Chapter 2
Models

After defining the concept of proof in the previous chapter, we will now study in this chapter some properties of proofs. In particular, we will introduce tools that will allow us to prove *independence results* of the form: the proposition A is not provable in the theory $\mathcal{T}$.

To define the notion of proof we had to restrict ourselves to combinatorial propositions, but to study properties of proofs we will not need to impose any restriction. Any mathematical tool can be used to show independence results.

2.1 The Notion of a Model

Definition 2.1 (Model) Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language. A *model* of this language is a structure $\mathcal{M} = ((\mathcal{M}_s)_{s\in\mathcal{S}}, \mathcal{B}, \mathcal{B}^+, (\hat{f})_{f\in\mathcal{F}}, (\hat{P})_{P\in\mathcal{P}}, \hat{\top}, \hat{\bot}, \hat{\neg}, \hat{\wedge}, \hat{\vee}, \hat{\Rightarrow}, \hat{\forall}, \hat{\exists})$ consisting of

- a non-empty set $\mathcal{M}_s$ for each sort s in $\mathcal{S}$,
- a non-empty set $\mathcal{B}$, and a subset $\mathcal{B}^+$ of $\mathcal{B}$,
- a function $\hat{f}$ from $\mathcal{M}_{s_1} \times \cdots \times \mathcal{M}_{s_n}$ to $\mathcal{M}_{s'}$ for each function symbol $f \in \mathcal{F}$ of arity $(s_1, \ldots, s_n, s')$,
- a function $\hat{P}$ from $\mathcal{M}_{s_1} \times \cdots \times \mathcal{M}_{s_n}$ to $\mathcal{B}$ for each predicate symbol $P \in \mathcal{P}$ of arity $(s_1, \ldots, s_n)$,
- two distinguished elements $\hat{\top}$ and $\hat{\bot}$ of $\mathcal{B}$, and
- a function $\hat{\neg}$ from $\mathcal{B}$ to $\mathcal{B}$, three functions $\hat{\wedge}$, $\hat{\vee}$ and $\hat{\Rightarrow}$ from $\mathcal{B} \times \mathcal{B}$ to $\mathcal{B}$ and two functions $\hat{\forall}$ and $\hat{\exists}$ from $\wp^+(\mathcal{B})$ to $\mathcal{B}$ where $\wp^+(\mathcal{B})$ is the set of all non-empty subsets of $\mathcal{B}$.

Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language and $\mathcal{M}$ a model of this language. We will define a function $[\![\ ]\!]$ associating to each term t of sort s an element $[\![t]\!]$ of $\mathcal{M}_s$, and to each proposition A an element $[\![A]\!]$ of $\mathcal{B}$. In addition, this function will be a morphism, that is, $[\![f(t_1, \ldots, t_n)]\!] = \hat{f}([\![t_1]\!], \ldots, [\![t_n]\!])$, $[\![P(t_1, \ldots, t_n)]\!] =$

G. Dowek, *Proofs and Algorithms*, Undergraduate Topics in Computer Science,
DOI 10.1007/978-0-85729-121-9_2, © Springer-Verlag London Limited 2011

$\hat{P}([\![t_1]\!], \ldots, [\![t_n]\!])$, $[\![A \wedge B]\!] = \hat{\wedge}([\![A]\!], [\![B]\!]), \ldots$ It is well known that a morphism between vector spaces is fully defined by the image of a basis. Similarly, a morphism between a language and a model is fully defined by the image of the variables. Therefore, we have the following definition.

Definition 2.2 (Valuation) Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language, $\mathcal{M}$ a model of this language and $(\mathcal{V}_s)_{s \in \mathcal{S}}$ a family of sets of variables. A *valuation* is a function, with a finite domain, that maps the variables $x_1, \ldots, x_n$ of sorts $s_1, \ldots, s_n$ to elements $a_1, \ldots, a_n$ of $\mathcal{M}_{s_1}, \ldots, \mathcal{M}_{s_n}$.

The valuation that associates the element a_1 to the variable $x_1, \ldots, a_n$ to the variable x_n will be written $x_1 = a_1, \ldots, x_n = a_n$. Let ϕ be a valuation, x a variable and a an element of $\mathcal{M}$, we denote by $(\phi, x = a)$ the valuation that coincides with ϕ everywhere except on x where it has the value a.

A valuation can be extended into a morphism $[\![\ ]\!]_\phi$ between terms and propositions of the language $\mathcal{L}$ with free variables in the domain of ϕ, and the model $\mathcal{M}$. The extension is defined as follows: $[\![x]\!]_\phi$ is $\phi(x)$, $[\![f(t_1, \ldots, t_n)]\!]_\phi$ is $\hat{f}([\![t_1]\!]_\phi, \ldots, [\![t_n]\!]_\phi)$, ... The definition is more complicated for bound variables and quantifiers. Indeed, the free variables of the proposition A are the free variables of $\forall x\ A$ and possibly x. To define $[\![\forall x\ A]\!]_\phi$ we must first consider all the values $[\![A]\!]_{\phi, x=a}$ obtained by associating x to an arbitrary element a of $\mathcal{M}_s$; we obtain in this way a non-empty subset of $\mathcal{B}$. We then apply the function $\hat{\forall}$ (which is a function from the set of all non-empty subsets of $\mathcal{B}$ to $\mathcal{B}$) to this set.

Definition 2.3 (Denotation) Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language, $\mathcal{M}$ a model of this language, $(\mathcal{V}_s)_{s \in \mathcal{S}}$ a family of sets of variables, ϕ a valuation and t a term with free variables in the domain of ϕ. The *denotation* of the term t in the model $\mathcal{M}$ under the valuation ϕ is the element $[\![t]\!]_\phi$ of $\mathcal{M}_s$ defined by induction over the structure of t as follows.

- $[\![x]\!]_\phi = \phi(x)$,
- $[\![f(t_1, \ldots, t_n)]\!]_\phi = \hat{f}([\![t_1]\!]_\phi, \ldots, [\![t_n]\!]_\phi)$.

Let A be a proposition with free variables in the domain of ϕ. The *denotation* of the proposition A in the model $\mathcal{M}$ under the valuation ϕ is an element $[\![A]\!]_\phi$ of $\mathcal{B}$ defined by induction over the structure of A as follows.

- $[\![P(t_1, \ldots, t_n)]\!]_\phi = \hat{P}([\![t_1]\!]_\phi, \ldots, [\![t_n]\!]_\phi)$,
- $[\![\top]\!]_\phi = \hat{\top}$,
- $[\![\bot]\!]_\phi = \hat{\bot}$,
- $[\![\neg A]\!]_\phi = \hat{\neg}([\![A]\!]_\phi)$,
- $[\![A \wedge B]\!]_\phi = \hat{\wedge}([\![A]\!]_\phi, [\![B]\!]_\phi)$,
- $[\![A \vee B]\!]_\phi = \hat{\vee}([\![A]\!]_\phi, [\![B]\!]_\phi)$,
- $[\![A \Rightarrow B]\!]_\phi = \hat{\Rightarrow}([\![A]\!]_\phi, [\![B]\!]_\phi)$,
- $[\![\forall x\ A]\!]_\phi = \hat{\forall}(\{[\![A]\!]_{\phi, x=a} \mid a \in \mathcal{M}_s\})$,
- $[\![\exists x\ A]\!]_\phi = \hat{\exists}(\{[\![A]\!]_{\phi, x=a} \mid a \in \mathcal{M}_s\})$.

Proposition 2.1 (Substitution)

$$\llbracket (u/x)t \rrbracket_\phi = \llbracket t \rrbracket_{\phi, x = \llbracket u \rrbracket_\phi}$$
$$\llbracket (u/x)A \rrbracket_\phi = \llbracket A \rrbracket_{\phi, x = \llbracket u \rrbracket_\phi}$$

Proof By induction over the structure of t and the structure of A. □

Definition 2.4 (Validity) Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language, $\mathcal{M}$ a model of this language, and $(\mathcal{V}_s)_{s\in\mathcal{S}}$ a family of sets of variables. A closed proposition is *valid* in the model $\mathcal{M}$ if $\llbracket A \rrbracket_\varnothing$ is in the set $\mathcal{B}^+$. In this case we will also say that $\mathcal{M}$ *is a model* of A.

A proposition A with free variables $x_1, \ldots, x_n$ is *valid* in the model $\mathcal{M}$ if the closed proposition $\forall x_1 \ldots \forall x_n\ A$ is valid, that is, if for every valuation ϕ whose domain includes the variables $x_1, \ldots, x_n$, $\llbracket A \rrbracket_\phi$ belongs to the set $\mathcal{B}^+$.

A sequent $A_1, \ldots, A_n \vdash B_1, \ldots, B_p$ is *valid* in the model $\mathcal{M}$ if the proposition $(A_1 \wedge \cdots \wedge A_n) \Rightarrow (B_1 \vee \cdots \vee B_p)$ is valid.

A theory $\mathcal{T}$ is *valid* in a model if all of its axioms are valid.

Definition 2.5 (Two-valued model) Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language. A *two-valued* model of $\mathcal{L}$ is a model such that $\mathcal{B} = \{0, 1\}$, $\mathcal{B}^+ = \{1\}$, $\hat{\top} = 1$, $\hat{\bot} = 0$ and $\hat{\neg}$, $\hat{\wedge}$, $\hat{\vee}$, $\hat{\Rightarrow}$ $\hat{\forall}$ and $\hat{\exists}$ are the functions

$\hat{\neg}$	0	1
	1	0

$\hat{\wedge}$	0	1
0	0	0
1	0	1

$\hat{\vee}$	0	1
0	0	1
1	1	1

$\hat{\Rightarrow}$	0	1
0	1	1
1	0	1

$\hat{\forall}$	$\{0\}$	$\{0, 1\}$	$\{1\}$
	0	0	1

$\hat{\exists}$	$\{0\}$	$\{0, 1\}$	$\{1\}$
	0	1	1

All the models that we will consider in the rest of the book will be two-valued.

Exercise 2.1 Consider a language with one term sort, consisting of a binary function symbol $+$ and a binary predicate $=$. Let $\mathcal{M}_1$ be the model consisting of the set $\mathbb{N}$, addition on $\mathbb{N}$ and the characteristic function of equality in $\mathbb{N}$, that is, the function $\hat{=}$ from $\mathbb{N}^2$ to $\{0, 1\}$ such that $\hat{=}(n, p) = 1$ if $n = p$ and $\hat{=}(n, p) = 0$ otherwise. Is the proposition $\forall x \forall y \exists z\ (x + z = y)$ valid in this model?

Same question for the model $\mathcal{M}_2$ consisting of the set $\mathbb{Z}$, addition and the characteristic function of equality in $\mathbb{Z}$.

Is the proposition $\forall x \forall y\ (x + y = y + x)$ valid in $\mathcal{M}_1$? And in $\mathcal{M}_2$? Give an example of a model in which this proposition is not valid.

2.2 The Soundness Theorem

One of the motivations for the study of models is that validity in a model is an invariant of provability: provable sequents are valid in all models. Thus, if a proposition is provable in a theory, then it is valid in all the models of the theory. This suggests a method to show that a proposition is not provable in a given theory: it is sufficient to show that there is a model of the theory in which the proposition is not valid. The second formulation of the soundness theorem given below states this principle.

Proposition 2.2 *If a sequent $A_1, \ldots, A_n \vdash B_1, \ldots, B_p$ is provable in natural deduction, then it is valid in all models.*

Proof By induction over the structure of proofs. □

The soundness theorem is a consequence of this proposition, and can be formulated in three different (equivalent) ways.

Theorem 2.1 (Soundness) *Let $\mathcal{T}$ be a theory and A a proposition.*

1. *If A is provable in $\mathcal{T}$, then A is valid in all the models of $\mathcal{T}$.*
2. *If there exists a model of $\mathcal{T}$ that is not a model of A, then A is not provable in $\mathcal{T}$.*
3. *If $\mathcal{T}$ has a model, then $\mathcal{T}$ is consistent.*

Proof Let $\mathcal{M}$ be a model of the theory $\mathcal{T}$ and let A be a proposition that is provable in $\mathcal{T}$. There exists a finite subset $H_1, \ldots, H_n$ of $\mathcal{T}$ such that the sequent $H_1, \ldots, H_n \vdash A$ is provable. By Proposition 2.2, this sequent is valid in $\mathcal{M}$, that is, the proposition $(H_1 \wedge \cdots \wedge H_n) \Rightarrow A$ is valid in this model. The propositions $H_1, \ldots, H_n$ are valid in $\mathcal{M}$, therefore, also A is valid in $\mathcal{M}$. This proves the first claim. The second claim is a trivial consequence of the first. The third is a consequence of the second taking $A = \bot$. □

Exercise 2.2 Consider the theory consisting of the axiom $P(c) \vee Q(c)$. Show that the proposition $P(c)$ is not provable in this theory. Show that the proposition $\neg P(c)$ is not provable either. What can be said of proposition $Q(c)$?

We can use the soundness theorem to prove that the axiom of infinity is not provable from the other axioms in *ZF*.

Definition 2.6 (The set of hereditarily finite sets) Let V_n be a sequence of sets defined by induction: $V_0 = \emptyset$ and $V_{i+1} = \wp(V_i)$. Let $V_\omega = \bigcup_i V_i$.

Proposition 2.3 *Let $\mathcal{M} = (\mathcal{M}_\iota, \mathcal{M}_\sigma, \hat{\epsilon}_2, \hat{=}, \hat{\in})$ be the model where $\mathcal{M}_\iota = V_\omega$, $\mathcal{M}_\sigma = \wp(\mathcal{M}_\iota \times \mathcal{M}_\iota)$, $\hat{\epsilon}_2$ is the function from $\mathcal{M}_\iota \times \mathcal{M}_\iota \times \mathcal{M}_\sigma$ to $\{0, 1\}$ such that $\hat{\epsilon}_2(a, b, c) = 1$ if (a, b) is in c and $\hat{\epsilon}_2(a, b, c) = 0$ otherwise, $\hat{=}$ is the function from $\mathcal{M}_\iota \times \mathcal{M}_\iota$ to $\{0, 1\}$ such that $\hat{=}(a, b) = 1$ if $a = b$ and $\hat{=}(a, b) = 0$ otherwise, $\hat{\in}$ the* *function from* $\mathcal{M}_\iota \times \mathcal{M}_\iota$ *to* $\{0, 1\}$ *such that* $\hat{\in}(a, b) = 1$ *if* a *is in* b *and* $\hat{\in}(a, b) = 0$ *otherwise.*

Then $\mathcal{M}$ *is a model of each of the axioms of ZF except the axiom of infinity.*

Proof We prove the case corresponding to the axiom of union. First, note that the union of a family of subsets of V_j is also a subset of V_j, and the union of a family of elements of V_{j+1} is an element of V_{j+1}. We will show that, if c is an element of V_ω, the union $\bigcup_{b\in c} b$ of the elements of c is also in V_ω. Since $c \in V_\omega$, by definition of V_ω there exists a natural number i different from zero such that $c \in V_i$. If $i = 1$, $c = \emptyset$ and the union of the elements of c is also the empty set, therefore it is an element of V_ω. Otherwise, there exists some natural number j such that $i = j + 2$. Since $c \in V_{j+2}$, $c \subseteq V_{j+1}$ and the elements of c are in V_{j+1}. Therefore, the union of the elements of c is also in V_{j+1}, hence in V_ω. Thus,

$$[\![\forall w\ (w \in z \Leftrightarrow (\exists v\ (w \in v \wedge v \in x)))]\!]_{x=c, z=\bigcup_{b\in c} b} = 1$$

and therefore

$$[\![\forall x \exists z \forall w\ (w \in z \Leftrightarrow (\exists v\ (w \in v \wedge v \in x)))]\!] = 1$$

We can prove in the same way that the axiom of extensionality, the axiom of the power set and the axiom of replacement are valid in this model.

The axioms of equality and the comprehension schema are trivially valid in this model.

Finally, we show by contradiction that the axiom of infinity is not valid in this model. First, note that we can prove by induction on i that all the elements of V_i are finite sets. As a consequence, all the elements of V_ω are finite sets.

Assume the axiom of infinity is valid in V_ω, then there is a set a in V_ω that contains the empty set and if it contains the set b it contains also the set $b \cup \{b\}$. Therefore, this set contains all the elements in the sequence defined by induction as follows: $e_0 = \emptyset$, $e_1 = \{e_0\}$, $e_2 = \{e_0, e_1\}$, $e_3 = \{e_0, e_1, e_2\}, \ldots, e_{i+1} = e_i \cup \{e_i\}, \ldots$. Since these elements are all different, the set a is infinite (contradiction). □

Proposition 2.4 *The axiom of infinity cannot be proved from the other axioms in ZF.*

Proof All the axioms in *ZF*, except the axiom of infinity, are valid in the model $\mathcal{M}$ defined in Proposition 2.3. □

2.3 The Completeness Theorem

The soundness theorem tells us that if a proposition A is provable in a theory $\mathcal{T}$ then it is valid in all the models of the theory. The completeness theorem, first proved in 1930 by K. Gödel (although it should not be confused with Gödel's famous theorem), is the converse of the soundness theorem.

2.3.1 Three Formulations of the Completeness Theorem

Similarly to the soundness theorem, the completeness theorem can be formulated in three different (but equivalent) ways.

Theorem 2.2 (Completeness) *Let $\mathcal{T}$ be a theory and A a proposition.*

1. *If A is valid in all the models of $\mathcal{T}$ then A is provable in $\mathcal{T}$.*
2. *If A is not provable in $\mathcal{T}$, then there exists a model of $\mathcal{T}$ which is not a model of A.*
3. *If $\mathcal{T}$ is consistent then $\mathcal{T}$ has a model.*

The first two formulations are trivially equivalent. The third one is a consequence of the second, taking $A = \perp$. We will show that (2) is a consequence of (3). Consider a theory $\mathcal{T}$ and a proposition A not provable in this theory. By Proposition 1.7, the proposition $\perp$ is not provable in the theory $\mathcal{T}, \neg A$. Therefore by (3) the theory $\mathcal{T}, \neg A$ has a model. This model is a model of $\mathcal{T}$ but not a model of A.

2.3.2 Proving the Completeness Theorem

We will prove the third formulation of the completeness theorem, restricting ourselves to the case of a finite or countable language.

Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be such a language and $\mathcal{T}$ a consistent theory in this language. We will build a model for this theory. The idea is to define the domain $\mathcal{M}_s$ as a set of closed terms of sort s, the function $\hat{f}$ as the function that associates to the closed terms $t_1, \dots, t_n$ the term $f(t_1, \dots, t_n)$ and $\hat{P}$ as the function that associates $t_1, \dots, t_n$ to 1 if the proposition $P(t_1, \dots, t_n)$ is provable and 0 if it is not provable.

There is a problem though: even if we assume that the theory $\mathcal{T}$ is consistent, this structure is not necessarily a model of the theory. For instance, if the theory $\mathcal{T}$ consists of the axiom $P(c) \vee Q(c)$, neither the proposition $P(c)$ nor the proposition $Q(c)$ is provable—see Exercise 2.2. Thus, according to the construction above, we have to define $\hat{P}(c) = 0$ and $\hat{Q}(c) = 0$, which means that the proposition $P(c) \vee Q(c)$ is not valid in this model.

To make sure that this construction works, first we need to complete the theory: if a proposition A is undetermined, that is, neither A nor $\neg A$ is provable, we must choose to add either the axiom A or the axiom $\neg A$. In our example, if we add the axiom $P(c)$ then when we build the model we will have $\hat{P}(c) = 1$ and thus the proposition $P(c) \vee Q(c)$ is valid in the model. If we decide to add the axiom $\neg P(c)$ instead, then the proposition $Q(c)$ becomes provable, and when we build the model we have $\hat{Q}(c) = 1$, thus the proposition $P(c) \vee Q(c)$ is again valid.

However, it is not sufficient to complete the theory. For example, consider the theory $\neg P(c), \exists x \; P(x)$. In this case, according to the construction described above, we have to define $\mathcal{M} = \{c\}$ and $\hat{P}(c) = 0$. Therefore the proposition $\exists x \; P(x)$ is not valid in this model. The problem here is that no closed term can be used as a witness of the fact that there is an object satisfying the property P. To solve this problem, we need to add a constant d and an axiom $P(d)$ before building the model. This constant d is called *Henkin's witness* for the proposition $\exists x\ P(x)$.

To prove the completeness theorem we need to show first the following property.

Proposition 2.5 *Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a language and $\mathcal{T}$ a consistent theory in this language. There exists a language $\mathcal{L}'$ such that $\mathcal{L} \subseteq \mathcal{L}'$, and a theory $\mathcal{U}$ in the language $\mathcal{L}'$, such that $\mathcal{T} \subseteq \mathcal{U}$ and the following properties hold.*

1. *The theory $\mathcal{U}$ is consistent.*
2. *For any closed proposition A in the language $\mathcal{L}'$, either the proposition A or the proposition $\neg A$ is provable in $\mathcal{U}$.*
3. *If the proposition $\exists x\ A$ is provable in $\mathcal{U}$, there exists a constant c such that $(c/x)A$ is provable in $\mathcal{U}$.*

To prove this proposition we proceed as in the proof of the theorem of the incomplete basis: we inspect all the propositions, one by one, in order to select some of the them. When inspecting a proposition A, we check whether A or $\neg A$ is provable from the axioms in $\mathcal{T}$ and the propositions already retained. If A is provable, we select it. If $\neg A$ is provable, we select it. If neither A nor $\neg A$ is provable, we choose A to be retained (this is an arbitrary choice). Moreover, if A has the form $\exists x\ B$, then we also retain the proposition $(c/x)B$ where c is a new constant to be added to the language.

Proof Let $\mathcal{H} = \{c_i^s\}$ be a countable set containing an infinite number of constants $c_0^s, c_1^s, c_2^s, \ldots$ for each sort s. Let $\mathcal{L}'$ be the language $(\mathcal{S}, \mathcal{F} \uplus \mathcal{H}, \mathcal{P})$.

The language $\mathcal{L}'$ and the sets $\mathcal{V}_s$ are countable, therefore the set of propositions in this language is countable. Let $A_0, A_1, A_2, \ldots$ be the elements in this set. We define a family of theories $\mathcal{U}_n$ as follows. We start by defining $\mathcal{U}_0 = \mathcal{T}$. If A_n is provable in the theory $\mathcal{U}_n$, we define $B = A_n$; if $\neg A_n$ is provable in the theory $\mathcal{U}_n$, we define $B = \neg A_n$ and if neither of them is provable in the theory $\mathcal{U}_n$, then we arbitrarily define $B = A_n$. If B does not have the form $\exists x\ C$, then we define $\mathcal{U}_{n+1} = \mathcal{U}_n \cup \{B\}$; if B has the form $\exists x\ C$, we define $\mathcal{U}_{n+1} = \mathcal{U}_n \cup \{B, (c_i^s/x)C\}$, where s is the sort of x and i is the least natural number such that the constant c_i^s is neither in $\mathcal{U}_n$ nor in B. Such a constant exists because each $\mathcal{U}_i$ contains only a finite number of constants from $\mathcal{H}$. Finally, we define $\mathcal{U} = \bigcup_i \mathcal{U}_i$.

We can show by induction on i that all the theories $\mathcal{U}_i$ are consistent. As a consequence the theory $\mathcal{U}$ is also consistent. Indeed, if we assume that a proof for $\perp$ exists in $\mathcal{U}$ we obtain a contradiction: If $\perp$ is provable, then there is a finite subset $B_1, \ldots, B_n$ of $\mathcal{U}$ such that the sequent $B_1, \ldots, B_n \vdash \perp$ is provable. Each proposition B_j belongs to one of the sets $\mathcal{U}_{i_j}$ and they all belong to $\mathcal{U}_k$ where k is the greatest of the i_j. This means that the theory $\mathcal{U}_k$ is contradictory (a contradiction).

Let A be an arbitrary closed proposition. There exists an index i such that $A_i = A$ and either A or $\neg A$ is an element of $\mathcal{U}_{i+1}$. Hence, the theory $\mathcal{U}$ contains the axiom A or the axiom $\neg A$ and one of these propositions is provable.

Finally, if the proposition $\exists x\ A$ is provable in $\mathcal{U}$, then there exists an index i such that $A_i = \exists x\ A$. Since the theory $\mathcal{U}_i$ is consistent and the proposition A_i is provable, the proposition $\neg A_i$ is not provable. Therefore, $\mathcal{U}_{i+1} = \mathcal{U}_i \cup \{\exists x\ A, (c/x)A\}$ for some constant c. This means that the theory $\mathcal{U}$ contains the axiom $(c/x)A$ and this proposition is provable. □

Proposition 2.6 *Let $\mathcal{U}$ be a theory satisfying the following properties*:

1. *The theory $\mathcal{U}$ is consistent.*
2. *For any closed proposition A, either A or $\neg A$ is provable in $\mathcal{U}$.*
3. *If the proposition $\exists x\ A$ is provable in $\mathcal{U}$, there exists a closed term t such that the proposition $(t/x)A$ is also provable in $\mathcal{U}$.*

Then

- *The proposition $\neg A$ is provable in $\mathcal{U}$ if and only if the proposition A is not provable in $\mathcal{U}$.*
- *The proposition $A \wedge B$ is provable in $\mathcal{U}$ if and only if the proposition A is provable in $\mathcal{U}$ and the proposition B is provable in $\mathcal{U}$.*
- *The proposition $A \vee B$ is provable in $\mathcal{U}$ if and only if the proposition A is provable in $\mathcal{U}$ or the proposition B is provable in $\mathcal{U}$.*
- *The proposition $A \Rightarrow B$ is provable in $\mathcal{U}$ if and only if the proposition A is provable in $\mathcal{U}$, then so is the proposition B.*
- *The proposition $\forall x\ A$ is provable in $\mathcal{U}$ if and only if for all closed term t, the proposition $(t/x)A$ is provable in $\mathcal{U}$.*
- *The proposition $\exists x\ A$ is provable in $\mathcal{U}$ if and only if there exists a closed term t such that the proposition $(t/x)A$ is provable in $\mathcal{U}$.*

Proof

- If the proposition A is provable in $\mathcal{U}$ then the proposition $\neg A$ is not, because the theory $\mathcal{U}$ is consistent. Conversely, the second condition implies that if the proposition $\neg A$ is not provable in $\mathcal{U}$, then the proposition A is provable in $\mathcal{U}$.
- If the propositions A and B are provable in $\mathcal{U}$ then the proposition $A \wedge B$ is also provable, using the $\wedge$-intro rule. Conversely, if the proposition $A \wedge B$ is provable in $\mathcal{U}$, then the propositions A and B are also provable, using the $\wedge$-elim rule.
- If the proposition A or the proposition B is provable in $\mathcal{U}$ then so is the proposition $A \vee B$, using the $\vee$-intro rule. Conversely, if the proposition $A \vee B$ is provable in $\mathcal{U}$, then, the second condition implies that the proposition A or the proposition $\neg A$ is provable in $\mathcal{U}$. In the first case, the proposition A is provable in $\mathcal{U}$, and in the second, since the proposition $A \vee B$ and $\neg A$ are provable, the proposition B is also provable in $\mathcal{U}$ using the rules *axiom*, $\neg$-elim, $\bot$-elim and $\vee$-elim.
- Assume that if the proposition A is provable in $\mathcal{U}$ then the proposition B is provable in $\mathcal{U}$. The second condition implies that either the proposition A or the proposition $\neg A$ is provable in $\mathcal{U}$. In the first case, the proposition B is provable in $\mathcal{U}$ and therefore the proposition $A \Rightarrow B$ is provable using the $\Rightarrow$-intro rule. In the second case, the proposition $\neg A$ is provable and therefore the proposition $A \Rightarrow B$

is provable using the rules $\Rightarrow$-intro, $\bot$-elim and $\neg$-elim. Conversely, if $A \Rightarrow B$ is provable in $\mathcal{U}$, then, if A is provable in $\mathcal{U}$ then B is provable in $\mathcal{U}$ using the $\Rightarrow$-elim rule.

– Assume that for every closed term t the proposition $(t/x)A$ is provable in $\mathcal{U}$. If the proposition $\exists x\ \neg A$ is provable in $\mathcal{U}$, then, according to the third condition, there exists a closed term t such that $\neg(t/x)A$ is provable. But then the theory $\mathcal{U}$ would be contradictory, against our assumptions. Therefore the proposition $\exists x\ \neg A$ is not provable in $\mathcal{U}$ and $\neg\exists x\ \neg A$ is. The proposition $\forall x\ A$ is thus provable, by Proposition 1.8. Conversely, if the proposition $\forall x\ A$ is provable in the theory $\mathcal{U}$, all the propositions $(t/x)A$ are provable using the $\forall$-elim rule.
– If there exists a closed term t such that the proposition $(t/x)A$ is provable in $\mathcal{U}$ then the proposition $\exists x\ A$ is provable using the $\exists$-intro rule. Conversely, if the proposition $\exists x\ A$ is provable in $\mathcal{U}$ then, according to the third condition, there exists a closed term t such that $(t/x)A$ is provable in $\mathcal{U}$.

$\square$

We are finally in a position to prove the completeness theorem.

Proof Let $\mathcal{T}$ be a consistent theory and $\mathcal{U}$ the theory built in Proposition 2.5. We define the domain $\mathcal{M}_s$ to be the set of closed terms of sort s in the language $\mathcal{L}'$, the function $\hat{f}$ to be the function associating to the closed terms $t_1, \ldots, t_n$ the term $f(t_1, \ldots, t_n)$ and the function $\hat{P}$ to be the function associating to $t_1, \ldots, t_n$ the number 1 if the proposition $P(t_1, \ldots, t_n)$ is provable in $\mathcal{U}$ and 0 otherwise.

Let A be a closed proposition. We show by induction over the structure of the proposition A that A is provable in $\mathcal{U}$ if and only if A is valid in this model. If A is an atomic proposition, the equivalence follows directly from the definition of the functions $\hat{P}$. If A is a proposition of the form $B \wedge C$, then the proposition A is provable in $\mathcal{U}$ if and only if the propositions B and C are provable—Proposition 2.6—if and only if the propositions B and C are valid in $\mathcal{M}$—inductive hypothesis—if and only if the proposition A is valid in $\mathcal{M}$. The other cases are similar. $\square$

In this proof we have only considered finite or countable languages. The completeness theorem applies also to non-countable languages and the proof follows the same lines. Only the proof of Proposition 2.5 differs. First, we need to add a set of constants for each sort, which must have the same cardinal as the language. Second, instead of enumerating the propositions, we need to well-order them using the axiom of choice. Finally, the family of sets $(\mathcal{U}_i)_i$ will no longer be indexed by the natural numbers, we will need a greater ordinal.

2.3.3 Models of Equality—Normal Models

Definition 2.7 (Normal model) Let $\mathcal{L}$ be a language containing predicates $=_s$ of sort (s, s) for some sorts s, and $\mathcal{T}$ be a theory containing at least the axioms of equality for these sorts. A *normal model* of the theory $\mathcal{T}$ is a model in which the functions $\hat{=}_s$ over $\mathcal{M}_s$ are defined by $\hat{=}_s(x, y) = 1$ if $x = y$ and $\hat{=}_s(x, y) = 0$ otherwise.

Proposition 2.7 (Completeness of normal models) *Let $\mathcal{T}$ be a theory containing at least the axioms of equality. If $\mathcal{T}$ is consistent then it has a normal model.*

Proof Since the theory is consistent, it has a model $\mathcal{M}$. For every sort s for which there is an equality predicate in the language, let R_s be the relation containing the pairs of elements a and b such that $\hat{=}(a, b) = 1$. This is an equivalence relation. We define $\mathcal{M}'_s = \mathcal{M}_s/R_s$. Since the model $\mathcal{M}$ is a model of the equality axioms, the functions $\hat{f}$ and $\hat{P}$ can be defined on the quotient. In this way we can define a normal model $\mathcal{M}'$ that satisfies the same propositions as $\mathcal{M}$. It is therefore a model of $\mathcal{T}$. □

2.3.4 Proofs of Relative Consistency

The completeness theorem can be used to build proofs of *relative consistency*. The model V_ω defined in Sect. 2.2 is a model of the theory ZF^f, that is, the theory consisting of the axioms of *ZF* except that the axiom of infinity is replaced by its negation. It is possible to formalise the construction of this model in *ZF*. In other words, the proposition "There exists a model of ZF^f" is provable in *ZF*. The soundness theorem allows us to deduce then that the proposition "The theory ZF^f is consistent" is provable in *ZF*.

This kind of result is not standard, it is in fact an exception. If instead of the elementary theory ZF^f we consider a more interesting theory, such as *ZFC* or $ZF\neg C$, which are obtained by adding to the axioms of *ZF* the axiom of choice or its negation, respectively, then as a consequence of Gödel's second incompleteness theorem—which is out of the scope of this book, but shows that under general conditions the consistency of a theory cannot be proved in the same theory—we know that it is impossible to prove in *ZF* the consistency of *ZF*, and *a fortiori* that of *ZFC* or $ZF\neg C$.

Nevertheless, it is possible to prove in *ZF* relative consistency theorems. For instance, K. Gödel proved that if the theory *ZF* is consistent, then so is the theory *ZFC*, and A. Fraenkel and A. Mostowski proved that if the theory *ZF* is consistent then so is the theory $ZF\neg C$.

In other words, to prove the consistency of the theories *ZFC* and $ZF\neg C$, we add the axiom "The theory *ZF* is consistent" to the usual mathematical theories formalised in *ZF*. Then, these proofs will use the completeness theorem to deduce from the consistency of *ZF* the existence of a model of *ZF* and finally use this model to build a model of *ZFC* or $ZF\neg C$.

Exercise 2.3 In this exercise, inspired by the proof of relative consistency of $ZF\neg C$ proposed by Fraenkel and Mostowski, we will show that if *ZF* is consistent then

ZF$^+$ is consistent, where *ZF*$^+$ is the theory obtained by adding to *ZF* the axiom $\exists x\ (x \in x)$. In other words, if *ZF* is consistent then the proposition $\neg\exists x\ (x \in x)$ is not provable.

1. Show that the following propositions are equivalent.
   (a) If *ZF* is consistent then *ZF*$^+$ is consistent.
   (b) If *ZF* has a model then *ZF*$^+$ has a model.
   (c) If *ZF* has a normal model then *ZF*$^+$ has a normal model.
   Our aim is to prove the proposition (c). Let $\mathcal{M} = (\mathcal{M}, \mathcal{C}, \hat{\epsilon}_2, \hat{\in})$ be a normal model of *ZF*.
2. Show that there exists an element 0 in $\mathcal{M}$ such that none of the elements a of $\mathcal{M}$ satisfies $a \mathrel{\hat{\in}} 0$. Show that there exists an element 1 in $\mathcal{M}$ such that for every element a in $\mathcal{M}$, we have $a \mathrel{\hat{\in}} 1$ if and only if $a = 0$.

   Let f be the bijection from $\mathcal{M}$ to $\mathcal{M}$ defined by $f(0) = 1$, $f(1) = 0$ and $f(a) = a$ if a is different from 0 and 1. Let $\mathcal{M}'$ be the model $(\mathcal{M}, \mathcal{C}, \hat{\epsilon}_2, \hat{\in}')$ where $\hat{\in}'$ is the relation such that $a \mathrel{\hat{\in}'} b$ if and only if $a \mathrel{\hat{\in}} f(b)$. The goal is to prove that $\mathcal{M}'$ is a normal model of *ZF*$^+$.
3. Show that there exists a proposition *Zero* such that $[\![Zero]\!]^{\mathcal{M}}_{x=a} = 1$ if and only if $a = 0$. Show that there exists a proposition *One* such that $[\![One]\!]^{\mathcal{M}}_{x=a} = 1$ if and only if $a = 1$. Show that there exists a proposition F such that $[\![F]\!]^{\mathcal{M}}_{x=a,y=b} = 1$ if and only if $b = f(a)$. Show that there exists a proposition E such that $[\![E]\!]^{\mathcal{M}}_{x=a,y=b} = 1$ if and only if $a \mathrel{\hat{\in}'} b$. Show that $\mathcal{M}'$ is a model of the binary comprehension schema.
4. Show that the axiom of extensionality is valid in $\mathcal{M}'$.
5. Let a be an element of $\mathcal{M}$. Define $a_1 = f(a)$. Show that there exists an element a_2 of $\mathcal{M}$ such that $x \mathrel{\hat{\in}} a_2$ if and only if there exists some y such that $x = f(y)$ and $y \mathrel{\hat{\in}} a_1$. Show that there exists an element a_3 of $\mathcal{M}$ such that $x \mathrel{\hat{\in}} a_3$ if and only if there exists some z such that $x \mathrel{\hat{\in}} z$ and $z \mathrel{\hat{\in}} a_2$. Let $a_4 = f^{-1}(a_3)$. Show that $x \mathrel{\hat{\in}'} a_4$ if and only if there exists some y such that $x \mathrel{\hat{\in}'} y$ and $y \mathrel{\hat{\in}'} a$. Show that the axiom of union is valid in $\mathcal{M}'$.
6. Let a be an element of $\mathcal{M}$. Define $a_1 = f(a)$. Show that there exists an element a_2 of $\mathcal{M}$ such that $x \mathrel{\hat{\in}} a_2$ if and only if for every z, $z \mathrel{\hat{\in}} x$ implies $z \mathrel{\hat{\in}} a_1$. Show that there exists an element a_3 of $\mathcal{M}$ such that $x \mathrel{\hat{\in}} a_3$ if and only if $f(x) \mathrel{\hat{\in}} a_2$. Let $a_4 = f^{-1}(a_3)$. Show that $x \mathrel{\hat{\in}'} a_4$ if and only if for every z, $z \mathrel{\hat{\in}'} x$ implies $z \mathrel{\hat{\in}'} a$. Show that the axiom of the power set is valid in $\mathcal{M}'$.
7. Let a be an element of $\mathcal{M}$ and r an element of $\mathcal{C}$ that is a functional binary class (more precisely, if $a, b \mathrel{\hat{\epsilon}_2} r$ and $a, b' \mathrel{\hat{\epsilon}_2} r$ then $b = b'$). Define $a_1 = f(a)$. Show that there exists an element a_2 of $\mathcal{M}$ such that $x \mathrel{\hat{\in}} a_2$ if and only if there exists some y such that $y \mathrel{\hat{\in}} a_1$ and $y, x \mathrel{\hat{\epsilon}_2} r$. Let $a_3 = f^{-1}(a_2)$. Show that $x \mathrel{\hat{\in}'} a_3$ if and only if there exists some y such that $y \mathrel{\hat{\in}'} a$ and $y, x \mathrel{\hat{\epsilon}_2} r$. Show that the axiom of replacement is valid in $\mathcal{M}'$.
8. In this question we will assume that the following result is true (it was proved in Exercise 1.18): *If a is an element of $\mathcal{M}$ and r an element of $\mathcal{C}$ that is a functional binary class, then there exists an element E of $\mathcal{M}$ such that $a \mathrel{\hat{\in}} E$ and if $x \mathrel{\hat{\in}} E$ and $x, x' \mathrel{\hat{\epsilon}_2} r$ then $x' \mathrel{\hat{\in}} E$.*

   Show that there is no object a such that $a \mathrel{\hat{\in}'} 1$.

Let a be an element of $\mathcal{M}$. Let $S(a)$ be the element of $\mathcal{M}$ such that $x \mathrel{\hat{\in}} S(a)$ if and only if $x \mathrel{\hat{\in}} a$ or $x = a$ and let $S'(a)$ be the element of $\mathcal{M}$ such that $x \mathrel{\hat{\in}'} S'(a)$ if and only if $x \mathrel{\hat{\in}'} a$ or $x = a$. Show that if a is neither 0 nor 1, then $S'(a) = S(a)$. What is the object $S'(0)$? And the object $S'(1)$? Show that the binary class r such that $a, b \mathrel{\hat{\in}_2} r$ if $b = S'(a)$ is in $\mathcal{C}$ and is functional.

Show that there exists a set I' that contains 1 and such that if $a \mathrel{\hat{\in}} I'$ then $S'(a) \mathrel{\hat{\in}} I'$.

Show that the axiom of infinity is valid in $\mathcal{M}'$.

9. Show that $0 \mathrel{\hat{\in}'} 0$. Show that the proposition $\exists x\ (x \in x)$ is valid in $\mathcal{M}'$.

2.3.5 *Conservativity*

Definition 2.8 (Extension) Let $\mathcal{L}$ and $\mathcal{L}'$ be two languages such that $\mathcal{L} \subseteq \mathcal{L}'$. Let $\mathcal{T}$ be a theory in the language $\mathcal{L}$ and $\mathcal{T}'$ a theory in $\mathcal{L}'$. The theory $\mathcal{T}'$ is an *extension* of $\mathcal{T}$ if every proposition that is provable in $\mathcal{T}$ is also provable in $\mathcal{T}'$.

Definition 2.9 (Conservative extension) Let $\mathcal{L}$ and $\mathcal{L}'$ be two languages such that $\mathcal{L} \subseteq \mathcal{L}'$. Let $\mathcal{T}$ be a theory in the language $\mathcal{L}$ and $\mathcal{T}'$ a theory in $\mathcal{L}'$. Assume that $\mathcal{T}'$ is an extension of $\mathcal{T}$. The theory $\mathcal{T}'$ is a *conservative* extension of $\mathcal{T}$ if every proposition in $\mathcal{L}$ provable in $\mathcal{T}'$ is also provable in $\mathcal{T}$.

For example, if the language $\mathcal{L}$ contains a constant c and a predicate symbol P, and if the theory $\mathcal{T}$ consists of the axiom $P(c)$, then, by adding a constant d and the axiom $P(d)$ we obtain a conservative extension: although the proposition $P(d)$ is provable in $\mathcal{T}'$ but not in $\mathcal{T}$, we will see that all the propositions of the language $\mathcal{L}$—note that $P(d)$ is not one of them—that are provable in $\mathcal{T}'$ are also provable in $\mathcal{T}$.

Note that if the language $\mathcal{L}$ contains a constant c and a predicate symbol P, and if the theory $\mathcal{T}$ is empty, then by adding a constant d and the axiom $P(d)$ we obtain an extension which is not conservative. Indeed , the proposition $\exists x\ P(x)$, which is well formed in $\mathcal{T}$, is provable in $\mathcal{T}'$ but not in $\mathcal{T}$.

Although in a small example such as the one above it is possible to show that an extension is conservative by showing that proofs in $\mathcal{T}'$ can be translated into proofs in $\mathcal{T}$, in the general case the situation is more complicated. The completeness theorem is a useful tool to prove that a theory is a conservative extension of another one.

Definition 2.10 (Extension of a model) Let $\mathcal{L}$ and $\mathcal{L}'$ be two languages such that $\mathcal{L} \subseteq \mathcal{L}'$. Let $\mathcal{M}$ be a model of $\mathcal{L}$ and $\mathcal{M}'$ a model of $\mathcal{L}'$. The model $\mathcal{M}'$ is an *extension* of $\mathcal{M}$ if for every sort s of $\mathcal{L}$ we have $\mathcal{M}_s = \mathcal{M}'_s$ and for every function or predicate symbol f of $\mathcal{L}$ we have $\hat{f}^{\mathcal{M}} = \hat{f}^{\mathcal{M}'}$.

Proposition 2.8 *Let $\mathcal{L}$ be a language and $\mathcal{T}$ a theory in this language. Let $\mathcal{L}'$ be a language such that $\mathcal{L} \subseteq \mathcal{L}'$ and let $\mathcal{T}'$ be a theory in $\mathcal{L}'$ such that $\mathcal{T} \subseteq \mathcal{T}'$. If for* *every model $\mathcal{M}$ of $\mathcal{T}$ there exists an extension $\mathcal{M}'$ of $\mathcal{M}$ that is a model of $\mathcal{T}'$, then $\mathcal{T}'$ is a conservative extension of $\mathcal{T}$.*

Proof Let A be a proposition in the language $\mathcal{L}$. Assume that A is provable in $\mathcal{T}'$. Let $\mathcal{M}$ be an arbitrary model of $\mathcal{T}$. There exists a model $\mathcal{M}'$ of $\mathcal{T}'$ that is an extension of $\mathcal{M}$. Since $\mathcal{M}'$ is a model of $\mathcal{T}'$, the proposition A is valid in $\mathcal{M}'$, therefore its denotation in $\mathcal{M}'$ is 1. Since $\mathcal{M}'$ is an extension of $\mathcal{M}$ the denotation of A in $\mathcal{M}$ is also 1. The proposition A is therefore valid in $\mathcal{M}$. Since the proposition A is valid in all the models of $\mathcal{T}$, it is provable in $\mathcal{T}$. □

For example, if $\mathcal{L}$ contains c and P and the theory $\mathcal{T}$ consists of the axiom $P(c)$, then by adding a constant d and the axiom $P(d)$ we obtain a conservative extension. Indeed, any model $\mathcal{M}$ of $\mathcal{T}$ can be extended into a model of $\mathcal{T}'$ by defining $\hat{d} = \hat{c}$.

Exercise 2.4 In Exercise 1.6, we showed that the propositions A and theories $\mathcal{T}$ of a many-sorted language can be relativised to propositions $|A|$ and theories $|\mathcal{T}|$ in a single-sorted language. Then, if the closed proposition A is provable in $\mathcal{T}$, the proposition $|A|$ is provable in $|\mathcal{T}|$.

Show that the converse also holds: if $|A|$ is provable in $|\mathcal{T}|$ then A is provable in $\mathcal{T}$.

When formulating arithmetic or set theory, we can avoid introducing classes, and thus the sorts κ and σ and the symbols ϵ and ϵ_2, if we replace each axiom that uses classes by an axiom schema, that is, an infinite set of axioms. For example, the axiom of induction can be replaced by the induction schema, defined as the set of axioms

$$\forall x_1 \ldots \forall x_n \ ((0/y)A \Rightarrow \forall m \ ((m/y)A \Rightarrow (S(m)/y)A) \Rightarrow \forall n \ (n/y)A)$$

for each proposition A, where $x_1, \ldots, x_n$ are the free variables of A that are different from y. For example, for the proposition $y + 0 = y$ we have the axiom

$$0 + 0 = 0 \Rightarrow \forall m \ (m + 0 = m \Rightarrow S(m) + 0 = S(m)) \Rightarrow \forall n \ (n + 0 = n)$$

We obtain in this way the theory defined below.

Definition 2.11 The language of arithmetic contains a constant 0, a unary function symbol S, two binary function symbols $+$ and $\times$ and a binary predicate symbol $=$. In addition to the axioms of equality, we have the axioms

$$\forall x \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \ \neg(0 = S(x))$$

$$\forall x_1 \ldots \forall x_n \ ((0/y)A \Rightarrow \forall m \ ((m/y)A \Rightarrow (S(m)/y)A) \Rightarrow \forall n \ (n/y)A)$$

$$\forall y \ (0 + y = y)$$

$$\forall x \forall y\ (S(x) + y = S(x + y))$$

$$\forall y\ (0 \times y = 0)$$

$$\forall x \forall y\ (S(x) \times y = (x \times y) + y)$$

We can now show that the single-sorted theory of classes is a conservative extension of this theory. More generally, for any theory that contains an axiom schema, there is an alternative definition in the theory of classes where the schema is simply replaced by one axiom. We will show this result only for the case of arithmetic, to avoid having to formalise the notion of an axiom schema in the general case.

Proposition 2.9 *The formulation of the theory of arithmetic given in Definition* 1.33 *is a conservative extension of the one given in Definition* 2.11.

Proof Each instance of the induction schema can be proved in the theory given in Definition 1.33. Therefore, this theory is an extension of the one presented in Definition 2.11. To show that the extension is conservative, we show that every model of the theory given in Definition 2.11 can be extended to a model of the theory in Definition 1.33.

Let $(\mathcal{M}, \hat{0}, \hat{S}, \hat{+}, \hat{\times}, \hat{=})$ be a model of the theory given in Definition 2.11. A subset E of $\mathcal{M}$ is *definable in arithmetic* if there exists a proposition A in the language of the theory given in Definition 2.11, with free variables in $x_1, \ldots, x_n, y$, and elements $a_1, \ldots, a_n$ in $\mathcal{M}$, such that b is in E if and only if

$$[\![A]\!]_{x_1=a_1,\ldots,x_n=a_n,y=b} = 1$$

Let $\overline{\wp}(\mathcal{M})$ be the set of all the definable subsets of $\mathcal{M}$. We extend the model $\mathcal{M}$, by defining $\mathcal{M}_\kappa = \overline{\wp}(\mathcal{M})$ and $\hat{\epsilon}(b, E) = 1$ if b is an element of E and 0 otherwise.

The resulting structure is a model of the comprehencion schema. We now prove that it is a model of the axiom of induction.

$$\forall c\ (0 \epsilon c \Rightarrow \forall m\ (m \epsilon c \Rightarrow S(m) \epsilon c) \Rightarrow \forall n\ n \epsilon c)$$

For this, we consider an arbitrary element E of $\mathcal{M}_\kappa$ and show that

$$[\![(0 \epsilon c \Rightarrow \forall m\ (m \epsilon c \Rightarrow S(m) \epsilon c) \Rightarrow \forall n\ n \epsilon c)]\!]_{c=E} = 1$$

The set E is definable; let A and $a_1, \ldots, a_n$ be a proposition and elements of $\mathcal{M}$, respectively, defining E. Then $\mathcal{M}$ is a model of the instance of the induction schema corresponding to A, and therefore

$$[\![(0/y)A \Rightarrow \forall m\ ((m/y)A \Rightarrow (S(m)/y)A) \Rightarrow \forall n\ (n/y)A]\!]_{x_1=a_1,\ldots,x_n=a_n} = 1$$

Since the denotations of the propositions $t \epsilon c$ and $(t/y)A$ are exactly the same in a valuation where $\phi c = E, \phi x_1 = a_1, \ldots, \phi x_n = a_n$, we deduce that

$$[\![(0 \epsilon c \Rightarrow \forall m\ (m \epsilon c \Rightarrow S(m) \epsilon c) \Rightarrow \forall n\ n \epsilon c)]\!]_{c=E} = 1 \qquad \square$$

Exercise 2.5 Give a formulation of the theory *ZF* with an axiom schema. Show that the theory defined using binary classes is a conservative extension of this theory.

Using the axiom of the power set given in Definition 1.36

$$\forall x \exists z \forall w \ (w \in z \Leftrightarrow (\forall v \ (v \in w \Rightarrow v \in x)))$$

we can show that if A is a set, then there exists a set containing all the subsets of A. However, we do not have a notation (such as $\wp(A)$) for this set.

We could introduce a function symbol $\wp$ and an axiom

$$\forall x \forall w \ (w \in \wp(x) \Leftrightarrow (\forall v \ (v \in w \Rightarrow v \in x)))$$

and show that the theory obtained is a conservative extension of the theory of sets previously defined.

Theorem 2.3 (Skolem) *Let $\mathcal{T}$ be a theory and A a proposition of the form $\forall x_1 \ldots \forall x_n \exists y \ B$, provable in $\mathcal{T}$. Then the theory obtained by adding a function symbol f and the axiom $\forall x_1 \ldots \forall x_n \ (f(x_1, \ldots, x_n)/y)B$ is a conservative extension of $\mathcal{T}$.*

Proof Let $\mathcal{M}$ be a model of $\mathcal{T}$. We show that it can be extended into a model of this axiom. Let $a_1, \ldots, a_n$ be arbitrary elements of $\mathcal{M}$. There exists an element b of $\mathcal{M}$ such that

$$[\![B]\!]_{x_1=a_1,\ldots,x_n=a_n,y=b} = 1$$

Therefore, we can define $\hat{f}$ to be the function that associates to each n-tuple $a_1, \ldots, a_n$ such an element b. □

2.4 Other Applications of the Notion of Model

In this chapter, we have shown that the concept of model can be used to prove several properties of proofs, for example properties of independence, consistency, relative consistency, conservativity. However, in mathematics and in computer science, the concept of model is not just a tool to study proofs: it has multiple applications. We finish the chapter by giving some examples where models and languages are used for various different purposes.

2.4.1 Algebraic Structures

It is not particularly interesting to write proofs in the theory consisting of the equality axioms and the axioms

$$\forall x \forall y \forall z \ ((x + y) + z = x + (y + z))$$

$$\forall x\ (x + 0 = x \wedge 0 + x = x)$$

$$\forall x \exists y\ (x + y = 0 \wedge y + x = 0)$$

However, normal models of this theory are interesting in their own right: they are the groups. We can derive results in group theory by proving properties of the models of this theory. Let us give an example.

Theorem 2.4 (Löwenheim-Skolem) *Let $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$ be a finite or countable language, $\mathcal{T}$ a theory in this language and κ an arbitrary, infinite set. If the theory $\mathcal{T}$ has a finite model, it has a model of the same cardinality as κ.*

Proof This theorem is a simple consequence of the completeness theorem for an arbitrary cardinality.

Consider the language $(\mathcal{S}, \mathcal{F} \uplus \kappa, \mathcal{P} \uplus \{=\})$ obtained by adding to our initial language a symbol $=$ and a constant for each element of κ, and the theory $\mathcal{T}'$ obtained by adding to $\mathcal{T}$ the axioms of equality and the axioms $\neg a = b$ for each pair (a, b) of distinct elements in κ. Let $\mathcal{M}$ be an infinite model of the theory $\mathcal{T}$.

It is not difficult to show that any finite subset of $\mathcal{T}'$ is consistent: a finite subset of $\mathcal{T}'$ will only use a finite number of constants from κ; we can extend the model $\mathcal{M}$, associating to those constants different elements of $\mathcal{M}$ (this is always possible because $\mathcal{M}$ is infinite), and to the other constants in κ an arbitrary element.

We deduce that the theory $\mathcal{T}'$ is consistent. Indeed, assume it is not consistent, then there is a finite subset Γ of $\mathcal{T}'$, such that the sequent $\Gamma \vdash \bot$ is provable. This contradicts our assumption that all finite subsets of $\mathcal{T}'$ are consistent.

Let $\mathcal{M}'$ be the normal model of $\mathcal{T}'$ that we built in the proof of the completeness theorem. This model has at least as many elements as κ because the elements of κ are associated to different elements here. We can then show that since κ is infinite, there are as many closed terms in the language $(\mathcal{S}, \mathcal{F} \uplus \kappa, \mathcal{P} \uplus \{=\})$ as elements in κ and therefore the model has at most the number of elements of κ. It has therefore exactly the same cardinality as κ. $\square$

From this result we can derive the following corollary.

Proposition 2.10 *There are groups of every infinite cardinality. Every infinite set can be endowed with a group structure.*

Note that this theorem does not mention the concept of model. It is a well-known result in group theory, obtained as a corollary of a result in logic.

Another interesting consequence of the theorem of Löwenheim-Skolem is the existence of non-countable normal models of arithmetic, and more generally, of any theory that admits $\mathbb{N}$ as a model. This result might seem surprising, since at first sight all normal models of arithmetic seem to have the same cardinal as $\mathbb{N}$. Indeed, consider a normal model $\mathcal{M}$ of arithmetic, and the function F from $\mathbb{N}$ to $\mathcal{M}$ associating $\hat{S}^n(\hat{0})$ to n.

The image I of this function contains $\hat{0}$, is closed under $\hat{S}$ and $\mathcal{M}$ is a model of the axiom of induction. It seems then that all the elements of $\mathcal{M}$ should be in I, and therefore $\mathcal{M}$ should be countable. Where is the mistake?

The mistake stems from our assumption that if $\mathcal{M}$ is a model of the axiom of induction, every set I containing $\hat{0}$ and closed under $\hat{S}$ must contain all the set $\mathcal{M}$. This is only true if I is in the set $\mathcal{M}_\kappa$. But the comprehension schema requires $\mathcal{M}_\kappa$ to contain all the subsets of $\mathcal{M}$ that are definable by a proposition A, and that is not the case for the set I. In other words, amongst the subsets of $\mathbb{N}$ (and the power set of $\mathbb{N}$ is uncountable), the comprehension schema says that there is a small number—countable—of sets that are definable, and the axiom of induction says that if one of these sets contains 0 and is closed under successor, then it contains all the natural numbers. There is therefore a significant degree of freedom.

Definition 2.12 (Standard model) A *standard* model of the theory of classes is a model such that $\mathcal{M}_\kappa = \wp(\mathcal{M}_\iota)$.

Exercise 2.6 Show that all the standard models of arithmetic have the same cardinal as $\mathbb{N}$.

In the same way we can show that although the fields that are totally ordered, Archimedean and complete are isomorphic to $\mathbb{R}$, there are non standard models of this theory that are countable.

The notion of standard model is essential in the applications of model theory to algebra. However, it is not really useful to study proofs, since the theorem of Löwenheim-Skolem tells us that all the theories that can be defined in a finite or countable language have non-standard models.

2.4.2 Definability

Models can also be used to define the notion of *definable* set, or more generally, definable relation.

Definition 2.13 Let $\mathcal{M}$ be a set and $R_1, \ldots, R_n$ relations over this set. We will say that a relation S over $\mathcal{M}$ is *definable* in the structure $(\mathcal{M}, R_1, \ldots, R_n)$ if there exists a proposition A in the language that consists of the symbols $P_1, \ldots, P_n$ and with free variables $x_1, \ldots, x_p$, such that the elements $a_1, \ldots, a_p$ are in the relation S if and only if

$$[\![A]\!]_{x_1=a_1,\ldots,x_n=a_n} = 1$$

in the model $(\mathcal{M}, R_1, \ldots, R_n)$.

If R_1 and R_2 are two binary relations, their intersection is definable from R_1 and R_2 using the proposition $P_1(x, y) \wedge P_2(x, y)$. In general, if two relations of the same arity are definable, so is their intersection. The set of definable relations is therefore closed under intersection. It is also closed under union and complement. However, the set of definable relations contains more elements than the inductively defined set containing $R_1, \ldots, R_n$ and closed under intersection, union and complement. Indeed, since in a proposition the same variable can be used several times, and variables can be permuted, it is possible to define for instance the set of objects that relate to themselves, $P(x, x)$, or the inverse of a relation, $P(y, x)$. Moreover, the use of quantifiers opens up a wealth of possibilities, since we can, for instance, define the composition of two relations $\exists z\ (P_1(x, z) \wedge P_2(z, y))$.

However, not all relations are definable. We can for instance prove that the reflexive-transitive closure of a relation is not definable using the relation itself.

In database theory, definable relations correspond to definable queries.

Springer
http://www.springer.com/978-0-85729-120-2

Proofs and Algorithms
An Introduction to Logic and Computability
Dowek, G.
2011, XII, 156 p., Softcover
ISBN: 978-0-85729-120-2