, x_3))$
- $\forall x_1 \exists R (R(x_1) \wedge R_2(x_1, x_1))$
- $\forall x_1 \exists x_3 (R_1(x_1) \wedge R_3(x_1, x_2, x_3))$

2.2 Free variables

The intuition of what follows is to distinguish the *free variables* from the other: All of this is about the "$\forall x$" and "$\exists x$" which are binders *binders*: When we write $\forall x F$ or $\exists x F$, then x become some bound variable. In other words, when we will talk about the semantic of formulas, the truth value of $\forall x F$ or $\exists x F$ will intend not to depend on x: We could well write $\forall y F(y/x)$ (respectively: $\exists y F(y/x)$) where $F(y/x)$ denotes intuitively the formula that is obtained by replacing x by y in formula F.

Remark 3 *We have exactly the same phenomenon in symbols such as the integral symbol in mathematics: In the expression $\int_a^b f(t)dt$, the variable t is some* *bound (dummy) variable. In particular $\int_a^b f(u)du$ is exactly the same integral.*

Let's do this very properly. A same variable can appear several times in a given formula, and we need to be able to locate every occurrence, taking care to $\exists$ and $\forall$.

Definition 7 (Occurrence) *An* occurrence *of a variable x in some formula F is an integer n such that the nth symbol of word F is x and such that the $(n-1)th$ symbol is not $\forall$ nor $\exists$.*

Example 11 8 *and* 17 *are occurrences of x in the formula* (2)*.* 7 *and* 14 *are not:* 7 *because the* $7th$ *symbol of F is not an x (this is an open parenthesis) and* 14 *because the* $14th$ *symbol of F that is indeed a x is quantified by a $\exists$.*

Definition 8 (Free, bounded Variable)

- *An occurrence of a variable x in a formula F is a* bounded occurrence *if this occurrence appears in some subformula of F that is not starting by some quantifier $\forall x$ or $\exists x$. Otherwise the occurrence is said to be* free.
- *A variable is* free *in a formula if it has at least one free occurrence in the formula.*
- *A formula F is closed if it does not have any free variable.*

Example 12 *In the formula* (2)*, the occurrences* 8*,* 17 *and* 10 *of x and y are bounded. The occurrence* 19 *of y is free.*

Example 13 *In the formula $(R(x,z) \Rightarrow \forall z(R(y,z) \vee y = z))$, the only occurrence of x is free, the two other occurrences of y are free. The first (least) occurrence of z is free, and the others are bounded. The formula $\forall x \forall z(R(x,z) \Rightarrow \exists y(R(y,z) \vee y = z))$ is closed.*

The notation $F(x_1, \cdots, x_k)$ means that the free variables of the formula F are among $x_1, \cdots, x_k$.

Exercise 2 *(solution on page 233) Find all the free and the bounded occurrences in the following formulas:*

- $\exists x(l(x) \wedge m(x))$
- $(\exists x l(x)) \wedge m(x)$

Exercise 3 *Prove that the* free!variable $\ell(F)$ *of a formula* F *can be obtained by the following inductive definition:*

- $\ell(R(t_1,\cdots,t_n)) = \{x_i | x_i \in \mathcal{V}$ *and* x_i *appears in* $R(t_1,\cdots,t_n)\}$;
- $\ell(\neg G) = \ell(G)$;
- $\ell(G \vee H) = l(G \wedge H) = \ell(G \Rightarrow H) = \ell(G \Leftrightarrow H) = \ell(G) \cup \ell(H)$;
- $\ell(\forall x F) = \ell(\exists x F) = \ell(F) \backslash \{x\}$.

3 Semantic

We can now talk about the meaning that we give to formulas. Actually, to provide a meaning to formulas, we need to fix some meaning of the symbols of the signature, and this is the purpose of the notion of structure.

Definition 9 (Structure) *Let* $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$ *be a signature.*
A structure $\mathfrak{M}$ of signature Σ *is given by:*

- *a non-empty set* M*, called its* base set*, or* domain *of the structure;*
- *an element, denoted by* $c^{\mathfrak{M}}$*, for each constant symbol* $c \in \mathscr{C}$ *;*
- *a function, denoted by* $f^{\mathfrak{M}}$*, of* $M^n \to M$ *for each function symbol* $f \in \mathscr{F}$ *of arity* n *;*
- *a subset, denoted by* $R^{\mathfrak{M}}$*, of* M^n *for each relation symbol* $R \in \mathscr{F}$ *of arity* n.

We say that the constant c (respectively the function f, the relation R) is *interpreted* by $c^{\mathfrak{M}}$ (resp. $f^{\mathfrak{M}}$, $R^{\mathfrak{M}}$). A structure is sometimes also called a *realisation* of the signature.

Example 14 *A realisation of the signature* $\Sigma = (\{\mathbf{0}, \mathbf{1}\}, \{+, -\}, \{=, >\})$ *corresponds to the domain* $\mathbb{N}$ *of natural integers, with* $\mathbf{0}$ *interpreted by the integer* 0, $\mathbf{1}$ *interpreted by* 1, $+$ *interpreted by addition,* $-$ *interpreted by subtraction, and* $=$ *by equality on the integers: That is to say by the subset* $\{(x,x) | x \in \mathbb{N}\}$*, and* $>$ *by the order on the integers, that is to say by the subset* $\{(x,y) | x > y\}$*. It can be denoted by* $(\mathbb{N}, =, <, +, -, 0, 1)$.

Example 15 *Another realisation of this signature corresponds to the domain* $\mathbb{R}$ *of the reals, where* $\mathbf{0}$ *is interpreted by the real* 0, $\mathbf{1}$ *by the real* 1, $+$ *by addition,* $-$ *by subtraction, and* $=$ *by equality on the reals, and* $>$ *by the order on the reals. It can be denoted by* $(\mathbb{R}, =, <, +, -, 0, 1)$.

Example 16 *We can obtain a realisation of the signature $\mathscr{L}_2$ by considering the base set $\mathbb{R}$ of the reals, by interpreting R as the order relation $\leq$ on the reals, the function f as the function that to x associates $x+1$, the functions g and h as respectively the addition and the multiplication on the reals, the constants c and d as the reals 0 and 1. It can be denoted by $(\mathbb{R}, \leq, s, +, \times, 0, 1)$.*

We will then use the notion of structure to interpret the terms, the atomic formulas, and then inductively the formulas as one may expect.

3.1 Interpretation of terms

Definition 10 (Valuation) *Fix a structure $\mathfrak{M}$. A* valuation *v is a distribution of values to the variables, that is to say a function from $\mathcal{V}$ to the domain M of the structure $\mathfrak{M}$.*

Definition 11 (Interprétation des termes) *Let $\mathfrak{M}$ be a structure of signature $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$.*

Let t be a term of the form $t(x_1, \cdots, x_k)$ over Σ whose free variables are $x_1, \cdots, x_k$.

Let v be a valuation.

The interpretation $t^{\mathfrak{M}}$ of term t for the valuation v*, also denoted by $t^{\mathfrak{M}}[v]$, or $t^{\mathfrak{M}}$ is defined inductively as follows:*

- (B) *every variable is interpreted as its value by the valuation: if t is the variable $x_i \in v$, then $t^{\mathfrak{M}}$ is $v(x_i)$;*
- (B) *every constant is interpreted as its interpretation in the structure: if t is the constant $c \in \mathscr{C}$, then $t^{\mathfrak{M}}$ is $c^{\mathfrak{M}}$;*
- (I) *each function symbol is interpreted as its interpretation int the structure: if t is the term $f(t_1, \cdots, t_n)$, then $t^{\mathfrak{M}}$ est $f^{\mathfrak{M}}(t_1^{\mathfrak{M}}, \cdots, t_n^{\mathfrak{M}})$, where $t_1^{\mathfrak{M}}, \cdots, t_n^{\mathfrak{M}}$ are the respective interpretations of the terms $t_1, \cdots, t_n$.*

Remark 4 *The interpretation of a term is an element of M, where M is the base set of the structure $\mathfrak{M}$. In other words, the terms denote some elements of the structure.*

Example 17 *Let $\mathcal{N}$ be the structure $(\mathbb{N}, \leq, s, +, \times, 0, 1)$ of signature*

$$\mathscr{L}_2 = (\{c, d\}, \{f, g, h\}, \{R\}) :$$

- *the interpretation of $h(d, x)$ for a valuation such that $v(x) = 2$ is 2.*
- *the interpretation of term $f(g(d, h(y, z)))$ for a valuation such that $v(y) = 2, v(z) = 3$ is 8.*

3.2 Interpretation of atomic formulas

An atomic formula $F = F(x_1, \cdots, x_k)$ is an object that is interpreted either by *true* or by *false* in some valuation v. When F is interpreted by true, we say that the *valuation v satisfies* F, and this fact is denoted by $v \models F$. We denote $v \not\models F$ in the contrary case.

There only remain to define formally this notion:

Definition 12 (Interpretation of some atomic formula) *Let $\mathfrak{M}$ be a structure of signature $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$.*

The valuation v satisfies the atomic formula $R(t_1, t_2, \cdots, t_n)$ of free variables $x_1, \cdots, x_k$ if $(t_1^{\mathfrak{M}}[v], t_2^{\mathfrak{M}}[v], \cdots, t_n^{\mathfrak{M}}[v]) \in R^{\mathfrak{M}}$, where $R^{\mathfrak{M}}$ is the interpretation of relation symbol R in the structure.

Example 18 *For example, on the structure of Example 14, $x > \mathbf{1}+\mathbf{1}$ is interpreted by 1 (true) in the valuation $v(x) = 5$, and by 0 (false) in the valuation $v(x) = 0$. The atomic formula $\mathbf{0} = \mathbf{1}$ is interpreted by 0 (false).*

Example 19 *On the structure $\mathscr{N}$ of Example 17, the atomic formula $R(f(c), h(c, f(d)))$ is interpreted by false.*

3.3 Interpretation of formulas

More generally, a formula $F = F(x_1, \cdots, x_k)$ is an object that is interpreted either by *true* or by *false* in some valuation v. When F interprets to true, we say that *the valuation v satisfies* F, and we write this fact by $v \models F$, and $v \not\models F$ for the contrary case.

Definition 13 (Interpretation of some formula) *Let $\mathfrak{M}$ be a structure of signature $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$.*

The expression "the valuation v satisfies the formula $F = F(x_1, \cdots, x_k)$", denoted by $v \models F$, is defined inductively in the following way:

(B) *it has already been defined for some atomic formula;*

$\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ *are interpreted exactly as in the propositional calculus:*

(I) *the negation is interpreted by the logical negation:*
if F is of the form $\neg G$, then $v \models F$ if and only if $v \not\models G$;

(I) $\wedge$ *is interpreted as the logical conjunction:*
if F is of the form $(G \wedge H)$, then $v \models F$ if and only if $v \models G$ and $v \models H$;

(I) $\vee$ *is interpreted as the logical or*
if F is of the form $(G \vee H)$, then $v \models F$ if and only if $v \models G$ or $v \models H$;

(I) $\Rightarrow$ *is interpreted as the logical implication:*
if F is of the form $(G \Rightarrow H)$, then $v \models F$ if and only if $v \models H$ or $v \not\models G$;

(I) $\Leftrightarrow$ *is interpreted as the logical equivalence:*
if F *is of the form* $(G \Leftrightarrow H)$, *then* $v \models F$ *if and only if* ($v \models G$ *and* $v \models H$) *or* ($v \not\models G$ *and* $v \not\models H$).

$\exists x$ *and* $\forall x$ *are interpreted as existential and universal quantifications:*

(I) *if* F *is of the form* $\forall x_0 G(x_0, x_1, \cdots, x_k)$, *then* $v \models F$ *if and only if for all* $a_0 \in M$ $v' \models G$, *where* v' *is the valuation such that* $v'(x_0) = a_0$, *and* $v'(x) = v(x)$ *for all* $x \neq x_0$;

(I) *if* F *is of the form* $\exists x_0 G(x_0, x_1, \cdots, x_k)$, *then* $v \models F$ *if and only for a certain element* $a_0 \in M$, *we have* $v' \models G$, *where* v' *is the valuation such that* $v'(x_0) = a_0$, *and* $v'(x) = v(x)$ *for every* $x \neq x_0$.

Example 20

- *The formula* $F(x)$ *defined by* $\forall y R(x, y)$ *is true in the structure* $\mathcal{N}$ *for* 0 *(i.e. for a valuation such that* $v(x) = 0$*), but false for all the other integers.*
- *The formula* $G(x)$ *defined by* $\exists y\, x = f(y)$ *is true in the structure* $\mathcal{N}$ *for the integers distinct from* 0 *and false for* 0.
- *The closed formula* $\forall x \forall z \exists y (x = c \vee g(h(x, y), z) = c)$ *of language* $\mathcal{L}_2$ *is true in* $(\mathbb{R} \leq, s, +, \times, 0, 1)$ *and false in* $\mathcal{N} = (\mathbb{N}, \leq, s, +, \times, 0, 1)$.

In the case where the valuation v satisfies the formula F, one also says that F is *true* in v. In the contrary, we say that F is *false* in v.

Definition 14 (Model of a formula) *For a closed formula* F*,the satisfaction of* F *in a structure* $\mathfrak{M}$ *is not depending on the valuation* v. *In the case where the formula* F *is true, we say that the structure* $\mathfrak{M}$ *is a model of* F, *and we write* $\mathfrak{M} \models F$.

Exercise 4 *(solution on page 233) Let* Σ *be a signature made of some binary relation* R *and of the predicate* $=$. *Write some formula that is valid if and only if* R *is some order (we can suppose that* $=$ *is interpreted by equality).*

3.4 Substitutions

Definition 15 (Substitution in a term) *Given some term* t *and some variable* x *appearing in this term, we can replace all the occurrences of* x *by some other term* t'. *The new term is said to be obtained by* substitution *of* t' *to* x *in* t, *and is denoted by* $t(t'/x)$.

Example 21 *The result of the substitution of* $f(h(u,y))$ *to* x *in* $g(y,h(c,x))$ *is* $g(y,h(c,f(h(u,y))))$. *The result of the substitution of* $g(x,z)$ *to* y *in this new term is*

$$g(g(x,z),h(c,f(h(u,g(x,z))))).$$

To do a substitution of a term to some free variable in some formula, it is necessary to does it carefully: Otherwise the meaning of the formula can be completely modified by the phenomenon of capture of variables.

Example 22 *Let* $F(x)$ *be the formula* $\exists y(g(y,y)=x)$. *In the structure* $\mathcal{N}$ *where* g *is interpreted by addition the meaning of* $F(x)$ *is clear:* $F(x)$ *is true in* x *if and only if* x *is even.*

If we replace the variable x *by* z*, the obtained formula has the same meaning that the formula* $F(x)$ *(up to the renaming of the free variable).* $F(z)$ *is true in* z *if and only if* z *is even.*

But if we replace x *by* y*, the obtained formula* $\exists y(g(y,y)=y)$ *is a closed formula that is true in the structure* $\mathcal{N}$. *The variable* x *have been replaced by a variable that is quantified in the formula* F.

Definition 16 (Substitution) *The* Substitution *of a term* t *to a free variable* x *in some formula* F *is obtained by replacing all the free occurrences of this variable by the term* t*,under the reserve that the following condition is satisfied: For every variable* y *appearing in* t*,* y *has no free occurrence appearing in a subformula of* F *starting by a* $\forall$ *or* $\exists$ *quantifier. The result of this substitution, if it is possible, is denoted by* $F(t/x)$.

Example 23 *The result of the substitution of the term* $f(z)$ *to the variable* x *in the formula* $F(x)$ *given by*

$$(R(c,x)\wedge\neg x=c)\wedge(\exists y g(y,y)=x))$$

is the formula

$$(R(c,f(z))\wedge\neg f(z)=c)\wedge(\exists y g(y,y)=f(z))).$$

Proposition 2 *If* F *is a formula,* x *is some free variable in* F*, and* t *is a term such that the substitution of* t *in* x *in* F *is defined, then the formulas* $(\forall x F\Rightarrow F(t/x))$ *and* $(F(t/x)\Rightarrow\exists x F)$ *are valid.*

Proof: We prove by induction on the formula F that the satisfaction of the formula $F(t/x)$ by the valuation v is equivalent to the one of formula $F(x)$ by the valuation v_1 where v_1 is obtained from v by giving to x the interpretation of t for the valuation v.

The only cases requiring a justification are those where the formula F is of the form $\forall G$ and $\exists xG$. From the hypothesis for the substitution of t to x, the considered quantification is about some variable y distinct both from x and from all the variables from t. It suffices then to examine the satisfaction of the formula $G(t/x)$ by a valuation v' equals to v but on y. By induction hypothesis on G, the formula $G(t/x)$ is satisfied by v' if and only if G is satisfied by the valuation v'_1 where v'_1 is obtained from v' by giving to x the interpretation of t for the valuation v': Indeed, v and v' are equal on all the variables appearing in the term t. □

4 Equivalence, Normal forms

4.1 Equivalent formulas

Definition 17 *Let $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$ be as signature.*

- *A structure $\mathfrak{M}$ satisfies the formula $F(x_1, \cdots, x_k)$ if it satisfies the closed formula $\forall x_1 \cdots \forall x_k F(x_1, \cdots, x_k)$. This latter formula is called the* universal closure.
- *A closed formula F is said* valid *if it is satisfied by any structure $\mathfrak{M}$.*
- *A formula F is said* valid *if its universal closure is valid.*
- *Two formulas F and G are equivalent if for any structure, and for any valuation v, the formulas F and G take the same truth value. We write $F \equiv G$ in this case.*

Exercise 5 *Prove that the relation $\equiv$ is an equivalence relation.*

Proposition 3 *Let F be a formula. We have the following equivalences*

$$\neg \forall x F \equiv \exists x \neg F$$

$$\neg \exists x F \equiv \forall x \neg F$$

$$\forall x \forall y F \equiv \forall y \forall x F$$

$$\exists x \exists y F \equiv \exists y \exists x F$$

Proposition 4 *Suppose that the variable x is not free in the formula G. Let F be* *a formula. We have then the following equivalences:*

$$\forall x G \equiv \exists x G \equiv G \quad (3)$$

$$(\forall x F \vee G) \equiv \forall x (F \vee G) \quad (4)$$

$$(\forall x F \wedge G) \equiv \forall x (F \wedge G) \quad (5)$$

$$(\exists x F \vee G) \equiv \exists x (F \vee G) \quad (6)$$

$$(\exists x F \wedge G) \equiv \exists x (F \wedge G) \quad (7)$$

$$(G \wedge \forall x F) \equiv \forall x (G \wedge F) \quad (8)$$

$$(G \vee \forall x F) \equiv \forall x (G \vee F) \quad (9)$$

$$(G \wedge \exists x F) \equiv \exists x (G \wedge F) \quad (10)$$

$$(G \vee \exists x F) \equiv \exists x (G \vee F) \quad (11)$$

$$(\forall x F \Rightarrow G) \equiv \exists x (F \Rightarrow G) \quad (12)$$

$$(\exists x F \Rightarrow G) \equiv \forall x (F \Rightarrow G) \quad (13)$$

$$(G \Rightarrow \forall x F) \equiv \forall x (G \Rightarrow F) \quad (14)$$

$$(G \Rightarrow \exists x F) \equiv \exists x (G \Rightarrow F) \quad (15)$$

Each of the equivalence is rather simple to be established, but tedious, and we leave the proofs a exercises.

Exercise 6 *Prove Proposition 4.*

Exercise 7 *(solution on page 233) Are the following propositions equivalent ? If not, does the proposition on the left implies the one one the right?*

1. $\neg(\exists x P(x))$ *and* $(\forall x \neg P(x))$
2. $(\forall x P(x) \wedge Q(x))$ *and* $((\forall x P(x)) \wedge (\forall x Q(x)))$
3. $((\forall x P(x)) \vee (\forall x Q(x)))$ *and* $(\forall x P(x) \vee Q(x))$
4. $(\exists x P(x) \vee Q(x))$ *and* $((\exists x P(x)) \vee (\exists x Q(x)))$
5. $(\exists x P(x) \wedge Q(x))$ *and* $((\exists x P(x)) \wedge (\exists x Q(x)))$
6. $(\exists x \forall y P(x,y))$ *and* $(\forall y \exists x P(x,y))$

4.2 Prenex normal form

Definition 18 (Prenex form) *A formula F is said to be* in prenex form *if it is of the form*

$$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n F'$$

where each of the Q_i is either a $\forall$ quantifier or a $\exists$ quantifier, and F' is a formula not containing any quantifier.

Proposition 5 *Every formula F is equivalent to some formula in prenex normal form G.*

Proof: By structural induction on F.

Base case. If F is of the form $R(t_1, \cdots, t_n)$, for some relation symbol R, then F is in prenex normal form.

Inductive case:

- If F is of the form $\forall xG$ where $\exists xG$, by induction hypothesis G is equivalent to G' in prenex normal form, and so F is equivalent to $\forall xG'$ or $\exists xG'$ that is in prenex normal form.

- If F is of the form $\neg G$, by induction hypothesis G is equivalent to G' in prenex normal form $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G''$. By using the equivalences of the Proposition 3, F is equivalent to $Q'_1 x_1 Q'_2 x_2 \cdots Q'_n x_n \neg G''$, by taking $Q'_i = \forall$ if $Q_i = \exists$ and $Q'_i = \exists$ if $Q_i = \forall$.

- If F is of the form $(G \wedge H)$, by induction hypothesis G and H are equivalent to formulas G' and H' in prenex normal form. By applying the equivalences (4) à (11), we can "bring up" the quantifiers in front of the formula: We need to proceed with care, since for example $F = (F_1 \wedge F_2) = ((\forall x F'_1) \wedge F'_2)$ with x free in F'_2, we need first to rename the variable x in F_1 by replacing x by some new variable z not appearing nor in F_1 nor in F'_2, in order to be able to use the required equivalence among the equivalences (4) à (11).

- The other cases are treated in a similar way, by using the equations of the two previous propositions.

□

By using the idea of the conjunctive and disjunctive normal form of propositional calculus, we can even go further:

Definition 19
- *A* literal *is some atomic formula or the negation of some atomic formula.*
- *A* clause *is a disjunction of literals.*
- *A prenex formula $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G$ is in* conjunctive normal form *if the quantifier free formula G is a clause or a conjunction of clauses.*

The notion of *disjunctive normal form* can be defined in a dual way by considering disjunctions of conjunctions of atomic formulas instead of conjunctions of disjunctions of atomic formulas.

Proposition 6 *Every formula F is equivalent to some prenex formula*

$$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G,$$

where G is in conjunctive normal form.

Proposition 7 *Every formula F is equivalent to some prenex formula*

$$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G,$$

where G is in disjunctive normal form.

Proof: Let F be a formula and $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G$ a prenex equivalent formula equivalent to F. We denote by $A_1, A_2, \ldots, A_k$ the atomic formulas that appear in G. We can define a formula $H$of propositional calculus that uses the variables $\{p_1, p_2, \ldots, p_k\}$ such that the formula G corresponds to the formula $H(A_1/p_1, A_2/p_2, \ldots, A_k/p_k)$. Let H' be a conjunctive (respectively: disjunctive) normal form equivalent to H, obtained int he propositional calculus.

The formula G is equivalent to the formula G' given by expression $H'(A_1/p_1, A_2/p_2, \ldots, A_k/p_k)$ and then F is equivalent to $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G'$ in conjunctive (resp. disjunctive) normal form. $\square$

Exercise 8 *(solution on page 234) Determine an equivalent prenex normal form equivalent to*

$$(\exists x P(x) \wedge \forall x(\exists y Q(y) \Rightarrow R(x))).$$

Exercise 9 *Determine an equivalent normal form equivalent to*

$$(\forall x \exists y R(x, y) \Rightarrow \forall x \exists y (R(x, y) \wedge \forall z (Rxz \Rightarrow (Ryz \vee y = z))))$$

and to

$$\forall x \forall y ((R(x, y) \wedge \neg x = y) \Rightarrow \exists z (y = g(x, h(z, z)))).$$

4.3 Skolem form

The previous results where about transformations on formulas preserving the equivalence.

We will now focus on weaker transformations in order to eliminate the existential quantifiers. Starting form some closed formula F, we will obtain some formula F' that will not be necessarily equivalent. The formula F' will be written on a signature where possibly some new constant and function symbols have been added. It will have a model if and only if the initial formula has one.

Definition 20 *Let $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$ be a signature.*

- *A formula F is said to be* universal *it it is prenex and all the quantifiers appearing in F are $\forall$ quantifiers.*
- *A signature $\Sigma' = (\mathscr{C}', \mathscr{F}', \mathscr{R}')$ is a* Skolem extension *of Σ if it is obtained by adding to Σ some function symbols (possibly infinitely many) and some constant symbols (possibly infinitely many).*

A closed prenex formula of F of Σ' is either universal or of the form

$$\forall x_1 \forall x_2 \ldots \forall x_k \exists x G$$

where G is prenex. In the latter case, it may happen that $k = 0$ and F is then of the form $\exists x G$.

The transformation that we will apply consists in associating to F a formula F_1 given by $\forall x_1 \forall x_2 \ldots \forall x_k G(f(x_1, \ldots, x_k)/x)$ where f is some function symbol not appearing in formula G. In the particular case where F is $\exists x G$ (i.e. the case $k = 0$), we will associate some formula F_1 given by $G(c)$ where c is a constant symbol not appearing in formula G.

The formula F_1 obtained in this way has one less existential quantifier than the formula F.

Example 24 *To the formula F given by*

$$\forall x \forall y \exists z (R(f(x), g(z, y)) \Rightarrow (R(f(x), z) \wedge R(z, h(x, y))))$$

on the signature $\Sigma = (\{a, b\}, \{f, g, h\}, \{R\})$, we will associate the formula F_1 given by

$$\forall x \forall y (R(f(x), g(k(x, y), y)) \Rightarrow (R(f(x), k(x, y)) \wedge R(k(x, y), h(x, y))))$$

on the signature $\Sigma' = (\{a, b\}, \{f, g, h, k\}, \{R\})$ where we have added the symbol k or arity 2.

F has a model if and only if F' has a model.

Definition 21 *Let F be a closed prenex formula on the signature Σ' that has n existential quantifiers.*

- *A Skolem form of F is a formula obtained by applying n times successively the previous transformation.*
- *The new functions and constants introduced in these transformations are called the* Skolem functions and constants.

By construction, the Skolem form of F is some universal formula.

Example 25 *Staring from F given by*

$$\exists x \forall y \forall x' \exists y' \forall z (R(x,y) \Rightarrow (R(x',y') \wedge (R(x',z) \wedge (R(x',z) \Rightarrow (R(y',z) \vee y' = z)))))$$

a Skolem form of F is the formula

$$\forall y \forall x' \forall z (R(e,y) \Rightarrow (R(x',k(y,x')) \wedge (R(x',z) \Rightarrow (R(k(y,x'),z) \vee (k(y,x') = z)))))$$

The interest of this transformation lies in the following result:

Theorem 1 *Let F' be a Skolem form of F. Then F' has a model if and only if F has a model.*

Proof: We only need to prove that the property is true when F' is obtained from F by some of the transformation above (and repeat n times the argument in the general case): If F is given by

$$\forall x_1 \forall x_2 \ldots \forall x_k \exists x G$$

then F_1 is given by $\forall x_1 \forall x_2 \ldots \forall x_k G(f(x_1,\ldots,x_k)/x)$. If F_1 has a model, then F has a model: This comes from the validity of the formula

$$\forall x_1 \forall x_2 \ldots \forall x_k G(f(x_1,\ldots,x_k)/x) \Rightarrow \forall x_1 \forall x_2 \ldots \forall x_k \exists x G$$

The case $k = 0$ follows from the validity of the formula

$$G(c) \Rightarrow \exists x G(x).$$

To prove the converse direction, suppose that F has a model $\mathfrak{M}$ of base set M. It suffices to define the interpretation of the corresponding Skolem constant or function. If $F = \forall x_1 \forall x_2 \ldots \forall x_k \exists x G$ the interpretation of the Skolem function f is given by taking for each sequence $a_1, a_2, \ldots, a_k$ of elements of M an element $f^{\mathfrak{M}}(a_1, a_2, \ldots, a_k)$ among the $a \in M$ such that

$$\mathfrak{M} \models G(a_1, a_2, \ldots, a_k),$$

which is possible since $\mathfrak{M}$ is a model of F.

If F is of the form $\exists x G$, the interpretation of the Skolem constant c is taken by taking an element $c^{\mathfrak{M}}$ among the $b \in M$ satisfying G in $\mathfrak{M}$. □

5 Bibliographic notes

Suggested readings To go further on the notions of this chapter, we suggest [Cori and Lascar, 1993], [Dowek, 2008] or [Lassaigne and de Rougemont, 2004].

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

Index

Bibliography

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

[Dowek, 2008] Dowek, G. (2008). *Les démonstrations et les algorithmes.* Polycopié du cours de l'Ecole Polytechnique.

[Lassaigne and de Rougemont, 2004] Lassaigne, R. and de Rougemont, M. (2004). *Logic and complexity.* Discrete Mathematics and Theoretical Computer Science. Springer.