Foundations of Computer Science
Logic, models, and computations

Chapter: Models. Completeness.

Course INF412

of l'Ecole Polytechnique

Olivier Bournez

bournez@lix.polytechnique.fr

Version of July 16, 2023

Models. Completeness.

We can now describe various objects, and talk about their properties. We have indeed all the ingredients to talk about models and theories. In this chapter, after a few examples, we will then focus on the *completeness theorem*.

The basic concept is the the concept of theory.

Definition 1 (Theory)

- *A* theory $\mathcal{T}$ *is a set of closed formulas over some given signature. The formulas of a theory are called the* axioms *of this theory.*
- *A structure* $\mathfrak{M}$ *is a* model of the theory $\mathcal{T}$ *if* $\mathfrak{M}$ *is a model of each of the formulas of the theory.*

Definition 2 (Consistant theory) *A theory is said to be* consistent *if it has a model. It is said* inconsistent *if it is not consistent.*

Of course, the inconsistent theories have less interest.

Remark 1 *From a computer science point of view, one can see a theory as a* specification *of an object: We describe the object thanks to first order logic, i.e. thanks to axioms that describe it.*

A consistent specification (theory) is hence nothing but a theory that specifies at least one object.

Remark 2 *In this context, the question of completeness is to know if one describes correctly the object in question, or the class of objects in question: The completeness theorem states that this is indeed the case for a consistent theory, as long as one want to talk about the whole class of all the models of these specifications.*

We are going to start by giving several example of theories, in order to make our discussion less abstract.

1 Examples of theories

1.1 Graphs

An *oriented graph* can be seen as a model of the theory without any axiom over the signature $\Sigma = (\emptyset, \emptyset, \{E\})$, where the relation symbol E is of arity 2: $E(x,y)$ means that there is an arc between x and y.

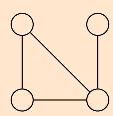
Example 1 *The formula* $\exists y(E(x,y) \wedge \forall z(E(x,z) \Rightarrow x = y))$ *is true in* x *if and only if* y *is of exterior degree* 1 *(modulo the comment of subsection that follows about equality).*

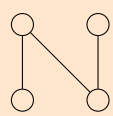
A non-oriented graph can be seen as a model of the theory with the unique axiom

$$\forall x \forall y\ (E(x,y) \Leftrightarrow E(y,x)), \tag{1}$$

on the same signature. This axioms states that if there is an arc between x and y, then there is an arc between y and x and conversely.

Example 2 *Here are two (non-oriented) graphs*





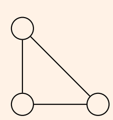
The formula $\exists x \forall y(\neg(x = y) \Rightarrow E(x,y))$ *is true on the first and not on the second.*

1.2 Simple remarks

Remark 3 *On the signature* $\Sigma = (\emptyset, \emptyset, \{E\})$*, there is no term. We hence cannot designate any particular vertex but using some free variable, or via some quantifiers.*

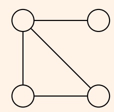
If one wants to designate one or some particular vertex, we can add one or several constant symbols. We can hence for example consider the signature $(V, \emptyset, \{E\})$ *where* $V = \{a, b, c\}$*.*

For example, the graph



is a model of $E(a,b) \wedge E(b,c) \wedge E(a,c)$.

But be careful, this is not the only one: The graph



is indeed also a model: The domain of a model can contains some elements that are not corresponding to any term.

Furthermore, the interpretation of a, b *or* c *could be the same element.*

Example 3 *One can sometimes avoid constants. The formula*

$$\exists x \exists y \exists z (\neg(x=y) \wedge \neg(y=z) \wedge \neg(x=z) \wedge E(x,y) \wedge E(y,z) \wedge E(x,z) \wedge \forall t (t=x \vee t=y \vee t=z)) \quad (2)$$

characterizes the triangles such as the graph above (modulo the comment of the following subsection concerning equality).

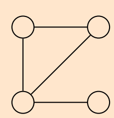
Remark 4 *Be careful: All the properties cannot be expressed easily. For example, one can prove that this is not possible to write a (first order) formula which characterizes the connected graphs. Exercise: Try to write it in order to feel where the problem is.*

Remark 5 *This is the presence of other models that the one that we intend to describe, and that is sometimes unavoidable, that would be at the heart of the difficulties about the axiomatisation of the integers.*

1.3 Equality

Be careful,the previous discussion is not totally correct: We have used at several times the equality symbol. The above discussion was supposing that the interpretation of equality is indeed equality.

Example 4 *Actually,*



is indeed a model of (2)*, and this is consequently perfectly false that* (2) *characterizes the triangles.*

Actually, let's call $\{a,b,c,d\}$ *the vertices from bottom to top and from left to right; we can consider the interpretation* $\equiv$ *of* $=$ *with* $a \equiv a, b \equiv b, c \equiv c, d \equiv b$ *and*

$a \not\equiv b, a \not\equiv c, b \not\equiv c$. Such a model satisfies indeed (2). However, $\equiv$, the interpretation of $=$ is not the equality. Observe that we have an edge between a and b, $b = d$ that is true, but no edge between a and d.

To make the above discussion fully correct, we can add a symbol $=$ to the signature to all the examples, and add the axioms satisfied by equality.

Let $\mathscr{R}$ be a set of relation symbols that contains at least the symbol $=$.

Definition 3 (Axioms of equality) *The axioms of equality for a signature $\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R})$, with $= \in \mathscr{R}$, are*

- *the axiom $\forall x\ x = x$;*
- *for every function symbol $f \in \mathscr{F}$ of arity n, the axiom*

$$\forall x_1 \cdots \forall x_i \forall x_i' \cdots \forall x_n (x_i = x_i' \Rightarrow f(x_1, \cdots, x_i, \cdots, x_n) = f(x_1, \cdots, x_i', \cdots, x_n));$$

- *for every relation symbol $R \in \mathscr{R}$ of arity n, the axiom*

$$\forall x_1 \cdots \forall x_i \forall x_i' \cdots \forall x_n (x_i = x_i' \Rightarrow (R(x_1, \cdots, x_i, \cdots, x_n) \Rightarrow R(x_1, \cdots, x_i', \cdots, x_n)).$$

All these axioms specify that the equality is reflexive, and is preserved by the relation and function symbols.

Exercise 1 *(solution on page 234) Prove that we then necessarily have $\forall x \forall y\ (x = y \Rightarrow y = x)$.*

Exercise 2 *Prove that we then necessarily have for each relation symbol $R \in \mathscr{R}$ or arity n,*

$$\forall x_1 \cdots \forall x_i \forall x_i' \cdots \forall x_n (x_i = x_i' \Rightarrow (R(x_1, \cdots, x_i, \cdots, x_n) \Leftrightarrow R(x_1, \cdots, x_i', \cdots, x_n)).$$

Exercise 3 *Prove that we then necessarily have for each formula $F(x_1, x_2, \ldots, x_n)$*

$$\forall x_1 \cdots \forall x_i \forall x_i' \cdots \forall x_n (x_i = x_i' \Rightarrow (F(x_1, \cdots, x_i, \cdots, x_n) \Leftrightarrow F(x_1, \cdots, x_i', \cdots, x_n)).$$

Exercise 4 *Prove that we then necessarily have $\forall x \forall y \forall z\ ((x = y \wedge y = z) \Rightarrow x = z)$.*

We deduce from the two previous exercises, that $=$ (and its interpretation) is some equivalence relation.

1.4 Small digression

Definition 4 *A model $\mathfrak{M}$ of a theory $\mathcal{T}$ over a signature with the relation symbol $=$ is said to respect equality if the interpretation of $=$ in $\mathfrak{M}$ is equality.*

In other terms, the interpretation of symbol $=$ in $\mathfrak{M}$ is the subset $\{(x,x) | x \in M\}$ where M is the base set of $\mathfrak{M}$.

It turns out if this is not the case, and if the axioms of equality are among the theory $\mathcal{T}$, we can come back to this case.

Proposition 1 *Let $\mathcal{T}$ be a theory with a signature Σ, with at least the symbol $=$ as a relation symbol, which contains the axioms of equality for Σ.*

If $\mathcal{T}$ has a model, then $\mathcal{T}$ has also some model that respects equality.

Proof: We can quotient the domain M of any model $\mathfrak{M}$ of $\mathcal{T}$ by the equivalence relation that puts in the same equivalence class x and y when the interpretation of $x = y$ is true in $\mathfrak{M}$ (i.e. the interpretation of $=$). The quotient model,that is to say the model whose elements are the equivalence classes for this equivalence relation, is by definition, respecting equality. □

As a consequence, a theory $\mathcal{T}$ has a model that respects equality if and only if the theory plus all the axioms of equality (for the corresponding signature) has a model.

Example 5 *In the example 3, the sentence should be: The models that respects equality of the formula* (2) *characterize the triangles.*

Or possibly: The theory made of the formula (2) *and the axioms of equality (in that case $\forall x\; x = x, \forall x \forall x' \forall y (x = x' \Rightarrow (R(x,y) \Rightarrow R(x',y))), \forall x \forall y \forall y' (y = y' \Rightarrow (R(x,y) \Rightarrow R(x,y'))))$) characterize the triangles.*

1.5 Groups

Let's start by talking about groups, in group theory.

Example 6 (Group) *A group is a model of the theory made of the axioms of equality and of the two formulas:*

$$\forall x \forall y \forall z\; x * (y * z) = (x * y) * z \tag{3}$$

$$\exists e \forall x\; (x * e = e * x = x \wedge \exists y (x * y = y * x = e)) \tag{4}$$

on the signature $\Sigma = (\emptyset, \{*\}, \{=\})$, where $*$ and $=$ are of arity 2.

The first property asserts that the law $*$ of the group is associative, and the second that there is some neutral element, e, and that any element has some inverse.

Example 7 (Commutative group) *A commutative group (also called an* Abelian group*) is a model of the theory made of the axioms of equality and of the three* *formulas:*

$$\forall x \forall y \forall z\; x * (y * z) = (x * y) * z \tag{5}$$

$$\exists e \forall x\; (x * e = e * x = x \wedge \exists y (x * y = y * x = e)) \tag{6}$$

$$\forall x \forall y\; x * y = y * x \tag{7}$$

over the same signature.

1.6 Fields

Example 8 (Commutative field) *A* commutative field *is a model of the theory made of the axioms of equality and of the formulas*

$$\forall x \forall y \forall z\; (x + (y + z) = (x + y) + z) \tag{8}$$

$$\forall x \forall y (x + y = y + x) \tag{9}$$

$$\forall x (x + \mathbf{0} = x) \tag{10}$$

$$\forall x \exists y (x + y = \mathbf{0}) \tag{11}$$

$$\forall x \forall y \forall z\; x * (y + z) = x * y + x * z \tag{12}$$

$$\forall x \forall y \forall z\; ((x * y) * z) = (x * (y * z)) \tag{13}$$

$$\forall x \forall y\; (x * y = y * x) \tag{14}$$

$$\forall x\; (x * \mathbf{1} = x) \tag{15}$$

$$\forall x \exists y (x = \mathbf{0} \vee x * y = \mathbf{1}) \tag{16}$$

$$\neg \mathbf{1} = \mathbf{0} \tag{17}$$

over a signature with two symbols of constants $\mathbf{0}$ *and* $\mathbf{1}$*, two symbols of functions* $+$ *and* $*$ *of arity* 2*, and the relation symbol* $=$ *of arity* 2*.*

For example, $\mathbb{R}$ and $\mathbb{C}$ with the usual interpretation are models of these theories.

If we add to the theory the formula F_p defined by $\mathbf{1} + \cdots + \mathbf{1} = \mathbf{0}$, where $\mathbf{1}$ is repeated p times, the models are the fields of characteristic p: For example, $\mathbb{Z}_p$, when p is some prime integer.

If we want to describe a field of characteristic 0, we must consider the theory made of the previous axioms, and the union of the negation of the axioms F_p for all prime integer p.

Example 9 (Algebraically closed field) *For every integer* n*, we consider the formula* G_n

$$\forall x_0 \forall x_1 \cdots \forall x_{n-1} \exists x (x_0 + x_1 * x + x_2 * x^2 + \cdots + x_{n-1} * x^{n-1} + x^n = 0)$$

where the reader would have guessed that x^k *is* $x * \cdots * x$ *with* x *repeated* k *times.*

An algebraically closed field is a model of the theory of commutative fields and of the union of the formulas G_n *for* $n \in \mathbb{N}$*.*

For example, $\mathbb{C}$ is algebraically closed. $\mathbb{R}$ is not algebraically closed, since x^2+1 has no real root.

1.7 Robinson Arithmetic

We can also try to axiomatise the integers. Here is a first attempt.

Example 10 (Robinson arithmetic) *Consider the signature made of the constant symbol* $\mathbf{0}$*, of the unary function symbol* s*, and of two binary function symbols* $+$ *and* $*$*, and of binary relation symbols* $<$ *and* $=$.

The axioms of Robinson arithmetic are the axioms of equality and

$$\forall x\ \neg s(x) = \mathbf{0} \tag{18}$$

$$\forall x\ \forall y\ (s(x) = s(y) \Rightarrow x = y) \tag{19}$$

$$\forall x\ (x = \mathbf{0} \vee \exists y\ \ s(y) = x) \tag{20}$$

$$\forall x\ \mathbf{0} + x = x \tag{21}$$

$$\forall x\ s(x) + y = s(x + y) \tag{22}$$

$$\forall x\ \mathbf{0} * x = \mathbf{0} \tag{23}$$

$$\forall x\ s(x) * y = x * y + y \tag{24}$$

$$\tag{25}$$

The structure whose base set is the integers, and where $+$ is interpreted by addition, $*$ by multiplication, and $s(x)$ by $x+1$ is a model of this theory. We call this model the *standard model of the integers*.

Observe that we can define in any model of the previous axioms some order, by the rule $x < y$ if and only if $\exists z\ (x + s(z) = y)$.

An alternative is to take $<$ as a primitive relation symbol of arity 2 and add the axioms

$$\forall x\ \neg x < \mathbf{0} \tag{26}$$

$$\forall x\ \mathbf{0} = x \vee \mathbf{0} < x \tag{27}$$

$$\forall x\ \forall y\ (x < y \Leftrightarrow (s(x) < y \vee s(x) = y)) \tag{28}$$

$$\forall x\ \forall y\ (x < s(y) \Leftrightarrow (x < y \vee x = y)) \tag{29}$$

Exercise 5 *Prove that the order defined by the rule* $x < y$ *if and only if* $\exists z\ (x + s(z) = y)$ *satisfies these formulas.*

Exercise 6 *(solution on page 234) Let n and m two integers. We write* $s^n(\mathbf{0})$ *for* $s(s(\cdots s(\mathbf{0})))$ *with s repeated n times, with the convention that* $s^{(0)} = \mathbf{0}$.

Prove by recurrence that

$$s^n(\mathbf{0}) + s^m(\mathbf{0}) = s^{n+m}(\mathbf{0}).$$

Find some model of Robinson axioms where two elements a and b are such that $a + b \neq b + a$.

Deduce that Robinson axioms are not sufficient to axiomatise the integers: There are other models that the standard model of the integers to these axioms.

Exercise 7 *Add* $\forall x \forall y (x + y = y + x)$ *to previous axioms to guarantee the commutativity of addition. Produce a model of the previous axioms that is not the standard model of the integers: For example, with tow elements a and b such that* $a * b \neq b * a$.

Instead of trying to add certain axioms in order to guarantee that properties such as commutativity of addition and of multiplication, we will consider a family of axioms.

1.8 Peano arithmetic

Example 11 (Peano arithmetic) *Consider a signature made of the constant symbol* $\mathbf{0}$*, for the unary function symbol s, and of two binary function symbols + and* $*$*, and of binary relation symbol =.*

The axioms of Peano arithmetic are the axioms of equality and

$$\forall x\ \neg(s(x) = \mathbf{0}) \tag{30}$$

$$\forall x \forall y\ (s(x) = s(y) \Rightarrow x = y) \tag{31}$$

$$\forall x\ (x = \mathbf{0} \vee \exists y\ s(y) = x) \tag{32}$$

$$\forall x\ \mathbf{0} + x = x \tag{33}$$

$$\forall x\ s(x) + y = s(x + y) \tag{34}$$

$$\forall x\ \mathbf{0} * x = \mathbf{0} \tag{35}$$

$$\forall x\ s(x) * y = x * y + y \tag{36}$$

$$\tag{37}$$

and the set of all the formulas of the form

$$\forall x_1 \cdots \forall x_n((F(\mathbf{0}, x_1, \cdots, x_n) \wedge \forall x_0(F(x_0, x_1, \cdots, x_n) \Rightarrow F(s(x_0), x_1, \cdots, x_n)))$$

$$\Rightarrow \forall x_0 F(x_0, x_1, \cdots, x_n)) \tag{38}$$

where n in any integer, and $F(x_0, \cdots, x_n)$ is any formula of free variables $x_0, \cdots, x_n$.

There are hence an infinity of axioms. The last axioms aims at capturing reasoning's by recurrence that are usually done on the integers.

Of course, these axioms guarantee the following property: The standard model of the integers is model of these axioms

Exercise 8 *Prove that the axiom $\forall x\ (x = \mathbf{0} \vee \exists y\ s(y) = x)$ is actually useless: This formula is a consequence of the others.*

One clear interest is that we have now:

Exercise 9 *(solution on page 235) Prove that in any model of Peano axioms, the addition is commutative: The formula $\forall x \forall y (x + y = y + x)$ is true.*

Exercise 10 *Prove that in any model of Peano axioms, the multiplication is commutative: The formula $\forall x \forall y (x * y = y * x)$ is true.*

In other words, this family of axioms is sufficient to guarantee a huge number of properties that are true on the integers.

We will see later on (incompleteness theorem) that there remain some other models than the standard integers to Peano axioms.

2 Completeness

The *completeness theorem*, due to Kurt Gödel, sometimes called the *first Gödel theorem*, is relating the notion of completeness to the notion of provability, by demonstrating that the two notions are the same.

2.1 Consequences

The notion of consequence is easy to define.

Definition 5 (Consequence) *Let F be a formula. The formula F is said to be a (semantic)* consequence *of a theory $\mathcal{T}$ if any model of the theory $\mathcal{T}$ is a model of F. We write in this case $\mathcal{T} \models F$.*

Example 12 *For example, the formula $\forall x \forall y\ x * y = y * x$, which expresses the commutativity , is not a consequence of the theory of groups (Definition 6), since* *there are groups which are not commutative.*

Example 13 *We can prove that the formula $\forall x\ \mathbf{0} + x = x$ is a consequence of Peano axioms.*

Example 14 *The exercise 6 proves that the formula $\forall x \forall y (x + y = y + x)$ (commutativity of addition) is not a consequence of Robinson axioms.*

2.2 Demonstration

We need to fix a notion of demonstration. We will do it, but let's first say that we have a notion of demonstration, such that we write $\mathcal{T} \vdash F$ if one can prove the closed formula F from the axioms of theory $\mathcal{T}$.

We expect at minimum from this notion of proof to be valid: That is to say to derive uniquely consequences: If F is a closed formula, and if $\mathcal{T} \vdash F$, then F is a consequence of $\mathcal{T}$.

2.3 Statement of completeness theorem

The completeness theorem states that actually we can succeed to reach all the consequences: The relations $\models$ and $\vdash$ are the same.

Theorem 1 (Completness theorem) *Let $\mathcal{T}$ be a theory over a denumerable signature. Let F be some closed formula. F is a consequence of $\mathcal{T}$ if and only if F is provable from $\mathcal{T}$.*

2.4 Meaning of the theorem

Let's take some time to understand what it does mean: In other words, the **provable statements are precisely those which are true in every model of the theory.**

This means in particular that:

- if some closed formula F is not provable, then there must exists a model that is not a model of F.
- if a closed formula F is true in any model of the axioms of the theory, then F is provable.

Example 15 *For example, the formula $\forall x \forall y\ x * y = y * x$, which expresses the commutativity, is not provable from the axioms of the theory of groups.*

Example 16 *The formula* $\forall x\, \mathbf{0} + x = x$ *is provable from the Peano axioms.*

2.5 Other formulation of the theorem

We say that a theory $\mathcal{T}$ is *coherent* if there is no formula F such that $\mathcal{T} \vdash F$ and $\mathcal{T} \vdash \neg F$.

We will see while doing the proof that the following also holds:

Theorem 2 (Théorème de complétude) *Let* $\mathcal{T}$ *be a theory over some denumerable signature.* $\mathcal{T}$ *has a model if and only if* $\mathcal{T}$ *is coherent.*

3 Proof of completeness theorem

3.1 A deduction system

We need to define a notion of demonstration. We choose to consider a notion of demonstration based on the notion of proof à la Frege and Hilbert, that is to say based on the modus ponens.

With respect to propositional calculus, we are not using anymore only the modus ponens rule, but also a *generalisation rule*: If F is a formula and if x is some variable, the generalisation rule deduces $\forall x F$ from F.

One ca be troubled by this rule, but this is nothing but what is regularly done in the common reasoning: If we succeed to prove $F(x)$ without any particular hypothesis on x, then we know that $\forall x F(x)$.

We then consider a certain number of axioms:

Definition 6 (Axiomes logiques du calcul des prédicats) *The* logical axioms of the predicate calculus *are:*

1. *every instance of the tautologies of propositional calculus;*
2. *the axioms of quantifiers, that is to say:*
   (a) *the formulas of the form* $(\exists x F \Leftrightarrow \neg\forall x \neg F)$, *where* F *is any formula and* x *is an arbitrary variable;*
   (b) *the formulas of the form* $(\forall x (F \Rightarrow G) \Rightarrow (F \Rightarrow \forall x G))$ *where* F *and* G *are arbitrary formulas and* x *is a variable that has no free occurrence in* F*;*
   (c) *the formulas of the form* $(\forall x F \Rightarrow F(t/x))$ *where* F *is a formula,* t *is a term and no free occurrence of* x *in* F *is covered by some quantifier bounding a variable of* t, *where* $F(t/x)$ *denotes the substitution of* x *by* t.

Exercise 11 *Prove that the logical axioms are valid.*

Remark 6 *We could not have put all the tautologies of propositional calculus, and, as we did for propositional calculus, restrict to certain axioms, essentially the axioms of Boolean logic. We does so here only to make the proofs simpler, but this could be possible and it would still work.*

We obtain the notion of demonstration.

Definition 7 (Demonstration by modus ponens and generalisation) *Let $\mathcal{T}$ be at theory and let F be some formula. A* proof of F from $\mathcal{T}$ *is a finite sequence $F_1, F_2, \cdots, F_n$ of formulas such that F_n is equal to F, and for all i, either F_i is in $\mathcal{T}$, or F_i is some logical axiom, or F_i is obtained by modus ponens from two formulas F_j, F_k with $j < i$ and $k < i$, or F_i is obtained by generalisation from a formula F_j with $j < i$.*

We write $\mathcal{T} \vdash F$ if F is provable from $\mathcal{T}$.

3.2 Finiteness theorem

We obtain first easily through the proof the finiteness theorem.

Theorem 3 (Finiteness theorem) *For every theory $\mathcal{T}$, and for any formula F, if $\mathcal{T} \vdash F$, then there exists a finite subset $\mathcal{T}_0$ of $\mathcal{T}$ such that $\mathcal{T}_0 \vdash F$.*

Proof: A demonstration is a finite sequence of formulas F_1, F_2, $\cdots, F_n$. Consequently, it is using only a finite number of formulas, hence a finite subset $\mathcal{T}_0$ of formulas of $\mathcal{T}$. This demonstration is also a demonstration of F in the theory $\mathcal{T}_0$. □

Corollary 1 *If $\mathcal{T}$ is a theory such that all finite subsets are coherent, then $\mathcal{T}$ is coherent.*

Proof: Otherwise $\mathcal{T}$ proves $(F \wedge \neg F)$, for some formula F, and by the finiteness formula, we deduce that there exists a finite subset $\mathcal{T}_0$ of $\mathcal{T}$ that also proves $(F \wedge \neg F)$. □

3.3 Some technical results

We need the following results, whose proofs are coming from a game on writing and rewriting on the demonstrations.

First of all an observation, but that has its importance:

Lemma 1 *If a theory $\mathcal{T}$ is not coherent, then any formula is provable in $\mathcal{T}$.*

Proof: Indeed, suppose that $\mathcal{T} \vdash F$ and that $\mathcal{T} \vdash \neg F$, and let G be some arbitrary formula. One can then put one after the other a demonstration of F and a demonstration of $\neg F$. To obtain a demonstration of G, it suffices to add the following formulas to this sequence: The tautology $F \Rightarrow (\neg F \Rightarrow G)$. The formula $\neg F \Rightarrow G$ which can then be obtained by modus ponens, since F has already appeared. Then the formula G, which can be obtained by modus ponens, since $\neg F$ has already appeared. □

Lemma 2 (Deduction lemma) *Suppose that $\mathcal{T} \cup \{F\} \vdash G$, with F some closed formula. Then $\mathcal{T} \vdash (F \Rightarrow G)$.*

Proof: From a demonstration $G_0 G_1 \cdots G_n$ of G in $\mathcal{T} \cup \{F\}$, we construct a demonstration of $(F \Rightarrow G)$ in $\mathcal{T}$ by inserting in the sequence $(F \Rightarrow G_0)(F \Rightarrow G_1) \cdots (F \Rightarrow G_n)$.

If G_i is a tautology, then there is nothing to do, since $(F \Rightarrow G_i)$ is also a tautology.

If G_i is F, then there is nothing to do, since $(F \Rightarrow G_i)$ is a tautology.

If G_i is an axiom of quantifiers or an element of $\mathcal{T}$, then it suffices to insert [1] between $(F \Rightarrow G_{i-1})$ and $(F \Rightarrow G_i)$ the formulas G_i and $(G_i \Rightarrow (F \Rightarrow G_i))$ (which is a tautology).

Suppose now that G_i is obtained by modus ponens: There are some integers $j, k < i$ such that G_k is $(G_j \Rightarrow G_i)$. We insert then between $(F \Rightarrow G_{i-1})$ and $(F \Rightarrow G_i)$ the formulas;

1. $((F \Rightarrow G_j) \Rightarrow ((F \Rightarrow (G_j \Rightarrow G_i)) \Rightarrow (F \Rightarrow G_i)))$ (a tautology);

2. $(F \Rightarrow (G_j \Rightarrow G_i)) \Rightarrow (F \Rightarrow G_i)$ that is obtained from modus ponens from the previous and thanks to $(F \Rightarrow G_j)$ which has already appeared;

3. $(F \Rightarrow G_i)$ is then deduced by modus ponens from this last formula and from $(F \Rightarrow (G_j \Rightarrow G_i))$, that has already appeared since it is $(F \Rightarrow G_k)$.

Suppose at last that G_i is obtained by generalisation from G_j with $j < i$. We insert in this case between $(F \Rightarrow G_{i-1})$ and $(F \Rightarrow G_i)$ the formulas:

1. $\forall x(F \Rightarrow G_j)$ obtained by generalisation starting from $(F \Rightarrow G_j)$;

2. $(\forall x(F \Rightarrow G_j) \Rightarrow (F \Rightarrow \forall x G_j))$ (a quantifier axiom). F being a closed formula, x is not free;

3. $(F \Rightarrow G_i)$ is then deduced by modus ponens from the two previous.

□

The corollary that follows can be seen as the justification of reasoning by contradictions.

Corollary 2 $\mathcal{T} \vdash F$ *if and only if* $\mathcal{T} \cup \{\neg F\}$ *is not coherent.*

[1] For $i = 0$, it suffices to position this formula at the beginning.

Proof: It is clear that if $\mathcal{T} \vdash F$ then $\mathcal{T} \cup \{\neg F\}$ is not coherent. Conversely, if $\mathcal{T} \cup \{\neg F\}$ is not coherent, it proves any formula, and in particular F by Lemma 1. Now, by the deduction lemma above, we obtain that $\mathcal{T} \vdash \neg F \Rightarrow F$. Now, $(\neg F \Rightarrow F) \Rightarrow F$ is a tautology, which proves that we have $\mathcal{T} \vdash F$. □

Lemma 3 *Let $\mathcal{T}$ be at theory, and let $F(x)$ be a formula whose only free variable is x. Let c be some constant symbol that is not appearing in F nor in $\mathcal{T}$. If $\mathcal{T} \vdash F(c/x)$ then $\mathcal{T} \vdash \forall x F(x)$.*

Proof: Consider a demonstration $F_1 F_2 \cdots F_n$ of $F(c/x)$ in $\mathcal{T}$. We consider a variable w that is in none of the formulas F_i and we call K_i the formula obtained by replacing in F_i the symbol c by w.

It turns out that this provides a proof of $F(w/x)$: If F_i is some logical axiom, then so does K_i; If F_i is deduced by modus ponens, and if $F_i \in \mathcal{T}$ then K_i is F_i.

By generalisation, we hence obtain a proof of $\forall w F(w/x)$, and by the remark that follows, we can then obtain a proof of $\forall x F(x)$. □

Remark 7 *If w is a variable that has no occurrence in F (nor free, nor bound), then we can prove $\forall w F(w/x) \Rightarrow \forall x F$: Indeed, since w has no occurrence in F, we can then prove $\forall w F(w/x) \Rightarrow F$, (axiom (c) of quantifiers, observing that $(F(w/x))(x/w) = F$ with these hypotheses). By generalisation, we obtain $\forall x(\forall w F(w/x) \Rightarrow F)$, and since x is not free in $\forall w F(w/x)$, the formula $\forall x(\forall w F(w/x) \Rightarrow F) \Rightarrow (\forall w F(w/x) \Rightarrow \forall x F)$ is among the axioms (b) of quantifiers, which allow to obtain $\forall w F(w/x) \Rightarrow \forall x F$ by modus ponens.*

3.4 Validity of the deduction system

The validity of the proof method is easy to obtain.

Theorem 4 (Validity) *Let $\mathcal{T}$ be a theory. Let F be some formula.*
If $\mathcal{T} \vdash F$, then any model of $\mathcal{T}$ is a model of the universal closure of F.

Proof: It suffices to check that the logical axioms are valid, and that modus ponens and generalisation can only infer some valid facts in any model of $\mathcal{T}$. □

This is the easy direction of the completeness theorem.

3.5 Completeness of the deduction system

The other direction consists in proving that if F is a consequence of $\mathcal{T}$, then F can be proved by our proof method.

Definition 8

We say that a theory $\mathcal{T}$ is complete *if for any closed formula F, we have $\mathcal{T} \vdash F$ or $\mathcal{T} \vdash \neg F$.*

We say that a theory $\mathcal{T}$ admits some Henkin witnesses *if for any formula $F(x)$ with some free variable x, there exists some constant symbol c in the signature* *such that* $(\exists x F(x) \Rightarrow F(c))$ *is a formula of the theory* $\mathcal{T}$.

The proof of completeness theorem due to *Henkin* that we will present runs in two steps.

1. We prove that any coherent theory, complete, with Henkin witnesses admits a model.

2. We prove that any consistent theory admits some with these three properties.

Lemma 4 *If* $\mathcal{T}$ *is some coherent, complete, with Henkin witnesses, then* $\mathcal{T}$ *has a model.*

Proof: The trick is to construct from scratch a model, whose base set (domain) is the set M of closed terms on the signature of the theory: This domain is non-empty, since the signature has at least the constants.

The structure $\mathfrak{M}$ is defined in the following way:

1. If c is a constant, the interpretation $c^{\mathfrak{M}}$ of c is the constant c itself.

2. If f is a function symbol of arity n, its interpretation $f^{\mathfrak{M}}$ is the function that to closed terms $t_1, \cdots, t_n$ associate the closed term $f(t_1, \cdots, t_n)$.

3. If R is a relation symbol of arity n, its interpretation $R^{\mathfrak{M}}$ is the subset of M^n made of the $(t_1, \cdots, t_n)$ such that $\mathcal{T} \vdash R(t_1, \cdots, t_n)$.

We observe that the structure that is obtained satisfies the following property For any closed formula F, $\mathcal{T} \vdash F$ if and only if $\mathfrak{M}$ is a model of F. This is proved by structural induction on F.

The property is true for the atomic formulas.

Because of the properties of the quantifiers and connectors, and because of the possibility of using occurrences of tautologies of propositional calculus in our proof method, it suffices to get convinced of this fact inductively on the formulas of type $\neg G$, $(G \vee H)$ and $\forall x G$.

1. Case $\neg G$: Since $\mathcal{T}$ is complete, $\mathcal{T} \vdash \neg G$ if and only if $\mathcal{T} \nvdash G$, which means inductively $\mathfrak{M} \not\models G$, or if one prefers $\mathfrak{M} \models \neg G$.

2. Case $(G \vee H)$: Suppose $\mathfrak{M} \models (G \vee H)$, and so $\mathfrak{M} \models G$ or $\mathfrak{M} \models H$. In the first case for example, by induction hypothesis, we have $\mathcal{T} \vdash G$, and since $(G \Rightarrow (G \vee H))$ is a tautology, we have $\mathcal{T} \vdash (G \vee H)$. Conversely, suppose that $\mathcal{T} \vdash (G \vee H)$. Si $\mathcal{T} \vdash G$ then by the induction hypothesis $\mathfrak{M} \models G$ and so $\mathfrak{M} \models (G \vee H)$. Otherwise, this is because $\mathcal{T} \nvdash G$, and since the theory is complete, we have $\mathcal{T} \vdash \neg G$. But since $(G \vee H \Rightarrow (\neg G \Rightarrow H))$ is a tautology, we obtain that $\mathcal{T} \vdash H$ and by the induction hypothesis, $\mathfrak{M} \models H$ and so $\mathfrak{M} \models (G \vee H)$.

3. Case $\exists x G(x)$: If $\mathfrak{M} \models \exists x G(x)$ this is because there is some closed term t such that $\mathfrak{M} \models G(t/x)$. By induction hypothesis, $\mathcal{T} \vdash G(t/x)$. But it is easy to find

a demonstration of $\exists x G(x)$ from a demonstration of $G(t/x)$. Conversely, suppose that $\mathcal{T} \vdash \exists x G(x)$. Thanks to Henkin witnesses, we deduce that there exists some constant c such that $\mathcal{T} \vdash G(c/x)$, and by induction hypothesis $\mathfrak{M} \models G(c/x)$, and so $\mathfrak{M} \models \exists x G(x)$.

□

There remains the second step. An *extension of at theory* $\mathcal{T}$ is a theory $\mathcal{T}'$ that contains $\mathcal{T}$.

Proposition 2 *Every coherent theory* $\mathcal{T}$ *on a countable signature* Σ *has some extension* $\mathcal{T}'$ *on a denumerable signature* Σ' *(with* Σ' *that contains* Σ*) that is coherent, complete and with Henkin witnesses.*

Before proving this property, let us discuss what we are obtaining: Since a model of $\mathcal{T}'$ is a model of $\mathcal{T}$, the previous lemma and the previous proposition permit first to obtain:

Corollary 3 *A denumerable coherent theory has a model.*

The following remark is obtained by playing with definitions:

Proposition 3 *For every theory* $\mathcal{T}$ *and for every closed formula* F*,* F *is a consequence of* T *if and only if* $\mathcal{T} \cup \{\neg F\}$ *has no model.*

Proof: If F is a consequence of $\mathcal{T}$, then by definition every model of $\mathcal{T}$ is a model of F, in other words, there is no model of $\mathcal{T} \cup \{\neg F\}$. The converse is trivial. □

We obtain with this remark exactly the completeness theorem (or the missing direction of what we called the completeness theorem).

Theorem 5 *Let* F *be some closed formula. If* F *is a consequence of the theory* $\mathcal{T}$*, then* $\mathcal{T} \vdash F$*.*

Proof: If $\mathcal{T}$ does not prove F, then $\mathcal{T} \cup \{\neg F\}$ is coherent: By the previous corollary, $\mathcal{T} \cup \{\neg F\}$ has a model. This means that F is not a consequence of the theory $\mathcal{T}$.
□

There remains to prove Proposition 2.

Proof: The signature Σ' is obtained by adding some denumerable number of new constants to the signature Σ. The obtained signature Σ' remains denumerable and we can enumerate the closed formulas $(F_n)_{n \in \mathbb{N}}$ of Σ'. The theory $\mathcal{T}'$ is obtained as the union of a increasing sequence of theories $\mathcal{T}_n$, defined by recurrence, starting from $\mathcal{T}_0 = \mathcal{T}$. Suppose that $\mathcal{T}_n$ is constructed and coherent. To construct $\mathcal{T}_{n+1}$ we consider the formula F_{n+1} in the enumeration of the closed formulas of Σ'. If $\mathcal{T}_n \cup F_{n+1}$ is coherent, then we let $G_n = F_{n+1}$, otherwise we let $G_n = \neg F_{n+1}$. In the two cases $\mathcal{T}_n \cup \{G_n\}$ is coherent.

The theory $\mathcal{T}_{n+1}$ is defined by:

1. $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{G_n\}$ if G_n is not of the form $\exists x H$.

2. otherwise: $\mathscr{T}_{n+1} = \mathscr{T}_n \cup \{G_n, H(c/x)\}$ where c is a new constant symbol that is not appearing in any formula of $T_n \cup \{G_n\}$: There is always such a symbol, there there is a finite number of symbols in $T_n \cup \{G_n\}$.

The theory $\mathscr{T}_{n+1}$ is coherent: Indeed, if it were not, this would mean that G_n would be of the form $\exists x H$, and that $T_n \cup \{\exists x H\} \vdash \neg H(c/x)$. By the choice of the constant c, and by Lemma 3, we obtain that $T_n \cup \{\exists x H\} \vdash \forall x \neg H(x)$, which is impossible since otherwise $\mathscr{T}_n$ would not be coherent.

The theory $\mathscr{T}' = \bigcup_{n\in\mathbb{N}} \mathscr{T}_n$ defined as the union of the theories $\mathscr{T}_n$ is coherent since any finite subset of it is contained in one of the theories $\mathscr{T}_n$, and hence is coherent.

The theory $\mathscr{T}'$ is also complete: If F is some closed formula of Σ', it appears at some moment in the enumeration of the formulas F_n, and by construction, either $F_n \in \mathscr{T}_n$ or $\neg F_n \in \mathscr{T}_n$.

Finally the theory $\mathscr{T}'$ has some Henkin witnesses: If $H(x)$ is a formula with the free variable x, then the formula $\exists x H$ appears as a formula in the enumeration of the formulas F_n. There are then two cases: either $\neg F_n \in \mathscr{T}_{n+1}$ or there is some constant c such that $H(c/x) \in \mathscr{T}_{n+1}$. In the two cases, $\mathscr{T}_{n+1} \vdash \exists x H(x) \Rightarrow H(c/x)$, which proves that $(\exists x H(x) \Rightarrow H(c/x))$ is in $\mathscr{T}'$ (otherwise its negation would be there, and $\mathscr{T}'$ would not be coherent). □

4 Compactness

Observe that we have also established some other facts.

Theorem 6 (Compactness theorem) *Let $\mathscr{T}$ a theory on some denumerable signature such that any finite subset of $\mathscr{T}$ has a model. Then $\mathscr{T}$ has a model.*

Proof: Consider a finite subset of such a theory $\mathscr{T}$. This subset is coherent since it has a model. $\mathscr{T}$ is hence a theory such that any finite subset is coherent. By finiteness theorem, this means that the theory itself is coherent.

By Corollary 3, this means that $\mathscr{T}$ has a model. □

Exercise 12 *(solution on page 235) Use compactness theorem to prove that there exists some non-standard model of Peano axioms.*

5 Other consequences

Theorem 7 (Löwenheim-Skolem) *If $\mathscr{T}$ is a theory on some denumerable signature that has a model, then it has a model whose base set is denumerable.*

Exercise 13 *(solution on page 235) Prove the theorem.*

6 Bibliographic notes

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

Bibliography This chapter has been written by essentially using the books [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.