A program for the full axiom of choice

Jean-Louis Krivine

Université de Paris - C.N.R.S.

krivine@irif.fr

December 15, 2021

Introduction

The Curry-Howard correspondence enables to associate a program with each proof in classical natural deduction. But mathematical proofs not only use the rules of natural deduction, but also *axioms*, essentially those of Zermelo-Frænkel set theory with axiom of choice. In order to transform these proofs into programs, you must therefore associate with each of these axioms suitable instructions, which is far from obvious.

The theory of *classical realizability (c.r.)* solves this problem for all axioms of ZF, by means of a very rudimentary programming language : the λ_c-calculus, that is to say the λ-calculus with a control instruction [6].

The programs obtained in this way can therefore be written in practically any programming language. They are said to *realize* the axioms of ZF.

But, almost all the applications of mathematics in physics, probability, statistics, etc. use *Analysis*, that is to say *the axiom of dependent choice*. The first program for this axiom, known since 1998 [1], is a pure λ-term called *bar recursion* [20, 2, 21]. In fact, c.r. shows that it provides also a program for the *continuum hypothesis* [17].

Nevertheless, this method requires the programming language to be limited to λ_c-calculus, prohibiting any other instruction, which is a severe restriction.

Classical realizability provides other programs for the axiom of dependent choice [13, 14, 15], which require an additional instruction (clock, signature, ... , or as in this paper, introduction of *fresh variables*). On the other hand, this kind of solution is very flexible regarding the programming language.

There remained, however, the problem of the *full* axiom of choice. It is solved here, by means of new instructions which allow *branching* or *parallelism*[1]. Admittedly, the program obtained in this way is rather complicated and we may hope for new solutions as simple as bar recursion or clock. However, it already shows that we can turn all proofs of ZFC into programs (more precisions about this in the remark at the end of the paper).

Note that *the proof is constructive* i.e. it gives explicitly a program for AC : you "merely" need to formalize this proof itself in natural deduction and apply the proof-program correspondence to the result.

[1] A detailed study of the effect of such instructions on the characteristic Boolean algebra $\gimel 2$ is made in [5].

Outline of the paper.
The framework of this article is the *theory of classical realizability*, which is explained in detail in [13, 14, 15]. For the sake of simplicity, we will often refer to these papers for definitions and standard notations.

Section 1. Axioms and properties of *realizability algebras (r.a.)* which are first order structures, a generalization of both combinatory algebras and ordered sets of forcing conditions. Intuitively, their elements are programs.
Section 2. Each r.a. is associated with a *realizability model (r.m.)*, a generalization of the generic model in the theory of forcing. This model satisfies a set theory ZF_ε which is a conservative extension of ZF, with a strong non extensional membership relation ε.
Section 3. Generic extensions of realizability algebras and models. We explain how a generic extension of a given r.m. can be handled by means of a suitable extension of the corresponding r.a. A little technical because it mixes forcing and realizability.
Section 4. Definition and properties of a particular realizability algebra $\mathfrak{A}_0$. It contains an *instruction of parallelism* and the programming language allows the introduction of many other instructions. This is therefore, in fact, a class of algebras.
Using this r.a., we obtain a program for the *axiom of well ordered choice (WOC) : the product of a family of non-empty sets whose index set is well ordered is non-empty.*
We get, at the same time, a new proof that WOC is weaker than AC (joint work with Laura Fontanella ; cf. [8] for the usual proof).
Section 5. Construction of a generic extension $\mathfrak{A}_1$ of the algebra $\mathfrak{A}_0$ which allows to *realize the axiom of choice : every set can be well ordered.*

Sections 3 and 4 are independent.

Thanks to Asaf Karagila for several fruitful discussions [10]. He observed that, by exactly the same method, we obtain a program, not only for AC, but for every axiom which can be shown compatible with ZFC by forcing (theorem 33) ; for instance CH, $2^{\aleph_0} = \aleph_2$ + Martin's axiom, etc. (but this does not apply to V = L).

1 Realizability algebras (r.a.)

It is a first order structure, which is defined in [14]. We recall here briefly this definition and some essential properties :

A *realizability algebra* $\mathscr{A}$ is made up of three sets : Λ (the set of *terms*), Π (the set of *stacks*), $\Lambda\star\Pi$ (the set of *processes*) with the following operations :
$(\xi,\eta)\mapsto(\xi)\eta$ from Λ^2 into Λ (*application*) ;
$(\xi,\pi)\mapsto\xi\,.\,\pi$ from $\Lambda\times\Pi$ into Π (*push*) ;
$(\xi,\pi)\mapsto\xi\star\pi$ from $\Lambda\times\Pi$ into $\Lambda\star\Pi$ (*process*) ;
$\pi\mapsto\mathsf{k}_\pi$ from Π into Λ (*continuation*).

There are, in Λ, distinguished elements $\mathsf{B},\mathsf{C},\mathsf{I},\mathsf{K},\mathsf{W},\mathsf{cc}$, called *elementary combinators* or *instructions.*

Notation. The term $(\ldots(((\xi)\eta_1)\eta_2)\ldots)\eta_n$ will be also written as $(\xi)\eta_1\eta_2\ldots\eta_n$ or $\xi\eta_1\eta_2\ldots\eta_n$. For instance : $\xi\eta\zeta=(\xi)\eta\zeta=(\xi\eta)\zeta=((\xi)\eta)\zeta$.

We define a preorder on $\Lambda \star \Pi$, denoted by $\succ$, which is called *execution* ;
$\xi \star \pi \succ \xi' \star \pi'$ is read as : *the process* $\xi \star \pi$ *reduces to* $\xi' \star \pi'$.
It is the smallest reflexive and transitive binary relation, such that, for any $\xi, \eta, \zeta \in \Lambda$ and $\pi, \varpi \in \Pi$, we have :

$(\xi)\eta \star \pi \succ \xi \star \eta \centerdot \pi$ (*push*).
$\mathsf{I} \star \xi \centerdot \pi \succ \xi \star \pi$ (*no operation*).
$\mathsf{K} \star \xi \centerdot \eta \centerdot \pi \succ \xi \star \pi$ (*delete*).
$\mathsf{W} \star \xi \centerdot \eta \centerdot \pi \succ \xi \star \eta \centerdot \eta \centerdot \pi$ (*copy*).
$\mathsf{C} \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi \succ \xi \star \zeta \centerdot \eta \centerdot \pi$ (*switch*).
$\mathsf{B} \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi \succ \xi \star (\eta)\zeta \centerdot \pi$ (*apply*).
$\mathsf{cc} \star \xi \centerdot \pi \succ \xi \star \mathsf{k}_\pi \centerdot \pi$ (*save the stack*).
$\mathsf{k}_\pi \star \xi \centerdot \varpi \succ \xi \star \pi$ (*restore the stack*).

We are also given a subset $\perp\!\!\!\perp$ of $\Lambda \star \Pi$, called "the pole", such that :

$$\xi \star \pi \succ \xi' \star \pi',\ \xi' \star \pi' \in \perp\!\!\!\perp \ \Rightarrow\ \xi \star \pi \in \perp\!\!\!\perp.$$

Given two processes $\xi \star \pi, \xi' \star \pi'$, the notation $\xi \star \pi \ggcurly \xi' \star \pi'$ means :

$$\xi \star \pi \notin \perp\!\!\!\perp \Rightarrow \xi' \star \pi' \notin \perp\!\!\!\perp.$$

Therefore, obviously, $\xi \star \pi \succ \xi' \star \pi' \ \Rightarrow\ \xi \star \pi \ggcurly \xi' \star \pi'$.

Finally, we choose a set of terms $\mathsf{PL}_{\mathscr{A}} \subset \Lambda$, containing the elementary combinators : $\mathsf{B}, \mathsf{C}, \mathsf{I}, \mathsf{K}, \mathsf{W}, \mathsf{cc}$ and closed by application. They are called the *proof-like terms of the algebra* $\mathscr{A}$. We write also PL instead of $\mathsf{PL}_{\mathscr{A}}$ if there is no ambiguity about $\mathscr{A}$.

The algebra $\mathscr{A}$ is called *coherent* if, for every proof-like term $\theta \in \mathsf{PL}_{\mathscr{A}}$, there exists a stack π such that $\theta \star \pi \notin \perp\!\!\!\perp$.

Remark. A *set of forcing conditions* can be considered as a degenerate case of realizability algebra, if we present it in the following way : an inf-semi-lattice P, with a greatest element $\mathbf{1}$ and an initial segment $\perp\!\!\!\perp$ of P (the set of *false* conditions). Two conditions $p, q \in P$ are called *compatible* if their g.l.b. $p \wedge q$ is not in $\perp\!\!\!\perp$.
We get a realizability algebra if we set $\Lambda = \Pi = \Lambda \star \Pi = P$; $\mathsf{B} = \mathsf{C} = \mathsf{I} = \mathsf{K} = \mathsf{W} = \mathsf{cc} = \mathbf{1}$ and $\mathsf{PL} = \{\mathbf{1}\}$; $(p)q = p \centerdot q = p \star q = p \wedge q$ and $\mathsf{k}_p = p$. The preorder $p \succ q$ is defined as $p \le q$, i.e. $p \wedge q = p$. The condition of coherence is $\mathbf{1} \notin \perp\!\!\!\perp$.

We can translate λ-terms into terms of Λ built with the combinators $\mathsf{B}, \mathsf{C}, \mathsf{I}, \mathsf{K}, \mathsf{W}$ in such a way that weak head reduction is valid :

$$\lambda x\, t[x] \star u \centerdot \pi \succ t[u/x] \star \pi$$

where $\lambda x\, t[x], u$ are terms and π is a stack.
This is done in [14]. Note that the usual (K,S)-translation does not work.

λ-calculus is much more intuitive than combinatory algebra in order to write programs, so that we use it extensively in the following. But combinatory algebra is better for theory, in particular because it is a first order structure.

2 Realizability models (r.m.)

The framework is very similar to that of forcing, which is anyway a particular case.
We use a first order language with three binary symbols $\not\varepsilon, \notin, \subset$ (ε is intended to be a strong,

non extensional membership relation ; $\in$ and $\subset$ have their usual meaning in ZF).
First order formulas are written with the only logical symbols $\to, \forall, \perp, \top$.
The symbols $\neg, \wedge, \vee, \leftrightarrow, \exists$ are defined with them in the usual way.
Given a realizability algebra, we get a *realizability model (r.m.)* as follows :
We start with a model $\mathscr{M}$ of ZFC (or even ZFL) called the *ground model.* The axioms of ZFL are written with the sublanguage $\{\notin, \subset\}$.
We build a model $\mathscr{N}$ of a new set theory ZF$_\varepsilon$, in the language $\{\not\varepsilon, \notin, \subset\}$, the axioms of which are given in [13]. We recall them below, using the following rather standard abbreviations :
$F_1 \to (F_2 \to \ldots (F_n \to G)\ldots)$ is written $F_1, F_2, \ldots, F_n \to G$ or even $\vec{F} \to G$.
We use the notation $\exists x\{F_1, F_2, \ldots, F_n\}$ for $\forall x(F_1 \to (F_2 \to \cdots \to (F_n \to \perp)\cdots)) \to \perp$.
Of course, $x \,\varepsilon\, y$ and $x \in y$ are the formulas $x \not\varepsilon\, y \to \perp$ and $x \notin y \to \perp$.
The notation $x =_\in y \to F$ means $x \subset y, y \subset x \to F$. Thus $x =_\in y$, which represents the usual (extensional) equality of sets, is the pair of formulas $\{x \subset y, y \subset x\}$.
We use the notations $(\forall x \,\varepsilon\, a)F(x)$ for $\forall x(\neg F(x) \to x \not\varepsilon\, a)$ and
$(\exists x \,\varepsilon\, a)\vec{F}(x)$ for $\neg\forall x(\vec{F}(x) \to x \not\varepsilon\, a)$.
For instance, $(\exists x \,\varepsilon\, y)(t =_\in u)$ is the formula $\neg\forall x(t \subset u, u \subset t \to x \not\varepsilon\, y)$.

The axioms of ZF$_\varepsilon$ are the following :

0. Extensionality axioms.
$\forall x \forall y(x \in y \leftrightarrow (\exists z \,\varepsilon\, y) x =_\in z)$; $\forall x \forall y(x \subset y \leftrightarrow (\forall z \,\varepsilon\, x) z \in y)$.

1. Foundation scheme.
$\forall \vec{a}(\forall x((\forall y \,\varepsilon\, x)F(y, \vec{a}) \to F(x, \vec{a})) \to \forall x\, F(x, \vec{a}))$ for every formula $F(x, a_1, \ldots, a_n)$.

The intuitive meaning of these axioms is that ε is a well founded relation and the relation $\in$ is obtained by " collapsing " ε into an extensional relation.

The following axioms essentially express that the relation ε satisfies the axioms of Zermelo-Fraenkel *except extensionality.*

2. Comprehension scheme.
$\forall \vec{a} \forall x \exists y \forall z(z \,\varepsilon\, y \leftrightarrow (z \,\varepsilon\, x \wedge F(z, \vec{a}))$ for every formula $F(z, \vec{a})$.

3. Pairing axiom.
$\forall a \forall b \exists x\{a \,\varepsilon\, x, b \,\varepsilon\, x\}$.

4. Union axiom.
$\forall a \exists b(\forall x \,\varepsilon\, a)(\forall y \,\varepsilon\, x)\, y \,\varepsilon\, b$.

5. Power set axiom.
$\forall a \exists b \forall x(\exists y \,\varepsilon\, b)\forall z(z \,\varepsilon\, y \leftrightarrow (z \,\varepsilon\, a \wedge z \,\varepsilon\, x))$.

6. Collection scheme.
$\forall \vec{a} \forall x \exists y(\forall u \,\varepsilon\, x)(\exists v\, F(u, v, \vec{a}) \to (\exists v \,\varepsilon\, y)F(u, v, \vec{a}))$ for every formula $F(u, v, \vec{a})$.

7. Infinity scheme.
$\forall \vec{a} \forall x \exists y\{x \,\varepsilon\, y, (\forall u \,\varepsilon\, y)(\exists v\, F(u, v, \vec{a}) \to (\exists v \,\varepsilon\, y)F(u, v, \vec{a}))\}$ for every formula $F(u, v, \vec{a})$.

It is shown in [13] that ZF$_\varepsilon$ is a *conservative extension of ZF.*

For each formula $F(\vec{a})$ of ZF$_\varepsilon$ (i.e. written with $\not\varepsilon, \notin, \subset$) with parameters $\vec{a}$ in the ground model $\mathscr{M}$ we define, in $\mathscr{M}$, a *falsity value* $\|F(\vec{a})\|$ which is a subset of Π and a *truth value* $|F(\vec{a})|$ which is a subset of Λ. The notation $t \Vdash F(\vec{a})$ (read "t realizes $F(\vec{a})$" or "t forces $F(\vec{a})$" in the particular case of forcing) means $t \in |F(\vec{a})|$.

We set first $|F(\vec{a})| = \{t \in \Lambda\,;\ (\forall \pi \in \|F(\vec{a})\|)(t \star \pi \in \perp\!\!\!\perp)\}$ so that we only need to define $\|F(\vec{a})\|$, which we do by induction on F :

1. Definition of $\|a \not\varepsilon\, b\|$:
$\|a \not\varepsilon\, b\| = \{\pi \in \Pi\,;\ (a,\pi) \in b\}\,;\ \|\bot\| = \Pi\,;\ \|\top\| = \emptyset$;

2. Definition of $\|a \subset b\|$ and $\|a \notin b\|$ by induction on $(\mathrm{rk}(a) \cup \mathrm{rk}(b), \mathrm{rk}(a) \cap \mathrm{rk}(b))$:
$\|a \subset b\| = \bigcup_c \{t \,.\, \pi \in \Pi\,;\ t \Vdash c \notin b, (c,\pi) \in a\}$;
$\|a \notin b\| = \bigcup_c \{t \,.\, u \,.\, \pi \in \Pi\,;\ t \Vdash c \subset a, u \Vdash a \subset c, (c,\pi) \in b\}$.

3. Definition of $\|F\|$ for a non atomic formula F, by induction on the length :
$\|F \to F'\| = \{t \,.\, \pi \in \Pi\,;\ t \Vdash F, \pi \in \|F'\|\}$;
$\|\forall x\, F(x)\| = \bigcup_a \|F(a)\|$.

This notion of realizability has two essential properties given by theorems 1 and 2 below. They are proved in [13].

Theorem 1 (Adequacy lemma)**.** $\Vdash$ *is compatible with classical natural deduction, i.e. :*
If $t_1, \ldots, t_n, t$ are λ_c-terms such that $t_1 : F_1, \ldots, t_n : F_n \vdash t : F$ in classical natural deduction, then $t_1 \Vdash F_1, \ldots, t_n \Vdash F_n \Rightarrow t \Vdash F$.
In particular, any valid formula is realized by a proof-like term.

Remark. The proof of theorem 1 uses only item 3 in the above definition of $\|F\|$. In other words, the values of $\|F\|$ for atomic formulas F are arbitrary. This will be used in sections 3 and 5.

Theorem 2. *The axioms of ZF_ε are realized by proof-like terms.*

It follows that *every closed formula which is consequence of ZF_ε and, in particular, every consequence of ZF, is realized by a proof-like term.*
In the following, we shall simply say "the formula F is realized" instead of "realized by a proof-like term" and use the notation $\Vdash F$.

Theorem 2 is valid *for every r.a.* The aim of this paper is to realize the full axiom of choice AC in some particular r.a. *suitable for programming.*
Remark. Note that AC is realized for any r.a. associated with a set of forcing conditions (generic extension of $\mathscr{M}$). But in this case, there is only one proof-like term which is the greatest element **1**.

We define the strong (Leibnitz) equality $a = b$ by $\forall z(a \not\varepsilon\, z \to b \not\varepsilon\, z)$. It is trivially transitive and it is symmetric by comprehension. This equality satisfy the first order axioms of equality $\forall x \forall y(x = y \to (F(x) \to F(y)))$ (by comprehension scheme of ZF_ε) and is therefore the equality in the r.m. $\mathscr{N}$.

Lemma 3. $\|a = b\| = \|\top \to \bot\| = \{\xi \,.\, \pi\,;\ \xi \in \Lambda, \pi \in \Pi\}$ *if $a \neq b$;*
$\|a = a\| = \|\bot \to \bot\| = \{\xi \,.\, \pi\,;\ \xi \in \Lambda, \pi \in \Pi, \xi \star \pi \in \perp\!\!\!\perp\}$.

Let $z = \{b\} \times \Pi$ so that $\|b \not\varepsilon\, z\| = \Pi$. If $a \neq b$ then $\|a \not\varepsilon\, z\| = \emptyset$ and therefore :
$\|a \not\varepsilon\, z \to b \not\varepsilon\, z\| = \|\top \to \bot\|$.
If $a = b$, then $\|a \not\varepsilon\, z\| = \Pi$ and therefore $\|a = b\| = \|\bot \to \bot\|$.
Q.E.D.

Finally, it is convenient to define first $\neq$ by $\|a \neq a\| = \|\bot\| = \Pi$; $\|a \neq b\| = \|\top\| = \emptyset$ if $a \neq b$; and to define $a = b$ as $a \neq b \to \bot$.

We define a preorder $\le$ on the set $\mathscr{P}(\Pi)$ of "falsity values" by setting :
$X \le Y \Leftrightarrow$ there exists a proof-like term $\theta \Vdash X \to Y$. By theorem 1, we easily see [13] that $(\mathscr{P}(\Pi), \le)$ is a Boolean algebra $\mathfrak{B}_{\mathscr{A}}$ *if the r.a.* $\mathscr{A}$ *is coherent.* Every formula $F(\vec{a})$ of ZF_ε with parameters in the ground model $\mathscr{M}$ has a value $\|F(\vec{a})\|$ in this Boolean algebra.
By means of any ultrafilter on $\mathfrak{B}_{\mathscr{A}}$, we thus obtain a complete consistent theory in the language $\{\not\varepsilon, \notin, \subset\}$ with parameters in $\mathscr{M}$. We take any model $\mathscr{N}$ of this theory and call it *the realizability model (r.m.)* of the realizability algebra $\mathscr{A}$.
Therefore, $\mathscr{N}$ is a model of ZF_ε, and in particular, a model of ZF, that we will call $\mathscr{N}_\in$.
Thus $\mathscr{N}_\in$ is simply the model $\mathscr{N}$ restricted to the language $\{\notin, \subset\}$.

Remarks.

The ground model $\mathscr{M}$ is contained in $\mathscr{N}$ since every element of it is a symbol of constant. But $\mathscr{M}$ is not a submodel of $\mathscr{N}$ for the common language $\{\notin, \subset\}$; and, except in the case of forcing, not every element of $\mathscr{N}$ "has a name" in $\mathscr{M}$.
When F is a closed formula of ZF_ε, the two assertions $\mathscr{N} \models F$ and $\Vdash F$ have essentially the same meaning, since $\mathscr{N}$ represents *any r.m.* for the given r.a. But the second formulation requires a formal proof.

Functionals

A *functional relation defined in* $\mathscr{N}$ is given by a formula $F(x, y)$ of ZF_ε such that :
$\mathscr{N} \models \forall x \forall y \forall y'(F(x, y), F(x, y') \to y = y')$.
A *function* is a functional relation which is a set.
We define now some special functional relations on $\mathscr{N}$ which we call *functionals defined in* $\mathscr{M}$ or *functional symbols* :
For each functional relation $f : \mathscr{M}^k \to \mathscr{M}$ defined in the ground model $\mathscr{M}$, we add the functional symbol f to the language of ZF_ε. The application of f to an argument a will be denoted $f[a]$. Therefore f is also defined in $\mathscr{N}$.
We call this (trivial) operation *the extension to* $\mathscr{N}$ *of the functional* f defined in the ground model. It is a fundamental tool in all that follows.
Note the use of brackets for $f[a]$ in this case.

Theorem 4. *Let $t_1, u_1 \dots, t_n, u_n, t, u$ be k-ary terms built with functional symbols, such that :*
$\mathscr{M} \models \forall \vec{x}(t_1[\vec{x}] = u_1[\vec{x}], \dots, t_n[\vec{x}] = u_n[\vec{x}] \to t[\vec{x}] = u[\vec{x}])$.
Then $\lambda x_1 \dots \lambda x_n \lambda x(x_1) \dots (x_n)x \Vdash \forall \vec{x}(t_1[\vec{x}] = u_1[\vec{x}], \dots, t_n[\vec{x}] = u_n[\vec{x}] \to t[\vec{x}] = u[\vec{x}])$.

This easily follows from the definition above of $\|a = b\|$.
Q.E.D.

As a first example let the unary functional $\Phi_F[X]$ be defined in $\mathscr{M}$ by :

$$\Phi_F[X] = \{(x, \xi \centerdot \pi) \,;\, \xi \Vdash F(x), (x, \pi) \in X\}.$$

We shall denote it by $\{x \,\varepsilon\, X \,;\, F(x)\}$ (in this notation, x is a bound variable) because it corresponds to the comprehension scheme in the model $\mathscr{N}$. Note that the use of ε reminds that this expression must be interpreted in $\mathscr{N}$.

We define now in $\mathscr{M}$ the unary functional $\daleth X = X \times \Pi$, so that we have :
$\|x \not\varepsilon \daleth X\| = \Pi$ if $x \in X$ and $\|x \not\varepsilon \daleth X\| = \emptyset$ if $x \notin X$.
For any X in $\mathscr{M}$, we define the quantifier $\forall x^{\daleth X}$ by setting $\|\forall x^{\daleth X} F(x)\| = \bigcup_{x \in X} \|F(x)\|$.

Lemma 5. $\Vdash \forall x^{\gimel X} F(x) \leftrightarrow \forall x(x \,\varepsilon\, \gimel X \to F(x))$.

In fact, we have $\|\forall x(\neg F(x) \to x \not\varepsilon\, \gimel X)\| = \|\forall x^{\gimel X} \neg\neg F(x)\|$.
Now we have trivially $\lambda x(x)\mathsf{I} \Vdash \forall x^{\gimel X} F(x) \to \forall x^{\gimel X} \neg\neg F(x)$
and $\mathsf{cc} \Vdash \forall x^{\gimel X} \neg\neg F(x) \to \forall x^{\gimel X} F(x)$.

Q.E.D.

Lemma 6. *Let f be a functional k-ary symbol defined in $\mathcal{M}$ such that $f : X_1 \times \cdots \times X_k \to X$. Then its extension to $\mathcal{N}$ is such that $f : \gimel X_1 \times \cdots \times \gimel X_k \to \gimel X$.*

Trivial.

Q.E.D.

By theorem 4 and lemma 6, the algebra operations on the Boolean algebra $2 = \{0, 1\}$ extended to $\gimel 2$, turn it into a Boolean algebra which we call *the characteristic Boolean algebra* of the r.m. $\mathcal{N}$. In the ground model $\mathcal{M}$, we define the functional $(a, x) \mapsto ax$ from $2 \times \mathcal{M}$ into $\mathcal{M}$ by $0x = \emptyset$ and $1x = x$. It extends to $\mathcal{N}$ into a functional $\gimel 2 \times \mathcal{N} \to \mathcal{N}$ such that $(ab)x = a(bx)$ for $a, b \,\varepsilon\, \gimel 2$ and every x in $\mathcal{N}$.

Lemma 7.
$\mathsf{I} \Vdash \forall \vec{x} \forall \vec{y} \forall a^{\gimel 2}(af[\vec{x}, \vec{y}] = af[a\vec{x}, \vec{y}])$ for every functional symbol f defined in $\mathcal{M}$.

Immediate since $\xi \Vdash \forall a^{\gimel 2} F(a)$ means $(\xi \Vdash F(0)) \wedge (\xi \Vdash F(1))$.

Q.E.D.

For any formula $F(\vec{x})$ of ZF we define, in $\mathcal{M}$, a functional $\langle F(\vec{x})\rangle$ with value in $\{0, 1\}$ which is the truth value of this formula in $\mathcal{M}$.[2] The extension of this functional to the model $\mathcal{N}$ takes its values in the Boolean algebra $\gimel 2$ (cf. [16]).
The binary functionals $\langle x \notin y\rangle$ and $\langle x \subset y\rangle$ define on the r.m. $\mathcal{N}$ a structure of *Boolean model* on the Boolean algebra $\gimel 2$, that we denote by $\mathcal{M}_{\gimel 2}$. It is an elementary extension of $\mathcal{M}$ since the truth value of every closed formula of ZF with parameters in $\mathcal{M}$ is the same in $\mathcal{M}$ and $\mathcal{M}_{\gimel 2}$.
Any ultrafilter $\mathcal{U}$ on $\gimel 2$ would therefore give a (two-valued) model $\mathcal{M}_{\gimel 2}/\mathcal{U}$ which is an elementary extension of $\mathcal{M}$. In [16], it is shown that there exists one and only one ultrafilter $\mathcal{D}$ on $\gimel 2$ such that the model $\mathcal{M}_{\gimel 2}/\mathcal{D}$, which we shall denote as $\mathcal{M}_{\mathcal{D}}$, is well founded (in $\mathcal{N}$). The binary relations $\notin, \subset$ of $\mathcal{M}_{\mathcal{D}}$ are thus defined by $\langle x \notin y\rangle \,\varepsilon\, \mathcal{D}$ and $\langle x \subset y\rangle \,\varepsilon\, \mathcal{D}$.
Moreover, $\mathcal{M}_{\mathcal{D}}$ is isomorphic with a transitive submodel of $\mathcal{N}_{\in}$ with the same ordinals. In fact, if we start with a ground model $\mathcal{M}$ which satisfies V = L, then $\mathcal{M}_{\mathcal{D}}$ is isomorphic with the constructible class of $\mathcal{N}_{\in}$.
Remark. We have defined *four first order structures* on the model $\mathcal{N}$:

- The realizability model $\mathcal{N}$ itself uses the language $\{\not\varepsilon, \notin, \subset\}$ of ZF_ε ; the equality on $\mathcal{N}$ is the Leibnitz equality $=$, which is the strongest possible.
- The model $\mathcal{N}_{\in}$ of ZF is restricted to the language $\{\notin, \subset\}$; the equality on $\mathcal{N}_{\in}$ is the extensional equality $=_{\in}$.
- The Boolean model $\mathcal{M}_{\gimel 2}$ with the language $\{\notin, \subset\}$ of ZF and with truth values in $\gimel 2$; it is an elementary extension of the ground model $\mathcal{M}$. The equality on $\mathcal{M}_{\gimel 2}$ is $\langle x = y\rangle = 1$ which is the same as Leibnitz equality.

[2]The formal definition in ZF is : $\forall \vec{x}((F(\vec{x}) \to \langle F(\vec{x})\rangle = 1) \wedge (\neg F(\vec{x}) \to \langle F(\vec{x})\rangle = 0))$.

• The model $\mathcal{M}_{\mathscr{D}}$ with the same language, also an elementary extension of $\mathcal{M}$; if $F(\vec{a})$ is a closed formula of ZF with parameters (in $\mathcal{N}$), then $\mathcal{M}_{\mathscr{D}} \models F(\vec{a})$ iff $\mathcal{N} \models \langle F(\vec{a})\rangle \,\varepsilon\, \mathscr{D}$.
The equality on $\mathcal{M}_{\mathscr{D}}$ is given by $\langle x = y\rangle \,\varepsilon\, \mathscr{D}$.

The proof of existence of the ultrafilter $\mathscr{D}$ in [16] is not so simple. But it is useless in the present paper, because $\beth 2$ will be the four elements algebra, with two atoms a_0, a_1 which give the two trivial ultrafilters on $\beth 2$. It is easily seen (lemma 23) that one of them, say a_0 gives a well founded model denoted by $\mathcal{M}_{a_0}$ which is the class $a_0\mathcal{N} = \mathcal{M}_{\mathscr{D}}$. The class $\mathcal{M}_{a_1} = a_1\mathcal{N}$ is also an elementary extension of $\mathcal{M}$ (but not well founded, cf. the remark after lemma 29). Finally we have $\mathcal{M}_{\beth 2} = \mathcal{N} = a_0\mathcal{N} \times a_1\mathcal{N}$ since the Boolean model $\mathcal{M}_{\beth 2}$ is simply a product in this case, and equality is the same on $\mathcal{M}_{\beth 2}$ and $\mathcal{N}$, as remarked previously.

Integers

We define, in the ground model $\mathcal{M}$, the functional $x \mapsto x^+ = x \cup \{x\}$ and extend it to the r.m. $\mathcal{N}$. It is injective in $\mathcal{M}$ and therefore also in $\mathcal{N}$.
For each $n \in \mathbb{N}$, we define $\underline{n} \in \mathsf{PL}$ by induction : $\underline{0} = \lambda x \lambda y\, y = \mathsf{KI}$; $\underline{n^+} = s\underline{n}$
where $s = \lambda n \lambda f \lambda x (nf)(f)x = (\mathsf{BW})(\mathsf{B})\mathsf{B}$ (and n^+ is $n+1$).
We define $\widetilde{\mathbb{N}} = \{(n, \underline{n}\bullet\pi)\,;\ n \in \mathbb{N}, \pi \in \Pi\}$. We can use it as the set of integers of the model $\mathcal{N}$ as shown by the following theorem 8.
We define the quantifier $\forall n^{\mathrm{int}}$ by setting $\|\forall n^{\mathrm{int}} F(n)\| = \{\underline{n}\bullet\pi\,;\ n \in \mathbb{N}, \pi \in \|F(n)\|\}$.

Theorem 8. *For every formula $F(x)$ of ZF_ε, the following formulas are realized :*
i) $0 \,\varepsilon\, \widetilde{\mathbb{N}}$; $\forall n(n \,\varepsilon\, \widetilde{\mathbb{N}} \to n^+ \,\varepsilon\, \widetilde{\mathbb{N}})$;
ii) $F(0), \forall n(F(n) \to F(n^+)) \to (\forall n \,\varepsilon\, \widetilde{\mathbb{N}})F(n)$;
iii) $\forall n^{int} F(n) \leftrightarrow (\forall n \,\varepsilon\, \widetilde{\mathbb{N}})F(n)$.

i) Let $\xi \Vdash 0 \not\varepsilon\, \widetilde{\mathbb{N}}$; then $\xi \star \underline{0}\bullet\pi \in \perp\!\!\!\perp$ for all $\pi \in \Pi$. Therefore $\lambda x(x)\underline{0} \Vdash 0 \not\varepsilon\, \widetilde{\mathbb{N}} \to \perp$.
Let $\xi \Vdash n^+ \not\varepsilon\, \widetilde{\mathbb{N}}$ and $\underline{n}\bullet\pi \in \|n \not\varepsilon\, \widetilde{\mathbb{N}}\|$. We have $\xi \star s\underline{n}\bullet\pi \in \perp\!\!\!\perp$ and therefore $\theta \star \xi\bullet\underline{n}\bullet\pi \in \perp\!\!\!\perp$ with $\theta = \lambda x \lambda n(x)(s)n$. Thus $\theta \Vdash \forall n(n^+ \not\varepsilon\, \widetilde{\mathbb{N}} \to n \not\varepsilon\, \widetilde{\mathbb{N}})$.

ii) We show $\lambda x \lambda y \lambda z \lambda n(x)(n)yz \Vdash \neg F(0), \forall n(F(n^+) \to F(n)) \to \forall m(F(m) \to m \not\varepsilon\, \widetilde{\mathbb{N}})$.
Let $\xi \Vdash \neg F(0), \eta \Vdash \forall n(F(n^+) \to F(n)), \zeta \Vdash F(m)$ and $\underline{m}\bullet\pi \in \|m \not\varepsilon\, \widetilde{\mathbb{N}}\|$.
Let us show that $\underline{m}\eta\zeta \Vdash F(0)$ by induction on m :
This is clear if $m = 0$. Now, $\underline{m^+}\eta\zeta = s\underline{m}\eta\zeta \succ (\underline{m}\eta)(\eta)\zeta$ and $\eta\zeta \Vdash F(m)$ since $\zeta \Vdash F(m^+)$.
Therefore $(\underline{m}\eta)(\eta)\zeta \Vdash F(0)$ by the induction hypothesis.
It follows that $(\xi)(\underline{m})\eta\zeta \Vdash \perp$, hence the result.

iii) Let us use lemma 9. We have :
$\|\forall n(\urcorner F(n) \to n \not\varepsilon\, \widetilde{\mathbb{N}})\| = \{\mathsf{k}_\pi\bullet\underline{n}\bullet\varpi\,;\ n \in \mathbb{N}, \pi \in \|F(n)\|, \varpi \in \Pi\}$
and by definition : $\|\forall n^{\mathrm{int}} F(n)\| = \{\underline{n}\bullet\pi\,;\ n \in \mathbb{N}, \pi \in \|F(n)\|\}$.
It follows easily that :
$\lambda x \lambda n(\mathsf{cc})\lambda k(x)kn \Vdash \forall n(\urcorner F(n) \to n \not\varepsilon\, \widetilde{\mathbb{N}}) \to \forall n^{\mathrm{int}} F(n)$
$\lambda x \lambda k \lambda n(k)(x)n \Vdash \forall n^{\mathrm{int}} F(n) \to \forall n(\urcorner F(n) \to n \not\varepsilon\, \widetilde{\mathbb{N}})$.
Q.E.D.

Some useful notations

For every set of terms $X \subset \Lambda$ and every closed formula F we can define an "extended formula" $X \to F$ by setting $\|X \to F\| = \{\xi\bullet\pi\,;\ \xi \in X, \pi \in \|F\|\}$.

For instance, for every formula F, we define $\urcorner F = \{\mathsf{k}_\pi \,;\, \pi \in \|F\|\}$. It is a useful equivalent of $\neg F$ by the following :

Lemma 9. $\Vdash \urcorner F \leftrightarrow \neg F$.

If $\pi \in \|F\|$, then $\mathsf{k}_\pi \Vdash \neg F$ and therefore $\mathsf{I} \Vdash \urcorner F \to \neg F$.
Conversely, if $\xi \Vdash \urcorner F \to \bot$, then $\xi \star \mathsf{k}_\pi . \pi \in \perp\!\!\!\perp$ for every $\pi \in \|F\|$, therefore $\mathsf{cc} \Vdash \neg\urcorner F \to F$.

Q.E.D.

If t, u are terms of the language of ZF, built with functionals in $\mathscr{M}$, we define another "extended formula" $t = u \hookrightarrow F$ by setting :

$$\|t = u \hookrightarrow F\| = \emptyset \text{ if } t \neq u \,;\, \|t = u \hookrightarrow F\| = \|F\| \text{ if } t = u.$$

We write $(t_1 = u_1), \ldots, (t_n = u_n) \hookrightarrow F$ for $(t_1 = u_1) \hookrightarrow (\cdots \hookrightarrow ((t_n = u_n) \hookrightarrow F)\cdots)$.

Lemma 10. $\Vdash ((t = u \hookrightarrow F) \leftrightarrow (t = u \to F))$.

We have immediately $\mathsf{I} \Vdash \neg F, (t = u \hookrightarrow F) \to t \neq u$.
Conversely $\lambda x(x)\mathsf{I} \Vdash (t = u \to F) \to (t = u \hookrightarrow F)$.

Q.E.D.

For instance, the conclusion of theorem 4 may be rewritten as :
$\mathsf{I} \Vdash \forall \vec{x}(t_1[\vec{x}] = u_1[\vec{x}], \ldots, t_n[\vec{x}] = u_n[\vec{x}] \hookrightarrow t[\vec{x}] = u[\vec{x}])$.

Lemmas 11, 12, 13 and theorem 15 below will be used in the following sections.

Lemma 11. $\Vdash \forall x \forall y (x \,\varepsilon\, y \to \langle x \in \mathrm{Cl}[y]\rangle = 1)$.

In the model $\mathscr{M}$, the unary functional symbol Cl denotes the *transitive closure.*
We show $\mathsf{I} \Vdash \forall x \forall y (\langle x \in \mathrm{Cl}[y]\rangle \neq 1 \to x \not\varepsilon\, y)$: let $\xi \Vdash \langle x \in \mathrm{Cl}[y]\rangle \neq 1$ and $\pi \in \|x \not\varepsilon\, y\|$.
Then $(x, \pi) \in y$, therefore $x \in \mathrm{Cl}(y)$. It follows that $\xi \Vdash \bot$.

Q.E.D.

Lemma 12. *$\mathsf{I} \Vdash \forall X \forall a^{\daleth 2} \forall x(\langle ax \in aX\rangle \geq a \hookrightarrow ax \,\varepsilon\, \Phi[X])$ where Φ is the functional symbol defined in $\mathscr{M}$ by $\Phi[X] = (X \cup \{0\}) \times \Pi$ i.e. $\daleth(X \cup \{0\})$.*

Remark. The notation $b \geq a$ for $a, b \,\varepsilon\, \daleth 2$ means, of course, $ab = a$.

This amounts to show :
1. $x \in X \Rightarrow \mathsf{I} \Vdash x \not\varepsilon\, \Phi[X] \to \bot$;
2. $\mathsf{I} \Vdash 0 \not\varepsilon\, \Phi[X] \to \bot$.

Both are trivial.

Q.E.D.

Lemma 13. *Let $F(x, \vec{y})$ be a formula in ZF$_\varepsilon$. Then :*

$$\mathsf{I} \Vdash \forall \vec{y}(\forall \varpi^{\daleth \Pi} F(f[\varpi, \vec{y}], \vec{y}) \to \forall x F(x, \vec{y}))$$

for some functional symbol f defined in $\mathscr{M}$.

Let $\vec{a} = (a_1, \ldots, a_k)$ in $\mathscr{M}$. Then, we have :
$\pi \in \|\forall x F(x, \vec{a})\| \Leftrightarrow \mathscr{M} \models \exists x(\pi \in \|F(x, \vec{a})\|) \Leftrightarrow \mathscr{M} \models \pi \in \|F(f[\pi, \vec{a}], \vec{a})\|$
where f is a functional defined in $\mathscr{M}$, (choice principle in $\mathscr{M}$).
Thus we have $\|\forall x F(x, \vec{a})\| \subset \bigcup_{\varpi \in \Pi} \|F(f[\varpi, \vec{a}], \vec{a})\|$ hence the result.

Q.E.D.

Lemma 14.
If $X \in \mathscr{M}$ is transitive, then $\beth X$ is ε-transitive, i.e. $I \Vdash \forall x^{\beth X} \forall y (y \not\varepsilon \beth X \to y \not\varepsilon x)$.

Let $x \in X$, $\varpi \in \|y \not\varepsilon x\|$, i.e. $(y, \varpi) \in x$ and $\xi \in \mathbf{\Lambda}$ such that $\xi \Vdash y \not\varepsilon \beth X$. Since X is transitive, we have $y \in X$ and therefore $\xi \Vdash \perp$.

Q.E.D.

Theorem 15. *Let $\mathfrak{L}$ be the language $\{\varepsilon, \in, \subset\}$ of ZF_ε, with a symbol for each functional definable in $\mathscr{M}$. Then, there exists an ε-transitive $\mathfrak{L}$-elementary substructure $\widetilde{\mathscr{N}}$ of $\mathscr{N}$ such that, for all a in $\widetilde{\mathscr{N}}$, there is an ordinal α of $\mathscr{M}$ such that $\widetilde{\mathscr{N}} \models a \,\varepsilon\, \beth V_\alpha$.*

$\widetilde{\mathscr{N}}$ is made up of the elements a of $\mathscr{N}$ such that $a \,\varepsilon\, \beth V_\alpha$ for some ordinal α of $\mathscr{M}$ (note that it is not a class defined in $\mathscr{N}$). By lemma 14, each $\beth V_\alpha$ is ε-transitive and therefore $\widetilde{\mathscr{N}}$ is also.

Let $F(x, \vec{y})$ be a formula of $\mathfrak{L}$ and $\vec{b} = (b_1, \ldots, b_k)$ be in $\widetilde{\mathscr{N}}$. We assume $\widetilde{\mathscr{N}} \models \forall x\, F(x, \vec{b})$ and we have to show that $\mathscr{N} \models \forall x\, F(x, \vec{b})$ which we do by induction on F. By lemma 13, it suffices to show that $\mathscr{N} \models \forall \varpi^{\beth\Pi} F(f[\varpi, \vec{b}], \vec{b})$. Thus let $\pi \,\varepsilon\, \beth\Pi$; by definition of $\widetilde{\mathscr{N}}$, there exists X in $\mathscr{M}$ such that $\vec{b} \,\varepsilon\, \beth X$. Now, there exists α in $\mathscr{M}$ such that $f : \Pi \times X \to V_\alpha$ and therefore, in $\mathscr{N}$, we have $f : \beth\Pi \times \beth X \to \beth V_\alpha$. It follows that $f[\pi, \vec{b}] \,\varepsilon\, \beth V_\alpha$ and therefore $f[\pi, \vec{b}]$ is in $\widetilde{\mathscr{N}}$.
Thus $\widetilde{\mathscr{N}} \models F(f[\pi, \vec{b}], \vec{b})$, hence $\mathscr{N} \models F(f[\pi, \vec{b}], \vec{b})$ by the induction hypothesis.

Q.E.D.

Replacing $\mathscr{N}$ by this elementary substructure, we shall suppose from now on :

① *For all a in $\mathscr{N}$, there is an ordinal α of $\mathscr{M}$ such that $\mathscr{N} \models a \,\varepsilon\, \beth V_\alpha$.*

Theorem 16 below is not really useful in the following, but it gives a welcome information on the (very complex) structure of the r.m. $\mathscr{N}$.

Theorem 16. *$a\mathscr{N}$ is a proper class for all $a \,\varepsilon\, \beth 2$, $a \neq 0$; i.e. $I \Vdash \forall x (\forall a^{\beth 2} (\forall y (a y \,\varepsilon\, x) \to a = 0))$.*

Let us show, in fact, that $\mathsf{I} \Vdash \forall x (\forall a^{\beth 2} (a x \,\varepsilon\, x \to a = 0))$; in other words :
$\mathsf{I} \Vdash 0 \,\varepsilon\, x \to 0 = 0$ and $\mathsf{I} \Vdash x \,\varepsilon\, x \to 1 = 0$.
We have $(0 \,\varepsilon\, x) \equiv (0 \not\varepsilon x \to \perp)$ and $(0 = 0) \equiv (\perp \to \perp)$ hence the first result.
Furthermore, we have $\|x \not\varepsilon x\| = \{\pi \in \Pi\, ;\, (x, \pi) \in x\} = \emptyset$; thus $\|x \,\varepsilon\, x\| = \|x \not\varepsilon x \to \perp\| = \|\top \to \perp\|$ and $\|1 = 0\| = \|\top \to \perp\|$ hence the second result.

Q.E.D.

3 Extensional generic extensions

In this section we build some tools in order to manage generic extensions $\mathscr{N}_\in[G]$ of the *extensional* model $\mathscr{N}_\in$. We define a new r.a. and give, in this r.a., a new way to compute the truth value of ZF-formulas in $\mathscr{N}_\in[G]$.

Let $\mathbf{V}$ be fixed in $\mathscr{M}$. We have $\|x \not\varepsilon \beth\mathbf{V}\| = \|\langle x \in \mathbf{V}\rangle \neq 1\|$ and therefore :

$$\mathsf{I} \Vdash \forall x (x \,\varepsilon\, \beth\mathbf{V} \leftrightarrow \langle x \in \mathbf{V}\rangle = 1).$$

In other words, a set x strongly belongs to $\beth\mathbf{V}$ iff the Boolean ZF-model $\mathscr{M}_{\beth 2}$ says that " x belongs always to $\mathbf{V}$ ".
Remember also the important (and obvious) equivalence $\mathsf{I} \Vdash \forall x \forall y (x = y \leftrightarrow \langle x = y\rangle = 1)$ which follows from $\|x \neq y\| = \|\langle x = y\rangle \neq 1\|$ and *identifies the r.m. $\mathscr{N}$ with the Boolean model $\mathscr{M}_{\beth 2}$.*

Theorem 17. $\mathscr{N} \models \forall a \forall n^{int}\Big(a\,\varepsilon\,(\beth\mathbf{V})^n \to \exists! b^{\beth(\mathbf{V}^n)} \forall i^{int}(i < n \to a(i) = b[i])\Big).$
In other words, each finite sequence of $\beth\mathbf{V}$ *in* $\mathscr{N}$ *is represented by a unique finite sequence of* $\mathbf{V}$ *in the Boolean model* $\mathscr{M}_{\beth 2}$.

Unicity. Note first that, since there is no extensionality in $\mathscr{N}$, you may have two sequences $a \neq a'\,\varepsilon\,(\beth\mathbf{V})^n$ such that $a(i) = a'(i)$ for $i < n$. Now suppose $b, b'\,\varepsilon\,\beth(\mathbf{V}^n)$ be such that $b[i] = b'[i]$ for $i < n$. Then, we have $\langle b, b' \in \mathbf{V}^n\rangle = 1$ and $\langle(\forall i < n)(b[i] = b'[i])\rangle = 1$. Since the Boolean model $\mathscr{M}_{\beth 2}$ satisfies extensionality, we get $\langle b = b'\rangle = 1$ that is $b = b'$.

Existence. Proof by induction on n. This is trivial if $n = 0$: take $b = \emptyset$.
Now, let $a\,\varepsilon\,(\beth\mathbf{V})^{n+1}$ and a' be a restriction of a to n. Let $b'\,\varepsilon\,\beth(\mathbf{V}^n)$ such that $a'(i) = b'[i]$ for $i < n$ (induction hypothesis).
In the ground model $\mathscr{M}$, we define the binary functional $+$ as follows :
if u is a finite sequence $(u_0, \ldots, u_{n-1})$, then $u + v$ is the sequence $(u_0, \ldots, u_{n-1}, v)$.
We extend it to $\mathscr{N}$ and we set $b = b' + a(n)$ i.e. $\langle b = b' + a(n)\rangle = 1$. Therefore $\langle b[i] = b'[i]\rangle = 1$ for $i < n$ and $\langle b[n] = a(n)\rangle = 1$, i.e. $a(i) = b[i]$ for $i < n$ and $a(n) = b[n]$.

Q.E.D.

Consider an arbitrary ordered set $(C, \leq)$ in the model $\mathscr{N}$. By theorem 15 and property ① (section 2), we may suppose that $(C, \leq)\,\varepsilon\,\beth\mathbf{V}$ with $\mathbf{V} = V_\alpha$ in $\mathscr{M}$. $\beth\mathbf{V}$ is ε-transitive, by lemma 14.
As a set of forcing conditions, C is equivalent to the set $\mathfrak{C}$ of finite subsets X of $\beth\mathbf{V}$ such that $X \cap C$ has a lower bound in C, $\mathfrak{C}$ being ordered by inclusion.
Thus, we can define $\mathfrak{C}$ by the following formula of ZF_ε :

$$\mathfrak{C}(u) \equiv u\,\varepsilon\,(\beth\mathbf{V})^{<\omega} \wedge (Im(u) \cap C) \textit{ has a lower bound in } C$$

where $\mathrm{Im}(u) \subseteq \beth\mathbf{V}$ is the (finite) image of the finite sequence u.
We have $\mathscr{N} \models \mathfrak{C}(u) \to u\,\varepsilon\,(\beth\mathbf{V})^{<\omega}$ and therefore $\mathscr{N} \models \mathfrak{C}(u) \to u\,\varepsilon\,(\beth\mathbf{V}^{<\omega})$ by theorem 17.
Moreover, we have $\mathscr{N} \models \mathfrak{C}(\emptyset)$.

In $\mathscr{M}$, the function $(u, v) \mapsto uv$, from $(\mathbf{V}^{<\omega})^2$ into $\mathbf{V}^{<\omega}$, which is the concatenation of sequences, is associative with $\emptyset$ as neutral element, also denoted by $\mathbf{1}$ (monoïd).
This function extends to $\mathscr{N}$ into an application of $\beth(\mathbf{V}^{<\omega})^2$ into $\beth(\mathbf{V}^{<\omega})$ with the same properties. Thus, we write uvw for $u(vw), (uv)w$, etc.
The formula $\mathfrak{C}(uv)$ of ZF_ε means that u, v are two compatible finite sequences of elements of C, i.e. the union of their images has a lower bound in C. Thus $\mathfrak{C}$ becomes a set of forcing conditions equivalent to C by means of this compatibility relation.
This formula has the following properties :

$$\Vdash \mathfrak{C}(puvq) \to \mathfrak{C}(pvuq),\ \Vdash \mathfrak{C}(puvq) \to \mathfrak{C}(puq),\ \Vdash \mathfrak{C}(puq) \to \mathfrak{C}(puuq).$$

It will be convenient to have only one formula and to use simply the following consequence :

② *There exists a proof-like term* $\mathfrak{c}$ *such that* $\mathfrak{c} \Vdash \mathfrak{C}(pqrtuvw) \to \mathfrak{C}(ptruuv)$.

Consider now, in the ground model $\mathscr{M}$, a r.a. $\mathscr{A}_0$ which gives the r.m. $\mathscr{N}$.
We suppose to have an operation $(\pi, \tau) \mapsto \pi^\tau$ from $\Pi \times \Lambda$ into Π such that :

$$(\xi \cdot \pi)^\tau = \xi \cdot \pi^\tau \text{ for every } \xi, \tau \in \Lambda \text{ and } \pi \in \Pi.$$

and two new combinators χ *(read)* and χ' *(write)* such that :

$$\chi \star \xi \cdot \pi^\tau \succ \xi \star \tau \cdot \pi \text{ (i.e. } \xi \star \tau \cdot \pi \in \perp\!\!\!\perp \Rightarrow \chi \star \xi \cdot \pi^\tau \in \perp\!\!\!\perp)$$
$$\chi' \star \tau \cdot \xi \cdot \pi \succ \xi \star \pi^\tau \text{ (i.e. } \xi \star \pi^\tau \in \perp\!\!\!\perp \Rightarrow \chi' \star \tau \cdot \xi \cdot \pi \in \perp\!\!\!\perp).$$

Moreover, we suppose that χ, χ' may be used to form proof-like terms.
Intuitively, π^τ is obtained by putting the term τ *at the end* of the stack π, in the same way that $\tau \cdot \pi$ is obtained by putting τ *at the top* of π.

We define now, in the ground model $\mathscr{M}$, a new r.a. $\mathscr{A}_1$; its r.m. will be called *the extension of $\mathscr{N}$ by a $\mathfrak{C}$-generic (or a C-generic).*

We define the terms $\mathsf{B}^*, \mathsf{C}^*, \mathsf{I}^*, \mathsf{K}^*, \mathsf{W}^*, \mathsf{cc}^*$ and k_π^* by the conditions :

$\mathsf{B}^* = \mathsf{B}$; $\mathsf{I}^* = \mathsf{I}$;
$\mathsf{C}^* \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi^\tau \succ \xi \star \zeta \centerdot \eta \centerdot \pi^{\mathfrak{c}\tau}$; i.e. $\mathsf{C}^* = \lambda x \lambda y \lambda z(\chi)\lambda t((\chi')(\mathfrak{c})t)xzy$;
$\mathsf{K}^* \star \xi \centerdot \eta \centerdot \pi^\tau \succ \xi \star \pi^{\mathfrak{c}\tau}$; i.e. $\mathsf{K}^* = \lambda x \lambda y(\chi)\lambda t((\chi')(\mathfrak{c})t)x$;
③ $\mathsf{W}^* \star \xi \centerdot \eta \centerdot \pi^\tau \succ \xi \star \eta \centerdot \eta \centerdot \pi^{\mathfrak{c}\tau}$; i.e. $\mathsf{W}^* = \lambda x \lambda y(\chi)\lambda t((\chi')(\mathfrak{c})t)xyy$;
$\mathsf{k}_\pi^* \star \xi \centerdot \varpi^\tau \succ \xi \star \pi^{\mathfrak{c}\tau}$; i.e. $\mathsf{k}_\pi^* = \lambda x(\chi)\lambda t(\mathsf{k}_\pi)((\chi')(\mathfrak{c})t)x$;
$\mathsf{cc}^* \star \xi \centerdot \pi^\tau \succ \xi \star \mathsf{k}_\pi^* \centerdot \pi^{\mathfrak{c}\tau}$; i.e.
$\mathsf{cc}^* = \lambda x(\chi)\lambda t(\mathsf{cc})\lambda k(((\chi')(\mathfrak{c})t)x)\lambda x'(\chi)\lambda t'(k)((\chi')(\mathfrak{c})t')x'$.

When checking below the axioms of r.a., the property needed for each combinator is :

for C^* : $\mathfrak{c} \Vdash \mathfrak{C}(prtv) \to \mathfrak{C}(ptrv)$; for K^* : $\mathfrak{c} \Vdash \mathfrak{C}(pqr) \to \mathfrak{C}(pr)$;
④ for W^* : $\mathfrak{c} \Vdash \mathfrak{C}(puv) \to \mathfrak{C}(puuv)$; for cc^* : $\mathfrak{c} \Vdash \mathfrak{C}(pu) \to \mathfrak{C}(puu)$;
for k_π^* : $\mathfrak{c} \Vdash \mathfrak{C}(rtw) \to \mathfrak{C}(tr)$.

We get them replacing by $\mathbf{1}$ some of the variables p, q, r, t, u, v, w in the definition ② of $\mathfrak{c}$.

We define the r.a. $\mathscr{A}_1$ by setting $\boldsymbol{\Lambda} = \Lambda \times \mathbf{V}^{<\omega}$; $\boldsymbol{\Pi} = \Pi \times \mathbf{V}^{<\omega}$; $\boldsymbol{\Lambda} \star \boldsymbol{\Pi} = (\Lambda \star \Pi) \times \mathbf{V}^{<\omega}$.
$(\xi, u) \centerdot (\pi, v) = (\xi \centerdot \pi, uv)$;
$(\xi, u) \star (\pi, v) = (\xi \star \pi, uv)$;
$(\xi, u)(\eta, v) = (\xi\eta, uv)$.

The pole $\perp\!\!\!\perp$ of $\mathscr{A}_1$ is defined by :

$$(\xi \star \pi, u) \in \perp\!\!\!\perp \Leftrightarrow (\forall \tau \in \Lambda)(\tau \Vdash \mathfrak{C}(u) \Rightarrow \xi \star \pi^\tau \in \perp\!\!\!\perp).$$

The combinators are :
$\mathbf{B} = (\mathsf{B}, \mathbf{1}), \mathbf{C} = (\mathsf{C}^*, \mathbf{1}), \mathbf{I} = (\mathsf{I}, \mathbf{1}), \mathbf{K} = (\mathsf{K}^*, \mathbf{1}), \mathbf{W} = (\mathsf{W}^*, \mathbf{1}), \mathbf{cc} = (\mathsf{cc}^*, \mathbf{1})$ and $\mathbf{k}_{(\pi,u)} = (\mathsf{k}_\pi^*, u)$.
$\mathsf{PL}_{\mathscr{A}_1}$ is $\{(\theta, \mathbf{1})\ ;\ \theta \in \mathsf{PL}_{\mathscr{A}_0}\}$.

Theorem 18. *$\mathscr{A}_1$ is a coherent r.a.*

Let us prove first that $\mathscr{A}_1$ is coherent : let $\theta \in \mathsf{PL}_{\mathscr{A}_0}$; by definition of the formula $\mathfrak{C}$, there exists $\tau_0 \in \mathsf{PL}_{\mathscr{A}_0}$ such that $\tau_0 \Vdash \mathfrak{C}(\mathbf{1})$.
Since $\chi'\theta\tau_0 \in \mathsf{PL}_{\mathscr{A}_0}$, there exists $\pi \in \Pi$ such that $\chi'\theta\tau_0 \star \pi \notin \perp\!\!\!\perp$, thus $\theta \star \pi^{\tau_0} \notin \perp\!\!\!\perp$, therefore $(\theta, \mathbf{1}) \star (\pi, \mathbf{1}) \notin \perp\!\!\!\perp$.

We check now that $\mathscr{A}_1$ is a r.a. :

- $(\xi, u) \star (\eta, v) \centerdot (\pi, w) \in \perp\!\!\!\perp \Rightarrow (\xi, u)(\eta, v) \star (\pi, w) \in \perp\!\!\!\perp$.

By hypothesis, we have $(\xi \star \eta \centerdot \pi, uvw) \in \perp\!\!\!\perp$, therefore $(\forall \tau \in \Lambda)(\tau \Vdash \mathfrak{C}(uvw) \to \xi \star \eta \centerdot \pi^\tau \in \perp\!\!\!\perp)$ and therefore $(\forall \tau \in \Lambda)(\tau \Vdash \mathfrak{C}(uvw) \to \xi\eta \star \pi^\tau \in \perp\!\!\!\perp)$ hence the result.

- $(\xi, u) \star (\eta, v)(\zeta, w) \centerdot (\pi, z) \in \perp\!\!\!\perp \Rightarrow (\mathsf{B}, \mathbf{1}) \star (\xi, u) \centerdot (\eta, v) \centerdot (\zeta, w) \centerdot (\pi, z) \in \perp\!\!\!\perp$.

By hypothesis, we have $(\xi \star \eta\zeta \centerdot \pi, uvwz) \in \perp\!\!\!\perp$ therefore :
$(\forall \tau \in \Lambda)(\tau \Vdash \mathfrak{C}(uvwz) \to \xi \star \eta\zeta \centerdot \pi^\tau \in \perp\!\!\!\perp)$ thus $(\forall \tau \in \Lambda)(\tau \Vdash \mathfrak{C}(uvwz) \to \mathsf{B} \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi^\tau \in \perp\!\!\!\perp)$.

- $(\xi, u) \star (\zeta, w) \centerdot (\eta, v) \centerdot (\pi, z) \in \perp\!\!\!\perp \Rightarrow (\mathsf{C}^*, \mathbf{1}) \star (\xi, u) \centerdot (\eta, v) \centerdot (\zeta, w) \centerdot (\pi, z) \in \perp\!\!\!\perp$.

By hypothesis, we have $(\xi \star \zeta \centerdot \eta \centerdot \pi, uwvz) \in \perp\!\!\!\perp$, therefore :
$(\forall \tau \in \Lambda)(\mathfrak{c}\tau \Vdash \mathfrak{C}(uwvz) \to \xi \star \zeta \centerdot \eta \centerdot \pi^{\mathfrak{c}\tau} \in \perp\!\!\!\perp)$ therefore, by definition ③ of C^* :
$(\forall \tau \in \Lambda)(\mathfrak{c}\tau \Vdash \mathfrak{C}(uwvz) \to \mathsf{C}^* \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi^\tau \in \perp\!\!\!\perp)$. But, by the property ④ of $\mathfrak{c}$, we have :
$\tau \Vdash \mathfrak{C}(uvwz) \to \mathfrak{c}\tau \Vdash \mathfrak{C}(uwvz)$, hence the result.

- $(\xi, u) \star (\pi, v) \in \perp\!\!\!\perp \Rightarrow (\mathsf{I}, \mathbf{1}) \star (\xi, u) \centerdot (\pi, v) \in \perp\!\!\!\perp$.

Immediate.

- $(\xi,u)\star(\pi,w)\in\perp\!\!\!\perp\Rightarrow(\mathsf{K}^*,\mathbf{1})\star(\xi,u)\centerdot(\eta,v)\centerdot(\pi,w)\in\perp\!\!\!\perp$.

By hypothesis, we have $(\xi\star\pi,uw)\in\perp\!\!\!\perp$, therefore :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(uw)\to\xi\star\pi^{\mathfrak{c}\tau}\in\perp\!\!\perp)$, therefore by the definition ③ of K^* :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(uw)\to\mathsf{K}^*\star\xi\centerdot\eta\centerdot\pi^{\tau}\in\perp\!\!\perp)$. But, by ④, we have :
$\tau\Vdash\mathfrak{C}(uvw)\to\mathfrak{c}\tau\Vdash\mathfrak{C}(uw)$, hence the result.

- $(\xi,u)\star(\eta,v)\centerdot(\eta,v)\centerdot(\pi,w)\in\perp\!\!\!\perp\Rightarrow(\mathsf{W}^*,\mathbf{1})\star(\xi,u)\centerdot(\eta,v)\centerdot(\pi,w)\in\perp\!\!\!\perp$.

By hypothesis, we have $(\xi\star\eta\centerdot\eta\centerdot\pi,uvvw)\in\perp\!\!\!\perp$, therefore :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(uvvw)\to\xi\star\eta\centerdot\eta\centerdot\pi^{\mathfrak{c}\tau}\in\perp\!\!\perp)$, thus, by the definition ③ of W^* :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(uvvw)\to\mathsf{W}^*\star\xi\centerdot\eta\centerdot\pi^{\tau}\in\perp\!\!\perp)$. Now, by ④, we have :
$\tau\Vdash\mathfrak{C}(uvw)\to\mathfrak{c}\tau\Vdash\mathfrak{C}(uvvw)$, hence the result : $\tau\Vdash\mathfrak{C}(uvw)\to\mathsf{W}^*\star\xi\centerdot\eta\centerdot\pi^{\tau}\in\perp\!\!\perp$.

- $(\xi,v)\star(\pi,u)\in\perp\!\!\!\perp\Rightarrow(\mathsf{k}^*_\pi,u)\star(\xi,v)\centerdot(\varpi,w)\in\perp\!\!\!\perp$.

By hypothesis, we have $(\xi\star\pi,vu)\in\perp\!\!\!\perp$, therefore :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(vu)\to\xi\star\pi^{\mathfrak{c}\tau}\in\perp\!\!\perp)$, thus, by the definition ③ of k^*_π :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(vu)\to\mathsf{k}^*_\pi\star\xi\centerdot\varpi^{\tau}\in\perp\!\!\perp)$. Now, by ④, we have :
$\tau\Vdash\mathfrak{C}(uvw)\to\mathfrak{c}\tau\Vdash\mathfrak{C}(vu)$, hence the result : $\tau\Vdash\mathfrak{C}(uvw)\to\mathsf{k}^*_\pi\star\xi\centerdot\varpi^{\tau}\in\perp\!\!\perp$.

- $(\xi,u)\star(\mathsf{k}^*_\pi,v)\centerdot(\pi,v)\in\perp\!\!\!\perp\Rightarrow(\mathsf{cc}^*,\mathbf{1})\star(\xi,u)\centerdot(\pi,v)\in\perp\!\!\!\perp$.

By hypothesis, we have $(\xi\star\mathsf{k}^*_\pi\centerdot\pi,uvv)\in\perp\!\!\!\perp$, therefore :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(uvv)\to\xi\star\mathsf{k}^*_\pi\centerdot\pi^{\mathfrak{c}\tau}\in\perp\!\!\perp)$, thus, by the definition ③ of cc^* :
$(\forall\tau\in\Lambda)(\mathfrak{c}\tau\Vdash\mathfrak{C}(uvv)\to\mathsf{cc}^*\star\xi\centerdot\pi^{\tau}\in\perp\!\!\perp)$. But, by ④, we have :
$\tau\Vdash\mathfrak{C}(uv)\to\mathfrak{c}\tau\Vdash\mathfrak{C}(uvv)$, hence the result : $\tau\Vdash\mathfrak{C}(uv)\to\mathsf{cc}^*\star\xi\centerdot\pi^{\tau}\in\perp\!\!\perp$.

Q.E.D.

The C-forcing defined in $\mathcal{N}$

Let $F(\vec{a})$ be a closed formula of the language of ZF with parameters in $\mathcal{M}$.
We define the formula $p\Vdash F(\vec{a})$ (read "*p forces* $F(\vec{a})$") *as the formula of* ZF_ε *which expresses the C-forcing on* $\mathcal{N}_\epsilon$. In this formula, the variable p is restricted to $\mathbf{V}^{<\omega}$.
We define a subset $(\!(\!(F(\vec{a}))\!)\!)$ of $\mathbf{\Pi}$ by $(\!(\!(F(\vec{a}))\!)\!)=\{(\pi,p)\,;\,\pi\in\|p\not\Vdash\neg F(\vec{a})\|\}$.

Lemma 19.
For every formula $F(\vec{x})$ *of ZF, there exist two proof-like terms* $\mathfrak{p}_F,\mathfrak{p}'_F$ *of* $\mathcal{A}$ *such that :*
i) $\xi\Vdash(p\Vdash F(\vec{a}))\Rightarrow(\mathfrak{p}_F\xi,p)\Vvdash(\!(\!(F(\vec{a}))\!)\!)$
ii) $(\xi,p)\Vvdash(\!(\!(F(\vec{a}))\!)\!)\Rightarrow\mathfrak{p}'_F\xi\Vdash(p\Vdash F(\vec{a}))$
for every $\xi\in\Lambda$ *and* $p\in\mathbf{V}^{<\omega}$.

By a well known property of forcing [9, 18], the formula $p\Vdash F(\vec{x})$ is equivalent, in ZF_ε, to the formula $\forall q(\mathfrak{C}(pq)\to q\not\Vdash\neg F(\vec{x}))$.
It follows that there are two proof-like terms $\mathfrak{q}_F,\mathfrak{q}'_F$ such that :
(1) $\mathfrak{q}_F\Vdash(p\Vdash F(\vec{a}))\to\forall q(\mathfrak{C}(pq)\to q\not\Vdash\neg F(\vec{a}))$;
(2) $\mathfrak{q}'_F\Vdash\forall q(\mathfrak{C}(pq)\to q\not\Vdash\neg F(\vec{a}))\to(p\Vdash F(\vec{a}))$.

i) By applying (1) to the hypothesis, we obtain $\mathfrak{q}_F\xi\Vdash\forall q(\mathfrak{C}(pq)\to q\not\Vdash\neg F(\vec{a}))$ that is :
$\forall\pi\forall q\forall\tau(\tau\Vdash\mathfrak{C}(pq),\pi\in\|q\not\Vdash\neg F(\vec{a})\|\to\mathfrak{q}_F\xi\star\tau\centerdot\pi\in\perp\!\!\perp)$. It follows that :
$\forall\pi\forall q(\pi\in\|q\not\Vdash\neg F(\vec{a})\|\to\forall\tau(\tau\Vdash\mathfrak{C}(pq)\to(\chi)(\mathfrak{q}_F)\xi\star\pi^{\tau}\in\perp\!\!\perp))$.
Now $\pi\in\|q\not\Vdash\neg F(\vec{a})\|$ is the same as $(\pi,q)\in(\!(\!(F(\vec{a}))\!)\!)$ and

$\forall\tau(\tau \Vdash \mathfrak{C}(pq) \to (\chi)(\mathfrak{q}_F)\xi \star \pi^\tau \in \perp\!\!\!\perp)$ is the same as $(\mathfrak{p}_F\xi, p) \star (\pi, q) \in \perp\!\!\!\perp\!\!\!\perp$ with $\mathfrak{p}_F = \lambda x(\chi)(\mathfrak{q}_F)x$. Thus we obtain $(\mathfrak{p}_F\xi, p) \Vvdash (\!(\!(F(\vec{a}))\!)\!)$.

ii) The hypothesis gives $\forall\pi\forall q((\pi, q) \in (\!(\!(F(\vec{a}))\!)\!) \to (\xi \star \pi, pq) \in \perp\!\!\!\perp\!\!\!\perp)$ that is :
$\forall\pi\forall q\forall\tau(\pi \in \|q \not\Vdash \neg F(\vec{a})\|, \tau \Vdash \mathfrak{C}(pq) \to \xi \star \pi^\tau \in \perp\!\!\!\perp)$ and therefore :
$\forall\pi\forall q\forall\tau(\tau \Vdash \mathfrak{C}(pq), \pi \in \|q \not\Vdash \neg F(\vec{a})\| \to \chi'\xi \star \tau \,\bullet\, \pi \in \perp\!\!\!\perp)$.
It follows that $\chi'\xi \Vdash \forall q(\mathfrak{C}(pq) \to q \not\Vdash \neg F(\vec{a}))$ and therefore, by (2) :
$(\mathfrak{q}'_F)(\chi')\xi \Vdash (p \Vdash F(\vec{a}))$. We set $\mathfrak{p}'_F = \lambda x(\mathfrak{q}'_F)(\chi')x$.

Q.E.D.

In the general theory of classical realizability, we define a truth value for the formulas of ZF_ε and therefore, in particular, for the formulas of ZF. We will define here directly a new truth value $|||F(a_1, \dots, a_n)|||$ *for a formula of ZF* with parameters in $\mathscr{M}$ for the r.a. $\mathscr{A}_1$.
To this aim, we first define the truth values $|||a \notin b|||, |||a \subset b|||$ of the atomic formulas of ZF ; then that of $F(a_1, \dots, a_n)$, by induction on the length of the formula.
Theorem 1 (adequacy theorem) remains valid (cf. the remark after theorem 1) :

$|||a \notin b||| = (\!(\!(a \notin b)\!)\!)$; $|||a \subset b||| = (\!(\!(a \subset b)\!)\!)$;
$|||F \to F'||| = \{(\xi \,\bullet\, \pi, pq)\,;\, (\xi, p) \Vvdash F, (\pi, q) \in |||F'|||\}$;
$|||\forall x\, F(x, a_1, \dots, a_n)||| = \bigcup_a |||F(a, a_1, \dots, a_n)|||$.
Of course $\Vvdash$ is defined by : $(\xi, p) \Vvdash F \Leftrightarrow (\forall(\pi, q) \in |||F|||)((\xi, p) \star (\pi, q) \in \perp\!\!\!\perp\!\!\!\perp)$.

Remark. Be careful, as we said before, these are not the truth values, in the r.a. $\mathscr{A}_1$, of $a \notin b$ and $a \subset b$ *considered as formulas of* ZF_ε. We seek here to define directly the C-generic model on $\mathscr{N}_\in$ without going through a model of ZF_ε.

Theorem 20 below may be considered as a generalization of the well known result about iteration of forcing : the r.a. $\mathscr{A}_1$, which is a kind of product of $\mathscr{A}_0$ by $\mathfrak{C}$, gives the same r.m. as the $\mathfrak{C}$-generic extension of $\mathscr{N}_\in$.

Theorem 20.
For each closed formula F of ZF with parameters in the model $\mathscr{N}$, there exist two proof-like terms χ_F, χ'_F, which only depend on the propositional structure of F, such that we have, for every $\xi \in \Lambda$ and $p \in \mathbf{V}^{<\omega}$:
$\xi \Vdash (p \Vdash F) \;\Rightarrow\; (\chi_F\xi, p) \Vvdash F$ *and* $(\xi, p) \Vvdash F \;\Rightarrow\; \chi'_F\xi \Vdash (p \Vdash F)$.

The *propositional structure* of F is the propositional formula built with the connective $\to$ and only two atoms $O_\in, O_\subset$, which is obtained from F by deleting all quantifiers and by identifying all atomic formulas $t \notin u$, $t \subset u$ respectively with $O_\in, O_\subset$.
For instance, the propositional structure of the formula :
$\forall X(\forall x(\forall y((x, y) \notin Y \to y \notin X) \to x \notin X) \to \forall x(x \notin X))$ is $((O_\in \to O_\in) \to O_\in) \to O_\in$.

Proof by recurrence on the length of F.

- If F is atomic, we have $F \equiv a \notin b$ or $a \subset b$. Apply lemma 19 with $F(\vec{a}) \equiv a \notin b$ or $F(\vec{a}) \equiv a \subset b$.
- If $F \equiv \forall x\, F'$, then $p \Vdash F \equiv \forall x(p \Vdash F')$. Therefore $\xi \Vdash p \Vdash F \equiv \forall x(\xi \Vdash (p \Vdash F'))$.

Moreover, $(\xi, p) \Vvdash F \equiv \forall x((\xi, p) \Vvdash F')$.
The result is immediate, from the recurrence hypothesis.

- If $F \equiv F' \to F''$, we have $p \Vdash F \equiv \forall q(q \Vdash F' \to pq \Vdash F'')$ and therefore :

⑤ $\quad \xi \Vdash (p \Vdash F) \Rightarrow \forall\eta\forall q(\eta \Vdash (q \Vdash F') \to \xi\eta \Vdash (pq \Vdash F''))$.
Suppose that $\xi \Vdash (p \Vdash F)$ and put $\chi_F = \lambda x\lambda y(\chi_{F''})(x)(\chi'_{F'})y$.

We must show $(\chi_F\xi, p) \Vdash\!\!\vdash F' \to F''$; thus, let $(\eta, q) \Vdash\!\!\vdash F'$ and $(\pi, r) \in |||F''|||$.
We must show $(\chi_F\xi, p) \star (\eta, q) \bullet (\pi, r) \in \perp\!\!\!\perp$ that is $(\chi_F\xi \star \eta \bullet \pi, pqr) \in \perp\!\!\!\perp$.
Thus, let $\tau \Vdash \mathfrak{C}(pqr)$; we must show $\chi_F\xi \star \eta \bullet \pi^\tau \in \perp\!\!\!\perp$ or else $\chi_F \star \xi \bullet \eta \bullet \pi^\tau \in \perp\!\!\!\perp$.

From the recurrence hypothesis applied to $(\eta, q) \Vdash\!\!\vdash F'$, we have $\chi'_{F'}\eta \Vdash (q \Vdash F')$.
From ⑤, we have therefore $(\xi)(\chi'_{F'})\eta \Vdash (pq \Vdash F'')$.
Applying again the recurrence hypothesis, we get :
$((\chi_{F''})(\xi)(\chi'_{F'})\eta, pq) \Vdash\!\!\vdash F''$. But since $(\pi, r) \in |||F''|||$, we have :
$((\chi_{F''})(\xi)(\chi'_{F'})\eta, pq) \star (\pi, r) \in \perp\!\!\!\perp$, that is $((\chi_{F''})(\xi)(\chi'_{F'})\eta \star \pi, pqr) \in \perp\!\!\!\perp$.
Since $\tau \Vdash \mathfrak{C}(pqr)$, we have $(\chi_{F''})(\xi)(\chi'_{F'})\eta \star \pi^\tau \in \perp\!\!\!\perp$.
But, by definition of χ_F, we have $\chi_F \star \xi \bullet \eta \bullet \pi^\tau \succ (\chi_{F''})(\xi)(\chi'_{F'})\eta \star \pi^\tau$ which gives the desired result : $\chi_F \star \xi \bullet \eta \bullet \pi^\tau \in \perp\!\!\!\perp$.

Suppose now that $(\xi, p) \Vdash\!\!\vdash F' \to F''$; we set $\chi'_F = \lambda x \lambda y(\chi'_{F''})(x)(\chi_{F'})y$.
We must show $\chi'_F\xi \Vdash (p \Vdash F' \to F'')$ that is $\forall q(\chi'_F\xi \Vdash (q \Vdash F' \to pq \Vdash F''))$.
Thus, let $\eta \Vdash q \Vdash F'$ and $\pi \in \|pq \Vdash F''\|$; we must show $\chi'_F\xi \star \eta \bullet \pi \in \perp\!\!\!\perp$.
By the recurrence hypothesis, we have $(\chi_{F'}\eta, q) \Vdash\!\!\vdash F'$, therefore $(\xi, p)(\chi_{F'}\eta, q) \Vdash\!\!\vdash F''$ or else, by definition of the algebra $\mathscr{A}_1$: $((\xi)(\chi_{F'})\eta, pq) \Vdash\!\!\vdash F''$.
Applying again the recurrence hypothesis, we have $(\chi'_{F''})(\xi)(\chi_{F'})\eta \Vdash (pq \Vdash F'')$ and therefore $(\chi'_{F''})(\xi)(\chi_{F'})\eta \star \pi \in \perp\!\!\!\perp$. But we have, by definition of χ'_F :
$\chi'_F\xi \star \eta \bullet \pi \succ \chi'_F \star \xi \bullet \eta \bullet \pi \succ (\chi'_{F''})(\xi)(\chi_{F'})\eta \star \pi$; the desired result $\chi'_F\xi \star \eta \bullet \pi \in \perp\!\!\!\perp$ follows.

Q.E.D.

Theorem 21. *For each axiom A of ZF, there exists a proof like term Θ_A of the r.a. $\mathscr{A}_0$ such that $(\Theta_A, \mathbf{1}) \Vdash\!\!\vdash A$.*

Indeed, if we denote by $\mathscr{N}_\in[G]$ the C-generic model over $\mathscr{N}_\in$, with $G \subseteq C$ being the generic set, we have $\mathscr{N}_\in[G] \models$ ZF. Therefore, $\mathscr{N} \models (\mathbf{1} \Vdash A)$, which means that there is a proof-like term Θ'_A such that $\Theta'_A \Vdash (\mathbf{1} \Vdash A)$. By theorem 20, we can take $\Theta_A = \chi_A\Theta'_A$.

Q.E.D.

4 The algebra $\mathfrak{A}_0$

We define a r.a. $\mathfrak{A}_0$ which gives a very interesting r.m. $\mathscr{N}$. In the following, we use only this r.a. and a generic extension $\mathfrak{A}_1$.
The terms of $\mathfrak{A}_0$ are finite sequences of symbols :

$$), (, \mathsf{B}, \mathsf{C}, \mathsf{I}, \mathsf{K}, \mathsf{W}, \mathsf{cc}, \mathsf{a}, \mathsf{p}, \gamma, \kappa, \mathsf{e}, \chi, \chi', h_0, h_1, \ldots, h_i, \ldots$$

Λ is the least set which contains these symbols (except parentheses) and is such that :
$t, u \in \Lambda \Rightarrow (t)u \in \Lambda$.
A stack is a finite sequence of terms, separated by the symbol $\bullet$ and terminated by the symbol π_0 *(the empty stack)*.
Π is therefore the least set such that $\pi_0 \in \Pi$ and $t \in \Lambda, \pi \in \Pi \Rightarrow t \bullet \pi \in \Pi$.
k_π is defined by recurrence : $\mathsf{k}_{\pi_0} = \mathsf{a}$; $\mathsf{k}_{t.\pi} = \lambda x(\mathsf{k}_\pi)(x)t = ((\mathsf{C})(\mathsf{B})\mathsf{k}_\pi)t$.
The application $(\tau, \pi) \mapsto \pi^\tau$ from $\Lambda \times \Pi$ into Π consists in replacing π_0 by $\tau \bullet \pi_0$.
It is therefore recursively defined by : $\pi_0^\tau = \tau \bullet \pi_0$; $(t \bullet \pi)^\tau = t \bullet \pi^\tau$.
$\Lambda \star \Pi$ is $\Lambda \times \Pi$.

$\perp\!\!\!\perp$ is the least subset of $\Lambda \star \Pi$ satisfying the conditions :

1. $\mathsf{p} \star \pi \in \perp\!\!\!\perp$ for every stack $\pi \in \Pi$ *(stop)* ;
2. $\xi \star \pi_0 \in \perp\!\!\!\perp \Rightarrow \mathsf{a} \star \xi \centerdot \pi \in \perp\!\!\!\perp$ for every $\xi \in \Lambda, \pi \in \Pi$ *(abort)* ;
3. If at least two out of $\xi \star \pi, \eta \star \pi, \zeta \star \pi$ are in $\perp\!\!\!\perp$, then $\gamma \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi \in \perp\!\!\!\perp$ *(fork)* ;
4. $\xi \star \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{e} \star h_i \centerdot h_i \centerdot \eta \centerdot \xi \centerdot \pi \in \perp\!\!\!\perp$ for every $\xi, \eta \in \Lambda$ and $i \in \mathbb{N}$ *(elimination of constants)* ;
5. $\xi \star \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{e} \star h_i \centerdot h_j \centerdot \xi \centerdot \eta \centerdot \pi \in \perp\!\!\!\perp$ for every $\xi, \eta \in \Lambda$ and $i, j \in \mathbb{N}, i \neq j$ *(elimination of constants)* ;
6. $\xi \star h_n \centerdot \pi \in \perp\!\!\!\perp \Rightarrow \kappa \star \xi \centerdot \pi \in \perp\!\!\!\perp$ if h_n does not appear in ξ, π *(introduction of constants)* ;

and also the general axiomatic conditions for $\mathsf{B}, \mathsf{C}, \mathsf{I}, \mathsf{K}, \mathsf{W}, \mathsf{cc}, \chi, \chi'$ and the application :

7. $\xi \star \eta \centerdot \pi \in \perp\!\!\!\perp \Rightarrow (\xi)\eta \star \pi \in \perp\!\!\!\perp$ *(push)* ;
8. $\xi \star \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{I} \star \xi \centerdot \pi \in \perp\!\!\!\perp$ *(no operation)* ;
9. $\xi \star \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{K} \star \xi \centerdot \eta \centerdot \pi \in \perp\!\!\!\perp$ *(delete)* ;
10. $\xi \star \eta \centerdot \eta \centerdot \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{W} \star \xi \centerdot \eta \centerdot \pi \in \perp\!\!\!\perp$ *(copy)* ;
11. $\xi \star \zeta \centerdot \eta \centerdot \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{C} \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi \in \perp\!\!\!\perp$ *(switch)* ;
12. $\xi \star (\eta)\zeta \centerdot \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{B} \star \xi \centerdot \eta \centerdot \zeta \centerdot \pi \in \perp\!\!\!\perp$ *(apply)* ;
13. $\xi \star \mathsf{k}_\pi \centerdot \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{cc} \star \xi \centerdot \pi \in \perp\!\!\!\perp$ *(save the stack)* ;
14. $\xi \star \tau \centerdot \pi \in \perp\!\!\!\perp \Rightarrow \chi \star \xi \centerdot \pi^\tau \in \perp\!\!\!\perp$ *(read the end of the stack)* ;
15. $\xi \star \pi^\tau \in \perp\!\!\!\perp \Rightarrow \chi' \star \tau \centerdot \xi \centerdot \pi \in \perp\!\!\!\perp$ *(write at the end of the stack).*

The property :
$\xi \star \pi \in \perp\!\!\!\perp \Rightarrow \mathsf{k}_\pi \star \xi \centerdot \varpi \in \perp\!\!\!\perp$ *(restore the stack)*
now follows easily from the definition of k_π.

A term is defined to be *proof-like* if it contains neither a, p nor any h_i.
If $\xi \in \mathsf{PL}$ (the set of proof-like terms), then the process $\xi \star \pi_0$ does not contain the symbol p ; thus $\xi \star \pi_0 \notin \perp\!\!\!\perp$. It follows that *the algebra* $\mathfrak{A}_0$ *is coherent.*

Theorem 22. *The Boolean algebra* $\beth 2$ *has at most 4 elements.*

Let us show that $\gamma \Vdash \forall x^{\beth 2} \forall y^{\beth 2}(xy \neq 0, y \neq 1, xy \neq y \to \perp)$. This means exactly that γ realizes the three formulas $(\perp, \perp, \top \to \perp)$, $(\perp, \top, \perp \to \perp)$ and $(\top, \perp, \perp \to \perp)$, which follows immediately from rule 3 of the definition of $\perp\!\!\!\perp$.

Q.E.D.

If $\beth 2$ is trivial, everything in the following is also (cf. the remark before theorem 32). Therefore, we now assume that $\beth 2$ has 4 elements.

Let a_0, a_1 be the atoms of $\beth 2$. Then $\mathscr{M}_{a_0} = a_0\mathscr{N}$ and $\mathscr{M}_{a_1} = a_1\mathscr{N}$ are classes in the r.m. $\mathscr{N}$ respectively defined by the formulas $x = a_0 x$ and $x = a_1 x$.

We define the binary functional $\sqcup$ in $\mathscr{N}$ as the extension of the functional $(x, y) \mapsto x \cup y$ on $\mathscr{M}$. We don't use the symbol $\cup$, because it already denotes the union. For instance, we have $\beth\{0\} \sqcup \beth\{1\} = \beth 2$ but $\beth\{0\} \cup \beth\{1\} = \{0, 1\}$.
The identity $x = a_0 x \sqcup a_1 x$ gives a bijection from $\mathscr{N}$ onto $\mathscr{M}_{a_0} \times \mathscr{M}_{a_1}$.

We have $\mathscr{M} \prec \mathscr{M}_{a_0}, \mathscr{M}_{a_1}$. Let us show that one of them, say $\mathscr{M}_{a_0}$, is well founded in $\mathscr{N}$ and therefore :

$$\mathscr{M}_{a_0} = \mathscr{M}_{\mathscr{D}} \text{ and the class of ordinals } \mathrm{On} \text{ is defined in } \mathscr{N}.$$

Lemma 23. *The relation* $\langle x \in y \rangle = 1$ *is well founded.*

We show $\mathsf{Y} \Vdash \forall y(\forall x(\langle x \in y\rangle = 1 \hookrightarrow F(x)) \to F(y)) \to \forall y\, F(y)$ for any formula F of ZF_ε. Let $\xi \Vdash \forall y(\forall x(\langle x \in y\rangle = 1 \hookrightarrow F(x)) \to F(y))$. We show, by induction on $\mathrm{rk}(y_0)$ that $\mathsf{Y}\xi \Vdash F(y_0)$. Thus we have $(\forall x \in y_0)(\mathsf{Y}\xi \Vdash F(x))$ i.e. $\mathsf{Y}\xi \Vdash \forall x(\langle x \in y_0\rangle = 1 \hookrightarrow F(x))$ and therefore : $(\xi)(\mathsf{Y})\xi \Vdash F(y_0)$ by hypothesis on ξ. Hence the result since $\mathsf{Y}\xi \succ (\xi)(\mathsf{Y})\xi$.

Q.E.D.

The relation $\langle x \in y\rangle = 1$ is the product of the relations $\langle a_0 x \in a_0 y\rangle = a_0$ and $\langle a_1 x \in a_1 y\rangle = a_1$ respectively defined on $a_0\mathcal{N}$ and $a_1\mathcal{N}$. Since their product is well founded, one of them must be.

Remark. If the ground model $\mathcal{M}$ satisfies V = L, then $\mathcal{M}_{a_0} = \mathcal{M}_{\mathcal{D}}$ is isomorphic to $\mathrm{L}^{\mathcal{N}_\in}$, the class of constructible sets of $\mathcal{N}_\in$.

Execution of processes

If a given process $\xi \star \pi$ is in $\perp\!\!\!\perp$, it is obtained by applying precisely one of the rules of definition of $\perp\!\!\!\perp$: if ξ is an application, it is rule 7, else ξ is an instruction and there is one and only one corresponding rule.
In this way, we get a finite tree, which is the proof that $\xi \star \pi \in \perp\!\!\!\perp$; it is linear, except in the case of rule 3 (instruction γ) where there is a triple branch. This tree is called *the execution of the process* $\xi \star \pi$.
We can, of course, build this tree for any process ; it may then be infinite.

Computing with the instruction γ

Let us consider, in the ground model $\mathcal{M}$, some functions $f_i : \mathbb{N}^{k_i} \to \mathbb{N}$, satisfying a set of axioms of the form : $(\forall \vec{x} \in \mathbb{N}^k)(t_0[\vec{x}] = u_0[\vec{x}], \ldots, t_{n-1}[\vec{x}] = u_{n-1}[\vec{x}] \to t[\vec{x}] = u[\vec{x}])$
where t_i, u_i are terms built with the symbols f_i and the variables $\vec{x}$.
Moreover, one of these axioms concerns a particular function f, and says that f has at most one zero : $(\forall x, y \in \mathbb{N})(f[x] = f[y] = 0 \to x = y)$.
These function symbols are also interpreted in $\mathcal{N}$ where we have $f_i : \daleth\mathbb{N}^{k_i} \to \daleth\mathbb{N}$ and in this way, we have a set $\mathcal{E}$ of realized axioms :

$$\mathsf{I} \Vdash \forall \vec{x}^{\daleth\mathbb{N}^k}(t_0[\vec{x}] = u_0[\vec{x}], \ldots, t_{n-1}[\vec{x}] = u_{n-1}[\vec{x}] \hookrightarrow t[\vec{x}] = u[\vec{x}])$$

and in particular :

$$\mathsf{I} \Vdash \forall x^{\daleth\mathbb{N}} \forall y^{\daleth\mathbb{N}}(f[x] = 0, f[y] = 0 \hookrightarrow x = y).$$

Now suppose that, with the axioms $\mathcal{E}$ and some other axioms realized in $\mathcal{N}$, which do not contain the symbols f_i, like for instance :

$$\mathcal{E} + \mathrm{ZF}_\varepsilon + \daleth 2 \textit{ has at most 4 elements} + \daleth\mathbb{N} \textit{ is countable} + \cdots$$

we can prove $\exists n^{\mathrm{int}}(f[n] = 0)$. Since all these axioms are realized, we get, by theorem 1, a proof-like term θ such that $\theta \Vdash \forall n^{\mathrm{int}}(f[n] \neq 0) \to \perp$ and θ may contain the instructions e, κ and, above all, γ.
We shall show how θ allows to compute the (unique) solution n_0 of the equation $f[n] = 0$.
Note that *we do not assume that the f_i (in particular f) are recursive* (in fact, it is not even necessary that their domain or range is $\mathbb{N}$). On the other hand, we may add symbols for all recursive functions, since they are defined by axiom systems of this form.
Let us add a term constant δ and the rule $\delta \star \underline{n}_0 . \pi \in \perp\!\!\!\perp$ in the definition of $\perp\!\!\!\perp$ (of course,

without knowing the actual value of n_0). Thus, we have $\delta \Vdash \forall n^{\mathrm{int}}(f[n] \neq 0)$ and therefore $\theta \star \delta \bullet \pi_0 \in \perp\!\!\!\perp$.

But any process $\xi \star \pi \in \perp\!\!\!\perp$ which does not contain p (but possibly containing δ) computes n_0. We show this by recurrence on the number of applications of rules for $\perp\!\!\!\perp$ used to build it :

If this number is 1, the process is $\delta \star \underline{n}_0 \bullet \pi$. Else, the only non trivial case is when the process is $\gamma \star \xi \bullet \eta \bullet \zeta \bullet \pi$ and when two out of the three processes $\xi \star \pi, \eta \star \pi, \zeta \star \pi$ are in $\perp\!\!\!\perp$ (but we don't know which). By the recurrence hypothesis, at least two of them will give the integer n_0 which is therefore determined as the only integer obtained at least two times.

Example : $\gamma \star (((\gamma)(\delta)\underline{n})(\delta)\underline{n})(\delta)\underline{n}_0 \bullet (((\gamma)(\delta)\underline{n}_0)(\delta)\underline{n})(\delta)\underline{n}_0 \bullet (((\gamma)(\delta)\underline{n})(\delta)\underline{n}_0)(\delta)\underline{n}_0 \bullet \pi$.

Remarks.

1. Since f is not supposed recursive, the trivial method to find n_0 by trying $0, 1, 2, \ldots$ may not be available. A working algorithm is by proving $f[n_0] = 0$ by equational deduction from $\mathscr{E}$. Both are, in general, very heavy or totally impracticable. Moral : it is better to use the powerful set theoretical axioms than only the weak equational ones to get a working program.
2. If f may have several zeroes, we can easily define f' by a system of equations such that f' has only one zero which is the first zero of f, and apply the method to f'. This supposes f to be recursive.

ℷ2 is not (always) trivial

Although this will not be used in the following, it is interesting to show that there is a r.m. of $\mathfrak{A}_0$ in which ℷ2 is not trivial and is therefore the 4-elements Boolean algebra.

Lemma 24. *If $\theta \Vdash \forall x^{\gimel 2}(x \neq 0, x \neq 1 \to \perp)$ then, for any formulas F, G :*
$\theta' \Vdash F, G \to F$ and $\theta' \Vdash F, G \to G$ with $\theta' = \lambda x \lambda y(\mathsf{cc})\lambda k((\theta)(k)x)(k)y$.

The hypothesis means that $\theta \Vdash \perp, \top \to \perp$ and $\theta \Vdash \top, \perp \to \perp$.

We have $x : F, y : G, k : \neg F \vdash kx : \perp, (\theta)(k)x : \top \to \perp, ((\theta)(k)x)(k)y : \perp$.

It follows that $x : F, y : G \vdash (\mathsf{cc})\lambda k((\theta)(k)x)(k)y : F$ hence the first result.

We have $x : F, y : G, k : \neg G \vdash ky : \perp, (\theta)(k)x : \perp \to \perp, ((\theta)(k)x)(k)y : \perp$.

It follows that $x : F, y : G \vdash (\mathsf{cc})\lambda k((\theta)(k)x)(k)y : G$ hence the second result.

Q.E.D.

Suppose that, in every r.m. for the r.a. $\mathfrak{A}_0$, the Boolean algebra ℷ2 is trivial.

Then the hypothesis of lemma 24 is satisfied for some proof-like term θ.

Choose the formulas $F \equiv \exists n^{\mathrm{int}}(n = 0)$ and $G \equiv \exists n^{\mathrm{int}}(n = 1)$. Then, we have $\lambda x\, x\underline{0} \Vdash F$ and $\lambda x\, x\underline{1} \Vdash G$. By lemma 24, it follows that $\theta'' = ((\theta')\lambda x\, x\underline{0})\lambda x\, x\underline{1} \Vdash F$ and also $\Vdash G$.

Then, by the algorithm given above, the proof-like term θ'' computes simultaneously 0 and 1, which is a contradiction.

ℷℕ is countable

We define two sets, in the ground model $\mathscr{M}$:

$\mathbb{H} = \{h_i\, ;\, i \in \mathbb{N}\}$, $\mathsf{H} = \{(h_i, h_i \bullet \pi)\, ;\, i \in \mathbb{N}, \pi \in \Pi\}$

and also the bijection $\mathsf{h} : \mathbb{N} \to \mathbb{H}$ such that $\mathsf{h}[i] = h_i$ for every $i \in \mathbb{N}$.

This bijection extends to the model $\mathscr{N}$ into a bijection $\mathsf{h} : \gimel\mathbb{N} \to \gimel\mathbb{H}$. Moreover, we have trivially $\Vdash \mathsf{H} \subseteq \gimel\mathbb{H}$; in fact $\mathsf{I} \Vdash \forall x(x \not\varepsilon \gimel\mathbb{H} \to x \not\varepsilon \mathsf{H})$.

Lemma 25.
i) $\Vdash \forall i^{\daleth\mathbb{N}}\forall j^{\daleth\mathbb{N}}(h[i]\,\varepsilon\, H, h[j]\,\varepsilon\, H, \langle i=j\rangle \neq 0 \to i=j)$.
ii) H is countable.

i) By definition of H, we have $\|\mathsf{h}[i] \not\varepsilon\, \mathsf{H}\| = \|\{h_i\} \to \bot\|$.
Therefore, it suffices to show that $\mathsf{e} \Vdash \{h_i\}, \{h_j\}, \langle i=j\rangle \neq 0, i \neq j \to \bot$.
Let $t \Vdash \langle i=j\rangle \neq 0$ and $u \Vdash i \neq j$. We must show $\mathsf{e} \star h_i \bullet h_j \bullet t \bullet u \bullet \pi \in \perp\!\!\!\perp$, which follows immediately from the execution rule of e.
ii) Thus we have $\mathcal{N} \models \forall i^{\daleth\mathbb{N}}\forall j^{\daleth\mathbb{N}}(\mathsf{h}[i]\,\varepsilon\,\mathsf{H}, \mathsf{h}[j]\,\varepsilon\,\mathsf{H}, i a_0 = j a_0 \to i=j)$. Now, let $i\,\varepsilon\,\daleth\mathbb{N}$ be such that $\mathsf{h}[i]\,\varepsilon\,\mathsf{H}$. Then i is determined by $i a_0$, which is an integer of $\mathcal{M}_{a_0}$ and therefore an integer of $\mathcal{N}$. Since h is one-to-one, the result follows.

Q.E.D.

Define the function symbols $\mathrm{pr}_0, \mathrm{pr}_1 : \mathbb{N} \to \mathbb{N}$ by :
$n = \mathrm{pr}_1[n] + \frac{1}{2}(\mathrm{pr}_0[n] + \mathrm{pr}_1[n])(\mathrm{pr}_0[n] + \mathrm{pr}_1[n] + 1)$ (bijection from $\mathbb{N}^2$ onto $\mathbb{N}$).

Theorem 26.
i) $\kappa \Vdash \forall \nu^{\daleth\mathbb{N}}\exists n^{\daleth\mathbb{N}}\{h[n]\,\varepsilon\, H, \nu = pr_1[n]\}$.
ii) $\Vdash \daleth\mathbb{N}$ *is countable.*

i) Let $\nu \in \mathbb{N}, \pi \in \Pi$ and $\xi \Vdash \forall n^{\daleth\mathbb{N}}\{\nu = \mathrm{pr}_1[n] \hookrightarrow \mathsf{h}[n] \not\varepsilon\, \mathsf{H}\}$. Thus, we have $\xi \star h_n \bullet \pi \in \perp\!\!\!\perp$ for all $n \in \mathbb{N}$ such that $\nu = \mathrm{pr}_1[n]$. There is an infinity of such n, so that we can choose one such that h_n does not appear in ξ, π. It follows that $\kappa \star \xi \bullet \pi \in \perp\!\!\!\perp$.
ii) Since $\mathsf{h} : \daleth\mathbb{N} \to \daleth\mathbb{H}$ is a bijection, we obtain a surjection from H onto $\daleth\mathbb{N}$. It follows from lemma 25(ii) that $\mathcal{N} \models (\daleth\mathbb{N}$ *is countable*).

Q.E.D.

Theorem 27. $\mathcal{N} \models$ *NEPC (the non extensional principle of choice).*

This means that for any formula $R(x,y)$ of ZF_ε, there is a binary relation $\Phi(x,y)$ such that
$\Vdash \forall x \forall y \forall y'(\Phi(x,y), \Phi(x,y') \to y = y')$ (functional relation) ;
$\Vdash \forall x \forall y(R(x,y) \to \exists y'\{R(x,y'), \Phi(x,y')\})$ (choice).
This does not give the usual principle of choice in the model $\mathcal{N}_\in$ of ZF because, even if R is compatible with the extensional equivalence $=_\in$, Φ is not necessarily so.
By lemma 13, we have $\Vdash \forall x \forall y(R(x,y) \to \exists \varpi^{\daleth\Pi} R(x, f[x,\varpi]))$ where f is a functional symbol defined in $\mathcal{M}$. Now, Π is countable in $\mathcal{M}$, thus $\daleth\Pi$ is equipotent to $\daleth\mathbb{N}$ and therefore countable by theorem 26. Therefore, we can define $\Phi(x,y)$ as "$y = f[x,\varpi]$ for the first $\varpi\,\varepsilon\,\daleth\Pi$ such that $R(x, f[x,\varpi])$".

Q.E.D.

By the results of [14], it follows also that $\mathcal{N} \models (\mathbb{R}$ *is not well orderable*).
Note that these results do not really use the instruction γ : in the proof of lemma 25(ii), we could use the canonical ultrafilter on $\daleth 2$ (see [16]) instead of the atom a_0. Therefore, they are valid for any $\daleth 2$.
On the other hand, the following result uses γ, i.e. the fact that $\daleth 2$ is finite :

Theorem 28. $\mathcal{N} \models$ *the axiom of well ordered choice (WOC) i.e. : The product of a family of non void sets indexed by a well ordered set is non void.*

This follows immediately from NEPC and the fact that On is isomorphic to a class of $\mathcal{N}$.

Q.E.D.

Remark. In fact, since $\mathcal{N}$ satisfies NEPC, it also satisfies the well ordered principle of choice (WOPC).

Theorem 28 has two interesting consequences :

1. There exists a proof-like term $\Theta_{WOC} \Vdash$ WOC which means that we now have a program for the axiom WOC, which is a λ-term with the instructions $\gamma, \kappa, \mathsf{e}$.
2. This gives a new proof that AC (and even "$\mathbb{R}$ *is well orderable*") is not a consequence of ZF + WOC [8].

5 The algebra $\mathfrak{A}_1$ and a program for AC (and others)

Lemma 29. *Let $R(x,y)$ be a formula of ZF$_\varepsilon$ such that $R(a_0x, a_1y)$ defines, in $\mathcal{N}$, a functional from $\mathcal{M}_{a_0}$ into $\mathcal{M}_{a_1}$ or from $\mathcal{M}_{a_1}$ into $\mathcal{M}_{a_0}$. Then, this functional has a countable image.*

Remember that $\mathcal{M}_{a_i}(i = 0,1)$ is the class defined by $a_i x = x$.
Suppose, for instance, that $R(x,y)$ defines a functional from $\mathcal{M}_{a_0}$ into $\mathcal{M}_{a_1}$ i.e. :
$\mathcal{N} \models \forall x \forall y \forall y'(R(a_0x, a_1y), R(a_0x, a_1y') \to a_1y = a_1y')$.
Applying lemma 13 to the formula $\neg R(a_0x, a_1y)$, we obtain :

$$\mathsf{I} \Vdash \forall \varpi^{\beth\Pi} \neg R(a_0x, a_1 f[a_0x, \varpi]) \to \forall y \neg R(a_0x, a_1y)$$

for some functional $f : \mathcal{M} \times \Pi \to \mathcal{M}$ *defined in* $\mathcal{M}$.
By lemma 7, we have $a_1 f[a_0x, \varpi] = a_1 f[a_1a_0x, \varpi]$. Since $a_1a_0 = 0$, we get :

$$\mathsf{I} \Vdash \forall \varpi^{\beth\Pi} \neg R(a_0x, a_1 f[\emptyset, \varpi]) \to \forall y \neg R(a_0x, a_1y).$$

Now Π is countable (in $\mathcal{M}$), thus $\beth\Pi$ is equipotent to $\beth\mathbb{N}$; therefore $\beth\Pi$ is countable (in $\mathcal{N}$) by theorem 26. Hence we have, for some surjection g from $\mathbb{N}$ onto $\{f[\emptyset, \varpi] ; \varpi \,\varepsilon\, \beth\Pi\}$:

$$\Vdash \forall n^{\mathrm{int}} \neg R(a_0x, a_1 g(n)) \to \forall y \neg R(a_0x, a_1y).$$

Thus, we have $\Vdash \exists y\, R(a_0x, a_1y) \to \exists n^{\mathrm{int}} R(a_0x, a_1 g(n))$.
It follows that $a_1 g$ is a surjection from $\mathbb{N}$ onto the image of R.

Q.E.D.

Remark. This shows that $\mathcal{M}_{a_0}$ and $\mathcal{M}_{a_1}$ cannot be both well founded : otherwise, their classes of ordinals would be isomorphic, which is excluded by lemma 29 and theorem 16.
Much more general results are given in [14, 16].

In order to simplify a little, we suppose that the ground model $\mathcal{M}$ satisfy V = L (this is not really necessary). The important point is the *principle of choice (PC) : there is a bijective functional between $\mathcal{M}$ and* On.
We denote by On$_{a_0}$ the class of ordinals of $\mathcal{M}_{a_0}$, which is order isomorphic to the class On of ordinals of $\mathcal{N}_\in$.

Lemma 30. $\mathcal{N} \models \exists X \forall x \exists y \{x =_\in y, \langle a_1y \in a_1X \rangle \geq a_1\}$.

For each α in On$_{a_0}$, we can choose, by WOPC, an element W_α of the class of sets extensionally equivalent to V_α. Now, the functional $\alpha \mapsto a_1W_\alpha$ from On$_{a_0}$ into $\mathcal{M}_{a_1}$ has a countable image by lemma 29. It follows that there exists α_0 such that $a_1W_\alpha = a_1W_{\alpha_0}$ for an unbounded class U of α in On$_{a_0}$.
Now, we have $\forall x \exists \alpha \{U(\alpha), x \in W_\alpha\}$ (in any model of ZF, every set belongs to some V_α) and therefore $\forall x \exists y \exists \alpha \{U(\alpha), x =_\in y, y \,\varepsilon\, W_\alpha\}$. By lemma 11, it follows that :

$\forall x \exists y \exists \alpha \{U(\alpha), x =_\in y, \langle y \in \mathrm{Cl}[W_\alpha]\rangle = 1\}$. But, by lemma 7, we have :
$a_1 = a_1\langle y \in \mathrm{Cl}[W_\alpha]\rangle = a_1\langle a_1 y \in a_1\mathrm{Cl}[a_1 W_\alpha]\rangle$ and, by $U(\alpha)$, $a_1 W_\alpha = a_1 W_{\alpha_0}$.
Therefore, we have $\forall x \exists y \exists \alpha \{U(\alpha), x =_\in y, a_1\langle a_1 y \in a_1\mathrm{Cl}[a_1 W_{\alpha_0}]\rangle = a_1\}$.
Hence the result, with $X = \mathrm{Cl}[a_1 W_{\alpha_0}]$.

Q.E.D.

Theorem 31. *There exists a generic extension $\mathcal{N}_\in[G]$ of $\mathcal{N}_\in$ which satisfies AC.*

Let $Y = \{a_1 y\,;\, \langle a_1 y \in a_1 X\rangle \geq a_1\}$: such a set exists in $\mathcal{N}$ by lemma 12.
By lemma 30, $(a_0 x, a_1 y) \mapsto a_0 x \sqcup a_1 y$ is a surjective functional from $\mathcal{M}_{a_0} \times Y$ onto the whole model $\mathcal{N}_\in$ of ZF.
Since $\mathcal{M}_{a_0} \models \mathrm{V} = \mathrm{L}$, there exists a surjective functional $\Psi : \mathrm{On} \times Y \to \mathcal{N}_\in$ and therefore $\mathcal{N}_\in$ is the union of the Z_α with α in On where Z_α is the image by Ψ of $\{\alpha\} \times Y$.
Let us consider, for each ordinal α of $\mathcal{N}_\in$, the equivalence relation $\simeq_\alpha$ on Y defined by :
$y \simeq_\alpha y' \Leftrightarrow \Psi(\alpha, y) =_\in \Psi(\alpha, y')$. These equivalence relations form a set (included in $\mathcal{P}(Y^2)$).
Thus, there exist an ordinal α_0 and for all β, a surjection $S_\beta : Z \to Z_\beta$ with $Z = \bigcup_{\alpha<\alpha_0} Z_\alpha$.
Finally, using NEPC (non extensional principle of choice) we get a surjective functional from $\mathrm{On} \times Z$ onto $\mathcal{N}_\in$ (note that, by definition, Z is a set of $\mathcal{N}_\in$).
Let us now make Z countable (or even only well ordered) by means of a generic G on $\mathcal{N}_\in$; then $\mathcal{N}_\in[G] \models \mathrm{AC}$.

Q.E.D.

Take for $(C, \leq)$ the set of conditions of $\mathcal{N}_\in$ given by theorem 31 and apply the constructions of section 3. We obtain a r.a. $\mathfrak{A}_1$ and a generic model $\mathcal{N}_\in[G]$ which satisfies AC by theorem 31.
Therefore, we have $\mathcal{N}_\in \models (\mathbf{1} \Vdash \mathrm{AC})$.

Remark. The formula $\mathfrak{C}(u)$ which defines the forcing must specify that, if $\beth 2$ is the 2-elements Boolean algebra, the set of forcing conditions is trivial (for instance a singleton). Indeed, in this case, $\mathcal{N} = \mathcal{M}_{\mathcal{D}}$ is well ordered, therefore $\mathcal{N}_\in \models \mathrm{AC}$, and there is no need to extend it.

It follows that $\Vdash (\mathbf{1} \Vdash \mathrm{AC})$ and finally $|\!|\!\vdash \mathrm{AC}$ by theorem 20. Hence the :

Theorem 32. *There exists a proof-like term Θ_{AC} of the r.a. $\mathfrak{A}_0$ such that $(\Theta_{AC}, \mathbf{1}) \,|\!|\!\vdash \mathrm{AC}$.*

More generally by theorem 21, it follows that for each axiom A of ZFC, there exists a proof-like term Θ_A of the r.a. $\mathfrak{A}_0$ such that $(\Theta_A, \mathbf{1}) \,|\!|\!\vdash A$. Note that Θ_{AC} is the only one which contains the instructions $\gamma, \kappa, \mathsf{e}$.

Example of computation with Θ_{AC}

Consider a function $f : \mathbb{N} \to 2$ such that, in the theory ZF + AC + $\mathcal{E}$, we have a proof of $\exists n^{\mathrm{int}}(f[n] = 0)$, where $\mathcal{E}$ is a set of axioms of the form :
$(\forall \vec{x} \in \mathbb{N}^k)(t_0[\vec{x}] = u_0[\vec{x}], \ldots, t_{n-1}[\vec{x}] = u_{n-1}[\vec{x}] \to t[\vec{x}] = u[\vec{x}])$
(cf. section 4, *Computing with the instruction* γ).
We denote by $\mathcal{E}_\in$ the conjunction of the corresponding set, written in the language of $\mathcal{N}_\in$:
$(\forall \vec{x} \in \mathbb{N}^k)(t_0[\vec{x}] =_\in u_0[\vec{x}], \ldots, t_{n-1}[\vec{x}] =_\in u_{n-1}[\vec{x}] \to t[\vec{x}] =_\in u[\vec{x}])$.
This proof gives a term Φ written with the only combinators $\mathsf{B}, \mathsf{C}, \mathsf{I}, \mathsf{K}, \mathsf{W}, \mathsf{cc}$ such that :
$\vdash \Phi : \mathrm{ZFC}_0, \mathcal{E}_\in \to (\exists n \in \mathbb{N})(f[n] =_\in 0)$
for some finite conjunction ZFC_0 of axioms of ZFC.
Therefore, by theorems 1, 21 and 32, we have in the r.a. $\mathfrak{A}_1$:

$(\Phi^*\Theta_{ZFC_0},\mathbf{1}) \mid\!\mid\!\vdash (\mathscr{E}_\in \to (\exists n\in\mathbb{N})(f[n] =_\in 0))$
(remember that if $t\in\Lambda$, we obtain t^* replacing $\mathsf{C},\mathsf{K},\mathsf{W},\mathsf{cc}$ by $\mathsf{C}^*,\mathsf{K}^*,\mathsf{W}^*,\mathsf{cc}^*$).
By theorem 20 applied with $F\equiv \mathscr{E}_\in \to (\exists n\in\mathbb{N})(f[n] =_\in 0)$, it follows that :
$(\chi'_F)(\Phi^*)\Theta_{ZFC_0} \Vdash \Big(\mathbf{1} \Vdash (\mathscr{E}_\in \to (\exists n\in\mathbb{N})(f[n] =_\in 0))\Big)$.
Since $\Vdash$ is a forcing on $\mathscr{N}_\in$, and F is arithmetical, we have :
$\mathrm{ZF}_\varepsilon \vdash \Big(\mathbf{1} \Vdash (\mathscr{E}_\in \to (\exists n\in\mathbb{N})(f[n] =_\in 0))\Big) \to \Big(\mathscr{E} \to \exists n^{\mathrm{int}}(f[n]=0)\Big)$.
Hence, there is a proof-like term Ξ in the r.a. $\mathfrak{A}_0$ such that :
$(\Xi)(\chi'_F)(\Phi^*)\Theta_{ZFC_0} \Vdash \mathscr{E} \to \exists n^{\mathrm{int}}(f[n]=0)$.
Now we can apply the algorithm of section 4, *Computing with the instruction γ*.

Programs for other axioms. Consider an axiom A that we can prove consistent with ZFC by forcing. Let C_0 be the set of conditions given by theorem 31 and take for $(C,\le)$ the set of conditions which gives the iterated forcing for A over C_0. Applying the constructions of section 3, we obtain a r.a. $\mathfrak{A}_1$ and a generic model $\mathscr{N}_\in[G]$ which satisfies A. It follows that $\Vdash(\mathbf{1}\Vdash A)$ and finally $\mid\!\mid\!\vdash A$ by theorem 20.

Theorem 33. *For every formula A of the language of ZF which can be proved consistent with ZFC by forcing, there exists a proof-like term Θ_A of the r.a. $\mathfrak{A}_0$ such that $(\Theta_A,\mathbf{1}) \mid\!\mid\!\vdash F$.*

Then we can use Θ_A in computations as explained above.

Final remark.

In the introdution, I said we consider the problem of turning proofs in ZFC into programs. But we must be more precise because this may seem rather easy by means of classical realizability ; indeed, here is an algorithm to transform a proof in ZFC of an arithmetical formula A into a program : first, transform it into a proof of $\mathrm{ZF}\vdash A$ by restricting its quantifiers to L or HOD. Then, get a program from this new proof using c.r.

The problem solved in the present article is more difficult and is much more interesting from the point of view of computer science : consider the program P obtained from a proof of $\mathrm{ZF}\vdash(AC\to A)$ and, *forgetting this proof,* transform directly the program P.
This is more difficult because the program P contains much less information than the proof which gave it. In fact, the interesting point is that this is possible.
You may compare with the problem of modifying a program, knowing its source code or only its compiled code. It is well known that the first situation is (very) much easier.

References

[1] S. Berardi, M. Bezem and T. Coquand. *On the computational content of the axiom of choice.* J. Symb. Logic 63, 2 p. 600-622 (1998).

[2] U. Berger and P. Oliva. *Modified bar recursion and classical dependent choice.* Proc. Logic Colloquium 2001 (Springer) p. 89-107 (2005).

[3] H.B. Curry, R. Feys. *Combinatory Logic.* North-Holland (1958).

[4] L. Fontanella, G. Geoffroy. *Preserving cardinals and weak forms of Zorn's lemma in realizability models.* Math. Struct. in Comp. Sc. 30 p. 976–996 (2020).

[5] G. Geoffroy. *Classical realizability as a classifier for nondeterminism.* LICS 2018.

[6] T. Griffin. *A formulæ-as-type notion of control.*
Conf. record 17th A.C.M. Symp. on Principles of Progr. Languages (1990).

[7] W. Howard. *The formulas–as–types notion of construction.*
Essays on combinatory logic, λ-calculus, and formalism, J.P. Seldin and J.R. Hindley ed., Acad. Press p. 479–490 (1980).

[8] T.J. Jech. *The axiom of choice.* North Holland (1973).

[9] T.J. Jech. *Set theory.* Springer (2006)

[10] A. Karagila. *Realizing realizability results with classical constructions.*
Bull. Symb. Log. 25 p. 429-445 (2019).

[11] G. Kreisel. *On the interpretation of non-finitist proofs I.*
J. Symb. Log. 16, 4 p. 241-267 (1951).

[12] G. Kreisel. *On the interpretation of non-finitist proofs II.*
J. Symb. Log. 17, 1 p. 43-58 (1952).

[13] J.-L. Krivine. *Realizability algebras II : new models of ZF + DC.*
Log. Methods Comp. Sc. 8 (1:10) p. 1-28 (2012).

[14] J.-L. Krivine. *Realizability algebras III : some examples.*
Math. Struct. in Comp. Sc. 28, 1, p. 45-76 (2018)

[15] J.-L. Krivine. *Realizability in classical logic.*
Panoramas et synthèses, Société Mathématique de France, 27, p. 197-229 (2009).

[16] J.-L. Krivine. *On the structure of classical realizability models of ZF.*
Proc. TYPES'2014 - LIPIcs 39, p. 146-161 (2015).

[17] J.-L. Krivine. *Bar recursion in classical realizability : dependent choice and continuum hypothesis.* Proc. CSL 2016, LIPIcs 62, p. 25:1-25:11 (2016).

[18] K. Kunen. *Set theory. An introduction to independence proofs.* North Holland (1992).

[19] A. Miquel. *Forcing as a program transformation.*
Logic in Computer Science (LICS'11) p. 197-206 (2011).

[20] C. Spector. *Provably recursive functionals of analysis : a consistency proof of analysis by an extension of principles in current intuitionistic mathematics.* Recursive function theory : Proc. Symp. in pure math. vol. 5, Amer. Math. Soc. p.1-27 (1962).

[21] T. Streicher. *A classical realizability model arising from a stable model of untyped λ-calculus.* Log. Methods Comp. Sc. 13, 4 (2017).