Arch. Math. Logic 40, 189–205 (2001)
Digital Object Identifier (DOI):
10.1007/s001530000057

**Mathematical Logic**

Jean-Louis Krivine

# Typed lambda-calculus in classical Zermelo-Frænkel set theory

Received: 6 September 1999 / Published online: 25 January 2001 – 

In this paper, we develop a system of typed lambda-calculus for the Zermelo-Frænkel set theory, in the framework of classical logic. The first, and the simplest system of typed lambda-calculus is the *system of simple types*, which uses the intuitionistic propositional calculus, with the only connective $\to$. It is very important, because the well known Curry-Howard correspondence between proofs and programs was originally discovered with it, and because it enjoys the *normalization property*: every typed term is strongly normalizable. It was extended to second order intuitionistic logic, in 1970, by J.-Y. Girard [4], under the name of *system F*, still with the normalization property.

More recently, in 1990, the Curry-Howard correspondence was extended to classical logic, following Felleisen and Griffin [6] who discovered that the *law of Peirce* corresponds to *control instructions* in functional programming languages. It is interesting to notice that, as early as 1972, Clint and Hoare [1] had made an analogous remark for the *law of excluded middle* and *controlled jump instructions* in imperative languages.

There are now many type systems which are based on classical logic; among the best known are the system $LC$ of J.-Y. Girard [5] and the $\lambda\mu$-calculus of M. Parigot [11]. We shall use below a system closely related to the latter, called the $\lambda_c$-calculus [8, 9]. Both systems use classical second order logic and have the normalization property.

In the sequel, we shall extend the $\lambda_c$-calculus to the Zermelo-Frænkel set theory. The main problem is due to the axiom of extensionality. To overcome this difficulty, we first give the axioms of $ZF$ in a suitable (equivalent) form, which we call $ZF_\varepsilon$.

## 1. The $ZF_\varepsilon$ set theory

This theory is written in the first order predicate calculus *without equality*, with only three binary relation symbols : $\in$, $\subset$ (which have their usual meaning), and $\varepsilon$ (which

J.-L. Krivine: U.F.R. de Mathématiques, Université Paris VII, 2 Place Jussieu, 75251 Paris Cedex 05, France. e-mail: `krivine@logique.jussieu.fr`

*Mathematics Subject Classification (2000):* 03E40, 03B40, 68N18

is a kind of “ strong membership ” relation). The formula $x = y$ is an abbreviation for $x \subset y \wedge y \subset x$. We shall use the notation $(\forall x\, \varepsilon\, a)F(x)$ for $\forall x(x\, \varepsilon\, a \to F(x))$, and $(\exists x\, \varepsilon\, a)F(x)$ for $\exists x(x\, \varepsilon\, a \wedge F(x))$.

The axioms are the following :

0. Equality and extensionality axioms.
   $\forall x \forall y[x \in y \leftrightarrow (\exists z\, \varepsilon\, y)x = z]$ ; $\forall x \forall y[x \subset y \leftrightarrow (\forall z\, \varepsilon\, x)z \in y]$.
1. Foundation scheme.
   $\forall a[(\forall x\, \varepsilon\, a)F(x) \to F(a)] \to \forall a\, F(a)$ (for every formula $F(x, x_1, \ldots, x_n)$).

The intuitive meaning of axioms 0 and 1 is that $\varepsilon$ is a well founded relation, and that the relation $\in$ is obtained by “ collapsing ” $\varepsilon$ into an extensional binary relation.

The following axioms essentially express that the relation $\varepsilon$ satisfies the axioms of Zermelo-Frænkel *except extensionality*.

2. Comprehension scheme.
   $\forall a \exists b \forall x[x\, \varepsilon\, b \leftrightarrow (x\, \varepsilon\, a \wedge F(x))]$ (for every formula $F(x, x_1, \ldots, x_n)$).

3. Pairing axiom.
   $\forall a \forall b \exists x[a\, \varepsilon\, x \wedge b\, \varepsilon\, x]$
4. Union axiom.
   $\forall a \exists b(\forall x\, \varepsilon\, a)(\forall y\, \varepsilon\, x)\; y\, \varepsilon\, b$.
5. Power set scheme.
   $\forall a \exists b \forall x(\exists y\, \varepsilon\, b)\forall z(z\, \varepsilon\, y \leftrightarrow (z\, \varepsilon\, a \wedge F(z, x)))$
   (for every formula $F(z, x, x_1, \ldots, x_n)$).
6. Collection scheme.
   $\forall a \exists b(\forall x\, \varepsilon\, a)[\exists y\, F(x, y) \to (\exists y\, \varepsilon\, b)F(x, y)]$
   (for every formula $F(x, y, x_1, \ldots, x_n)$).
7. Infinity scheme.
   $\forall a \exists b\{a\, \varepsilon\, b \wedge (\forall x\, \varepsilon\, b)[\exists y\, F(x, y) \to (\exists y\, \varepsilon\, b)F(x, y)]\}$
   (for every formula $F(x, y, x_1, \ldots, x_n)$).

**Remark.** These axioms are clearly very redundant: indeed, the power set scheme contains the comprehension scheme, and the collection scheme could easily be merged in the infinity scheme. We give the axioms in this manner only in order to show the relation with $ZF$.

Let us show that this theory is a conservative extension of $ZF + AF$ ($AF$ is the *axiom of foundation* : $\forall a(\exists x \in a)(\forall y \in x)\; y \notin a)$. In the first place, it is clear that, if $ZF_\varepsilon \vdash F$, where $F$ is a formula of $ZF$ (i.e. written only with $\in$ et $\subset$), then $ZF + AF \vdash F$; indeed, it is sufficient to notice that, if we replace $\varepsilon$ by $\in$ in $ZF_\varepsilon$, we obtain a theory equivalent to $ZF + AF$.

Conversely, we must show that each axiom of $ZF + AF$ is a consequence of $ZF_\varepsilon$ .

**Theorem 1.** *$ZF_\varepsilon \vdash a \subset a$ (and thus $a = a$).*

We use the foundation scheme (this method is called " induction on the rank of $a$ "). We assume $\forall x(x\,\varepsilon\,a \to x \subset x)$, and we must show $a \subset a$; therefore, we add the hypothesis $x\,\varepsilon\,a$. It follows that $x \subset x$, then $x = x$, and therefore $\exists y(x = y \wedge y\,\varepsilon\,a)$, that is to say $x \in a$. Thus, we have $\forall x(x\,\varepsilon\,a \to x \in a)$, and therefore $a \subset a$.

Q.E.D.

**Lemma 2.** *$ZF_\varepsilon \vdash a \subset b,\ \forall x(x \in b \to x \in c) \to a \subset c$.*

We must show $x\,\varepsilon\,a \to x \in c$, which follows from $x\,\varepsilon\,a \to x \in b$ and $x \in b \to x \in c$.

Q.E.D.

If we replace $a$ with $b$ in Lemma 2, we get

**Corollary 3.** *$ZF_\varepsilon \vdash \forall x(x \in b \to x \in c) \to b \subset c$.*

Therefore, we have proved, in $ZF_\varepsilon$, the first axiom of $ZF$, namely:

- Extensionality axiom : $\forall x \forall y(\forall z(z \in x \leftrightarrow z \in y) \to x = y))$.

**Theorem 4.** *$ZF_\varepsilon \vdash \forall y \forall z(y = a,\ a \in z \to y \in z)$; $\forall y \forall z(a \subset y,\ z \in a \to z \in y)$.*

Call $F(a)$, $F'(a)$ these two formulas. We show $F(a)$ by induction on the rank of $a$. Thus, we suppose $\forall x(x\,\varepsilon\,a \to F(x))$.

We first show $F'(a)$: by hypothesis, we have $a \subset y$, $z \in a$; thus, there exists $a'$ such that $z = a'$ and $a'\,\varepsilon\,a$, and thus $F(a')$. From $a'\,\varepsilon\,a$ and $a \subset y$, we deduce $a' \in y$. From $z = a'$ and $a' \in y$, we deduce $z \in y$ by $F(a')$.

Then, we show $F(a)$: by hypothesis, we have $y = a$, $a \in z$, thus $a = y'$ and $y'\,\varepsilon\,z$ for some $y'$. In order to show $y \in z$, it is sufficient to show $y = y'$.

Now, we have $y = a$, $a = y'$, and thus $y' \subset a$, $a \subset y$. From $F'(a)$, we get $\forall z(z \in a \to z \in y)$; from $y' \subset a$, we deduce $y' \subset y$ by Lemma 2.

We have also $y \subset a$, $a \subset y'$. From $F'(a)$, we get $\forall z(z \in a \to z \in y')$; from $y \subset a$, we deduce $y \subset y'$ by lemma 2.

Q.E.D.

With Corollary 3, we obtain:

**Corollary 5.** *$ZF_\varepsilon \vdash b \subset c \leftrightarrow \forall x(x \in b \to x \in c)$.*

It is now easy to deduce the equality axioms of $ZF$, namely:

- Equality axioms: $\forall x(x = x)$, $\forall x \forall y(x = y \to y = x)$,

$\forall x \forall y \forall z(x = y, y = z \to x = z)$,

$\forall x \forall y \forall x' \forall y'(x = x',\ y = y' \to (x \subset y \leftrightarrow x' \subset y') \wedge (x \in y \leftrightarrow x' \in y'))$.

**Remark.** The equality $=$ is an equivalence relation, which is compatible with the relations $\in$ et $\subset$ *but not with the relation $\varepsilon$.*

- Foundation axiom: as is well known, it is equivalent to the scheme

$$\forall a[\forall x(x \in a \to F(x)) \to F(a)] \to \forall a\, F(a)$$

(for every formula $F(x, x_1, \ldots, x_n)$ which is written only with $\in$ and $\subset$).

From axiom scheme 1, it is sufficient to show:

$[\forall x(x \in a \to F(x)) \to F(a)] \to [\forall x(x \,\varepsilon\, a \to F(x)) \to F(a)]$, or else $\forall x(x \,\varepsilon\, a \to F(x)) \to \forall x(x \in a \to F(x))$.
From $x \in a$, we deduce $x = x'$ and $x' \,\varepsilon\, a$ for some $x'$, thus $F(x')$, and finally $F(x)$, since $F$ is compatible with $=$.

- Comprehension scheme: $\forall a \exists b \forall x[x \in b \leftrightarrow (x \in a \wedge F(x))]$
(for every formula $F(x, x_1, \ldots, x_n)$ written with $\subset, \in$).

From the axiom scheme 2 (comprehension scheme), we get $\forall x[x \,\varepsilon\, b \leftrightarrow (x \,\varepsilon\, a \wedge F(x))]$. If $x \in b$, then $x = x'$, $x' \,\varepsilon\, b$ for some $x'$. Thus $x' \,\varepsilon\, a$ and $F(x')$. From $x = x'$ and $x' \,\varepsilon\, a$, we deduce $x \in a$. Since the axioms of equality are satisfied for $\subset$ and $\in$, and therefore for $F$, we obtain $F(x)$.
Conversely, if we have $F(x)$ and $x \in a$, we have $x = x'$ and $x' \,\varepsilon\, a$ for some $x'$. Since $F$ is compatible with equality, we get $F(x')$, thus $x' \,\varepsilon\, b$ and $x \in b$.

- Pairing axiom: $\forall x \forall y \exists z[x \in z \wedge y \in z]$.

Trivial consequence of axiom 3, and

**Lemma 6.** $ZF_\varepsilon \vdash x \,\varepsilon\, y \to x \in y$.

Trivial consequence of axioms 0 and $x = x$.
Q.E.D.

- Union axiom: $\forall a \exists b \forall x \forall y[x \in a \wedge y \in x \to y \in b]$.

From $x \in a$ we have $x = x'$ and $x' \,\varepsilon\, a$ for some $x'$; we have $y \in x$, therefore $y \in x'$, thus $y = y'$ and $y' \,\varepsilon\, x'$. From axiom 4, $x' \,\varepsilon\, a$ and $y' \,\varepsilon\, x'$, we get $y' \,\varepsilon\, b$; therefore $y \in b$, by $y = y'$.

- Power set scheme: $\forall a \exists b \forall x \exists y[y \in b \wedge \forall z(z \in y \leftrightarrow (z \in a \wedge F(z, x)))]$
(for every formula $F(z, x, x_1, \ldots, x_n)$ written with $\in$ and $\subset$).

From axiom scheme 5, we have $y \,\varepsilon\, b$, and thus $y \in b$. If $z \in y$, we have $z = z'$ and $z' \,\varepsilon\, y$ for some $z'$, therefore $z' \,\varepsilon\, a$ and $F(z', x)$, thus $z \in a$ and $F(z, x)$ (because $F$ is compatible with $=$). Conversely, if $z \in a$ and $F(z, x)$, we have $z = z'$ and $z' \,\varepsilon\, a$ for some $z'$, therefore $F(z', x)$, thus $z' \,\varepsilon\, y$ and $z \in y$.

**Remark.** The usual statement of the power set axiom is the particular case of this axiom scheme, where $F(z, x)$ is the formula $z \in x$.

- Collection scheme : $\forall a \exists b \forall x[x \in a \wedge \exists y\, F(x, y) \to \exists y(y \in b \wedge F(x, y))]$
(for every formula $F(x, y, x_1, \ldots, x_n)$ written with $\in$ and $\subset$).

From $x \in a$ and $\exists y\, F(x, y)$, we get $x = x'$, $x' \,\varepsilon\, a$ for some $x'$, and thus $\exists y\, F(x', y)$ since $F$ is compatible with $=$. From axiom scheme 6, we get $\exists y(y \,\varepsilon\, b \wedge F(x', y))$, and therefore $\exists y(y \in b \wedge F(x, y))$, because $y \,\varepsilon\, b \to y \in b$ and $F$ is compatible with $=$.

- Infinity scheme : $\forall a \exists b\{a \in b \wedge \forall x[x \in b \wedge \exists y\, F(x, y) \to \exists y(y \in b \wedge F(x, y))]\}$ (for every formula $F(x, y, x_1, \ldots, x_n)$ written with $\in$ and $\subset$).

Same proof.

**Remark.** The usual statement of the axiom of infinity is the particular case of this scheme, where $a = \emptyset$, et $F(x, y)$ is the formula $y = x \cup \{x\}$.
Q.E.D.

## 2. The $\lambda_c$-calculus

### *2.1. λ-terms*

We are given a set of *λ-variables* $x, y, \ldots$, a set of *stack constants*, and two symbols $\mathrm{cc}$ and $\mathscr{A}$. We define inductively the set $\Lambda$ of *λ-terms* by the following rules:

1. Each λ-variable $x$, and the constant $\mathrm{cc}$ are λ-terms.
2. If $t, u$ are λ-terms and $x$ is a λ-variable, then $(t)u$ and $\lambda x\, t$ are λ-terms.
3. Si $t$ is a λ-term and $\pi$ a stack constant, then $(\mathscr{A})(t)\pi$ is a λ-term.

We consider $\alpha$-equivalent λ-terms as identical. The λ-term $(t)u$ will be also denoted by $tu$; the λ-term $(\ldots((t)u_1)\ldots u_{n-1})u_n$ will be also denoted by $(t)u_1\ldots u_n$ or $tu_1\ldots u_n$.

A *stack* is a finite sequence $(t_1,\ldots,t_n,\pi)$, where $t_1,\ldots,t_n$ are λ-terms, and $\pi$ is a stack constant. The set of stacks is denoted by $\Pi$.

An expression like $(t)\pi$, where $t \in \Lambda$ and $\pi$ is a stack constant, is called a *program*. Therefore, by rule 3, we have $\mathscr{A}\tau \in \Lambda$ for every program $\tau$. If $\sigma = (t_1,\ldots,t_n,\pi)$ is a stack and $t$ is a λ-term, then the program $(tt_1\ldots t_n)\pi$ is denoted by $(t)\sigma$ or $t\sigma$. The set of programs will be denoted naturally by $\Lambda\Pi$.

**Remark.** According to the context, an expression like $t\pi$ with $t \in \Lambda$ and $\pi \in \Pi$ may represent either a program or a stack (obtained by " pushing " the λ-term $t$ on the top of the stack $\pi$).

A λ-term built by the only rules 1 and 2, i.e. which does not involve the symbol $\mathscr{A}$, or equivalently a stack constant, will be called a *classical λ-term*. The set of these terms is denoted by $\Lambda_c$. A *pure* or *intuitionistic λ-term* is a λ-term which does not involve $\mathrm{cc}$ or $\mathscr{A}$. The set of pure λ-terms is denoted by $\Lambda_i$.

The execution of a program $\tau \in \Lambda\Pi$ is the *weak* $\mathrm{cc}$*-reduction*, denoted by $\succ_c$, which is defined as follows ($t, u \in \Lambda$ are arbitrary λ-terms, and $\pi, \pi' \in \Pi$ are arbitrary stacks):

$(\lambda x\, u)t\pi \succ_c u[t/x]\pi$;
$\mathrm{cc}\, t\pi \succ_c (t\,\lambda x(\mathscr{A})(x)\pi)\pi$;
$((\mathscr{A})(t)\pi)\pi' \succ_c t\pi$.

**Remark.** These rules explain the notation for $\mathrm{cc}$ and $\mathscr{A}$, which behave respectively as the instructions `Call/cc` and `abort`, in the language SCHEME (a variant of LISP).

Now we give ourselves a subset $\perp\!\!\!\perp$ of $\Lambda\Pi$, the elements of which will be called *executable programs* or briefly *executable*. We assume that $\perp\!\!\!\perp$ is $\mathrm{cc}$*-saturated*, which means that:

$$t\pi \in \perp\!\!\!\perp, t'\pi' \succ_c t\pi \Rightarrow t'\pi' \in \perp\!\!\!\perp.$$

Let $\mathscr{Z} \subset \Pi$; we denote by $\mathscr{Z} \to \perp\!\!\!\perp$ the set $\{t \in \Lambda;\ (\forall \pi \in \mathscr{Z})\, t\pi \in \perp\!\!\!\perp\}$. Such a subset of $\Lambda$ will be called a *truth value*; we shall denote by $\mathfrak{R}_{\perp\!\!\!\perp}$ the set of truth values, i.e. $\mathfrak{R}_{\perp\!\!\!\perp} = \{\mathscr{Z} \to \perp\!\!\!\perp;\ \mathscr{Z} \subset \Pi\}$.

If $\mathscr{X}, \mathscr{Y} \subset \Lambda$, we define $\mathscr{X} \to \mathscr{Y} = \{t \in \Lambda;\ (\forall u \in \mathscr{X})\, tu \in \mathscr{Y}\}$, which is also a subset of $\Lambda$.

$\mathfrak{R}_{\perp\!\!\!\perp}$ is closed by $\to$; more precisely, if $\mathscr{X} \subset \Lambda$ and $\mathscr{X}' \in \mathfrak{R}_{\perp\!\!\!\perp}$, then $(\mathscr{X} \to \mathscr{X}') \in \mathfrak{R}_{\perp\!\!\!\perp}$: indeed, if $\mathscr{X}' = (\mathscr{Z}' \to \perp\!\!\!\perp)$, then $(\mathscr{X} \to \mathscr{X}') = (\mathscr{Z}'' \to \perp\!\!\!\perp)$, with $\mathscr{Z}'' = \{t\pi;\ t \in \mathscr{X}, \pi \in \mathscr{Z}'\}$.

$\mathfrak{R}_{\perp\!\!\!\perp}$ is also closed by arbitrary intersection: indeed, if $\mathscr{X}_i = (\mathscr{Z}_i \to \perp\!\!\!\perp)$, then $\bigcap_i \mathscr{X}_i = (\bigcup_i \mathscr{Z}_i \to \perp\!\!\!\perp)$.

The least truth value is $\Pi \to \perp\!\!\!\perp$; it is denoted by $|\bot|$.

**Definitions.** The *weak head reduction* is the least reflexive and transitive binary relation on $\Lambda$, denoted by $\succ$, such that $(\lambda x\, u)tt_1 \ldots t_n \succ u[t/x]t_1 \ldots t_n$. A subset $\mathscr{X}$ of $\Lambda$ is called *saturated* if $t \in \mathscr{X}, t' \succ t \Rightarrow t' \in \mathscr{X}$.

**Lemma 7.** *Every truth value is saturated.*

Easy consequence of the fact that $\perp\!\!\!\perp$ is CC-saturated.

Q.E.D.

## *2.2. Types*

In our system of typed $\lambda$-calculus, the *types* are the formulas of $ZF_\varepsilon$ written with the only logical symbols $\to$, $\forall$ and the three binary relation symbol $\not\varepsilon$, $\notin$ and $\subset$. Notice that $\bot$ and $=$ are not symbols of the language. They are defined as follows:

The formula $\forall x \forall y(x \not\varepsilon\, y)$ is denoted by $\bot$. The formula $x \subset y,\ y \subset x \to F$ is denoted by $x = y \to F$; $x = y$ is thus considered as an ordered pair of formulas: $(x \subset y,\ y \subset x)$.

In the same way, the formula $A \leftrightarrow B$ is considered as the ordered pair of formulas $(A \to B, B \to A)$.

The formulas $x \not\varepsilon\, y \to \bot, x \notin y \to \bot$ and $x = y \to \bot$ are denoted respectively by $x\, \varepsilon\, y$, $x \in y$ and $x \neq y$.

Let us consider a standard model $\mathscr{U}$ of $ZF + AF$. To each closed type $F(a_1, \ldots, a_n)$ with parameters in $\mathscr{U}$ (i.e. first order formula, written with the symbols $\forall$, $\to$, $\not\varepsilon$, $\notin$ and $\subset$), we associate its truth value, denoted by $|F(a_1, \ldots, a_n)|$, which is an element of $\mathfrak{R}_{\perp\!\!\!\perp}$. We write $t \Vdash F(a_1, \ldots, a_n)$ for $t \in |F(a_1, \ldots, a_n)|$; this is a first order formula $F'(t, a_1, \ldots, a_n)$ *in the language of* $ZF$ (i.e. *without* $\varepsilon$) which can be interpreted in $\mathscr{U}$. The definition is given by induction on $F$:

$|F \to G| = (|F| \to |G|)$; $|\forall x\, F| = \bigcap_a |F[a/x]|$.

Therefore:

$t \Vdash (F \to G)$ is the formula $(\forall u \in \Lambda)(u \Vdash F \to tu \Vdash G)$;

$t \Vdash \forall x\, F$ is the formula $\forall x(t \Vdash F)$.

For atomic formulas, we put:

$|a \not\varepsilon\, b| = (\{\pi \in \Pi;\ (a, \pi) \in b\} \to \perp\!\!\!\perp)$; in other words

$t \Vdash x \not\varepsilon\, y$ is the formula $(\forall \pi \in \Pi)((x, \pi) \in y \to t\pi \in \perp\!\!\!\perp)$.

Notice that, if $a \notin Cl(b)$, then $|a \not\varepsilon\, b| = \Lambda$, and therefore $|F_1, \ldots, F_k \to a \not\varepsilon\, b| = \Lambda$.

Notice also that $|\forall x \forall y(x \not\varepsilon\, y)| = \bigcap_{a,b} a \not\varepsilon\, b = \Pi \to \perp\!\!\!\perp$ which the least truth value. This explains the notation $|\bot|$ for this truth value.

The case of the two remaining atomic formulas $a \notin b$ and $a \subset b$ is less simple; it will be treated in section 4, by defining the formulas $t \Vdash x \notin y$, $t \Vdash x \subset y$ in a manner analogous to the well known definition of *forcing* in set theory [7,10]. Another method is given in section 5, by showing that there exist first order formulas $x \in y$ and $x \subset y$, which satisfy axioms 0, and *which are written with the only relation symbol* $\varepsilon$.

**Definition.** Let $F$ be a closed formula, and $t \in \Lambda$ a classical $\lambda$-term (i.e. a $\lambda$-term which does not involve the symbol $\mathscr{A}$). We shall say that $t$ *realizes* $F$ (notation $t \mid\!\mid\!\Vdash F$) if we have $t \Vdash F$ for any choice of $\mathscr{U}$ and $\perp\!\!\!\perp$.

**Remark.** In particular, taking $\perp\!\!\!\perp = \emptyset$, we see that, if $F$ involves only the relation symbols $\notin$ and $\subset$ and $t \mid\!\mid\!\Vdash F$, then $\mathscr{U} \models F$ for every universe $\mathscr{U}$, i.e. $ZF + AF \vdash F$.

A closed formula $F$ will be said *realizable* if there exists $t \in \Lambda$ such that $t \mid\!\mid\!\Vdash F$.

Realizability is compatible with deduction in classical logic. Indeed, let us define now a system of typed $\lambda$-calculus by the following rules:

1. $x_1 : A_1, \dots, x_n : A_n \vdash x_i : A_i$ $(1 \le i \le n)$.
2. $x_1 : A_1, \dots, x_n : A_n \vdash t : A,\ x_1 : A_1, \dots, x_n : A_n \vdash u : A \to B$
$\Rightarrow x_1 : A_1, \dots, x_n : A_n \vdash ut : B$.
3. $x_1 : A_1, \dots, x_n : A_n, x : A \vdash t : B$
$\Rightarrow\ x_1 : A_1, \dots, x_n : A_n \vdash \lambda x\, t : A \to B$.
4. $x_1 : A_1, \dots, x_n : A_n, k : A \to B \vdash t : A$
$\Rightarrow\ x_1 : A_1, \dots, x_n : A_n \vdash (\mathrm{CC})\lambda k\, t : A$.
5. $x_1 : A_1, \dots, x_n : A_n \vdash t : A\ \Rightarrow\ x_1 : A_1, \dots, x_n : A_n \vdash t : \forall x\, A$
if $x$ is a variable which is not free in $A_1, \dots, A_n$.
6. $x_1 : A_1, \dots, x_n : A_n \vdash t : \forall x\, A\ \Rightarrow\ x_1 : A_1, \dots, x_n : A_n \vdash t : A[y/x]$
for every variable $y$.

The rules above are exactly the deduction rules of the classical first order predicate calculus. Then we have:

**Theorem 8.** *Let $A_1, \dots, A_n, A$ be formulas, the free variables of which are among $y_1, \dots, y_p$, and let $b_1, \dots, b_p$ be sets in a model $\mathscr{U}$ of $ZF + AF$. If $x_1 : A_1, \dots, x_n : A_n \vdash t : A$ is obtained with the above rules, and if $t_1 \Vdash A_1[b_1/y_1, \dots, b_p/y_p], \dots, t_n \Vdash A_n[b_1/y_1, \dots, b_p/y_p]$, then $t[t_1/x_1, \dots, t_n/x_n] \Vdash A[b_1/y_1, \dots, b_p/y_p]$.*

In particular, if $A$ is a closed formula and $\vdash t : A$ is obtained by the above rules, then $t \mid\!\mid\!\Vdash A$.

We prove the theorem by induction on the length of the derivation of $\Gamma \vdash t : A$ ($\Gamma$ being the context $x_1 : A_1, \dots, x_n : A_n$). We shall use the notations $t'$ for $t[t_1/x_1, \dots, t_n/x_n]$, and $A'$ for $A[b_1/y_1, \dots, b_p/y_p]$. We consider the last rule used; for the sake of brevity, we shall consider only the case of rules 3 and 4.

In the case of rule 3, we have $t = \lambda x\, u$, $A = B \to C$ and $\Gamma, x : B \vdash u : C$. By the induction hypothesis, $u'[v/x] \Vdash C'$ and therefore $(\lambda x\, u')v \Vdash C'$ (lemma 7.), for every $v$ such that $v \Vdash B'$. It follows that $t' \Vdash B' \to C'$, i.e. $t' \Vdash A'$.

In the case of rule 4, we have $t = (\mathrm{CC})\lambda k\, u$ and $\Gamma, k : A \to B \vdash u : A$. By the induction hypothesis, $u'[v/k] \Vdash A'$ and therefore $(\lambda k\, u')v \Vdash A'$ (lemma 7.), for every $v$ such that $v \Vdash A' \to B'$. If we set $w = \lambda k\, u$, we have $w'v \Vdash A'$ for every such $v$.

Let $|A'| = \mathscr{X} \to \perp\!\!\!\perp$, with $\mathscr{X} \subset \Pi$. If $\pi \in \mathscr{X}$, we have $w'v\pi \in \perp\!\!\!\perp$ for every $v$ such that $v \in |A' \to B'|$.
Let $v_0 = \lambda x(\mathscr{A})(x)\pi$; if $\xi \in |A'|$, and $\pi' \in \Pi$, then $((v_0)\xi)\pi' \succ_c ((\mathscr{A})(\xi)\pi)\pi' \succ_c (\xi)\pi \in \perp\!\!\!\perp$. Since $\perp\!\!\!\perp$ is (CC)-saturated, it follows that $((v_0)\xi)\pi' \in \perp\!\!\!\perp$ for every $\pi' \in \Pi$; therefore $v_0\xi \in |\bot|$ and thus $v_0\xi \in |B'|$. Finally, we see that $v_0 \in |A' \to B'|$. It follows that $w'v_0\pi \in \perp\!\!\!\perp$, in other words $(w'\lambda x(\mathscr{A})(x)\pi)\pi \in \perp\!\!\!\perp$. Since $\perp\!\!\!\perp$ is (CC)-saturated, it follows that CC $w'\pi \in \perp\!\!\!\perp$. Since this is true for every $\pi \in \mathscr{X}$, it follows that CC $w' \in |A'|$, which is the desired result, since $t =$ CC $w$.

Q.E.D.

## 3. Realization of axioms 1 to 7 of $ZF_\varepsilon$

We will show below that the axioms of $ZF_\varepsilon$ are realizable. It will result that *the axioms of $ZF + AF$ are realizable*, since they are consequences of $ZF_\varepsilon$ in classical logic.

We first prove this for the axioms 1 to 7 of $ZF_\varepsilon$, *because we do not need for this the definitions of $|a \notin b|$ and $|a \subset b|$*, provided, of course, that $t \Vdash x \notin y$ and $t \Vdash x \subset y$ are formulas of $ZF$.

**Notation.** We shall write $\vec{t}$ for $(t_1, \dots, t_n)$ ($t_i \in \Lambda$, $n = 2$ by default), and $\vec{A}$ for $(A_1, \dots, A_n)$. Therefore, we shall write $\vec{t} \Vdash \vec{A}$ for $t_i \Vdash A_i$ ($i = 1, \dots, n$). In particular, the notation $\vec{t} \Vdash a = b$ means $t_1 \Vdash a \subset b$, $t_2 \Vdash b \subset a$; the notation $\vec{t} \Vdash A \leftrightarrow B$ means $t_1 \Vdash A \to B$, $t_2 \Vdash B \to A$.

### 3.1. Foundation scheme

**Theorem 9.** *Let* Y *be a fixed point operator, i.e.* $\mathsf{Y}\phi \succ \phi.\mathsf{Y}\phi$. *For every formula $F(x)$ with one free variable with parameters (written with the symbols $\not\varepsilon$, $\notin$, $\subset$), we have*:

$$\mathsf{Y} \Vdash \forall a[\forall x(F(x) \to x \not\varepsilon\, a), F(a) \to \bot] \to \forall a(F(a) \to \bot).$$

Indeed, let $\phi \Vdash \forall a[\forall x(F(x) \to x \not\varepsilon\, a), F(a) \to \bot]$; we show, by induction on the rank of $a$, that $\mathsf{Y}\phi \Vdash F(a) \to \bot$. In fact, if $(x, \pi) \in a$ for a stack $\pi$, we have $\mathsf{Y}\phi \Vdash F(x) \to \bot$ by induction hypothesis; thus $\mathsf{Y}\phi \Vdash F(x) \to x \not\varepsilon\, a$. If $(x, \pi) \notin a$ for every stack $\pi$, we have $|x \not\varepsilon\, a| = \Lambda$, and therefore, of course $\mathsf{Y}\phi \Vdash F(x) \to x \not\varepsilon\, a$. Finally, $\mathsf{Y}\phi \Vdash \forall x[F(x) \to x \not\varepsilon\, a]$; thus $\phi.\mathsf{Y}\phi \Vdash F(a) \to \bot$. Since $\mathsf{Y}\phi \succ \phi.\mathsf{Y}\phi$, we get $\mathsf{Y}\phi \Vdash F(a) \to \bot$ by Lemma 7.

Q.E.D.

**Remark.** The same result is easily proved for any λ-term which has the same Böhm tree as Y.

### 3.2. Comprehension scheme

Let $a$ be a set, and $F(x)$ a formula with parameters. We put $b = \{(x, t\pi); (x, \pi) \in a, t \Vdash F(x)\}$; we show $|x \not\varepsilon\, b| = |F(x) \to x \not\varepsilon\, a|$. Indeed:

$$t \Vdash x \not\varepsilon\, b \Leftrightarrow (\forall u;\ u \Vdash F(x))(\forall \pi;\ (x, \pi) \in a)tu\pi \in \perp\!\!\!\perp \Leftrightarrow$$
$$\forall u(u \Vdash F(x) \to tu \Vdash x \not\varepsilon\, a) \Leftrightarrow t \Vdash F(x) \to x \not\varepsilon\, a.$$

Therefore $(I, I) \Vdash \forall x[x \not\varepsilon\, b \leftrightarrow (F(x) \to x \not\varepsilon\, a)]$, with $I = \lambda x\, x$.

### 3.3. *Pairing axiom*

We consider two sets $a$ and $b$, and we put $c = \{a, b\} \times \Pi$. We have $t \Vdash a \notin c \Leftrightarrow t\pi \in \perp\!\!\!\perp$ for every $\pi \in \Pi$, therefore $|a \notin c| = |\perp|$, thus $I \Vdash a \,\varepsilon\, c$ ($a \,\varepsilon\, c$ is the formula $a \notin c \to \perp$). In the same way, $I \Vdash b \,\varepsilon\, c$.

### 3.4. *Union axiom*

Given a set $a$, let $b = Cl(a)$ (the least transitive set which contains $a$). We will show $|y \notin x \to x \notin a| \subset |y \notin b \to x \notin a|$: we may assume $x \in Cl(a)$, since, otherwise $|x \notin a| = \Lambda$, and thus $|y \notin b \to x \notin a| = \Lambda$. Therefore, we have $x \subset Cl(a) = b$, thus $|y \notin b| \subset |y \notin x|$. This gives immediately the result we are looking for.

It follows that $I \Vdash \forall x \forall y[(y \notin x \to x \notin a) \to (y \notin b \to x \notin a)]$.

### 3.5. *Power set scheme*

Given a set $a$, let $b = \mathscr{P}(Cl(a) \times \Pi) \times \Pi$. For every set $x$, we put $y = \{(z, t\pi);\ (z, \pi) \in a, t \Vdash F(z, x)\}$. It follows from what we have seen above (comprehension scheme) that $(I, I) \Vdash \forall z[z \notin y \leftrightarrow (F(z, x) \to z \notin a)]$.
Now, it is obvious that $y \in \mathscr{P}(Cl(a) \times \Pi)$, and therefore $(y, \pi) \in b$ for every $\pi \in \Pi$. Thus, if $t \Vdash y \notin b$, we have $t\pi \in \perp\!\!\!\perp$ for every $\pi$, and so $t \in \perp$ ; in other words, we have $|y \notin b| = |\perp|$. Therefore $I \Vdash y \,\varepsilon\, b$, and finally $(I, (I, I)) \Vdash y \,\varepsilon\, b \wedge \forall z[z \notin y \leftrightarrow (F(z, x) \to z \notin a)]$.

### 3.6. *Collection Scheme*

Given a set $a$, and an arbitrary formula $F(x, y)$, let:

$b = \bigcup\{\Phi(x, p) \times Cl(a);\ x \in Cl(a),\ p \in \Lambda\}$, with

$\Phi(x, p) = \{y$ of minimum rank ; $p \Vdash F(x, y)\}$, or $\Phi(x, p) = \emptyset$ if there is no such $y$.
We show that $|\forall y(F(x, y) \to y \notin b)| \subset |\forall y(F(x, y) \to x \notin a)|$:
Suppose indeed that $\tau \Vdash \forall y(F(x, y) \to y \notin b)$ and $p \Vdash F(x, y)$. By definition of $\Phi(x, p)$, there exists $y' \in \Phi(x, p)$. Let $\pi \in \Pi$ such that $(x, \pi) \in a$; then $x, \pi \in Cl(a)$, and therefore $(y', \pi) \in b$; it follows that $|y' \notin b| \subset |x \notin a|$. But $y' \in \Phi(x, p)$, and therefore $p \Vdash F(x, y')$; thus $\tau p \Vdash y' \notin b$, and finally $\tau p \Vdash x \notin a$.
We have proved that $I \Vdash \forall y(F(x, y) \to y \notin b) \to \forall y(F(x, y) \to x \notin a)$.

### 3.7. *Infinity scheme*

Given a set $a$, we define $b =$ the least set such that $\{a\} \times \Pi \subset b$ and $\forall x(\forall \pi \in \Pi)$ $[(x, \pi) \in b \Rightarrow \Phi(x, p) \times \Pi \subset b]$. We have $\{a\} \times \Pi \subset b$, thus $|a \notin b| = |\perp|$, and therefore $I \Vdash a \,\varepsilon\, b$.
We now show that $|\forall y(F(x, y) \to y \notin b)| \subset |\forall y(F(x, y) \to x \notin b)|$: let us assume that $\tau \Vdash \forall y(F(x, y) \to y \notin b)$, and $p \Vdash F(x, y)$. By definition of $\Phi(x, p)$, there exists $y' \in \Phi(x, p)$. We want to show that $\tau p \Vdash x \notin b$; we may assume $(x, \pi) \in b$ for some $\pi \in \Pi$, since otherwise $|x \notin b| = \Lambda$. It follows that $(y', \pi) \in b$ for every $\pi \in \Pi$, thus $|y' \notin b| = |\perp|$. Now, we have $p \Vdash F(x, y')$ and therefore $\tau p \Vdash y' \notin b$.

Therefore $\tau p \Vdash \bot$ and thus, obviously, $\tau p \Vdash x \notin b$.
It follows that $I \Vdash \forall y(F(x,y) \to y \notin b) \to \forall y(F(x,y) \to x \notin b)$ and therefore:
$(I, I) \Vdash a \,\varepsilon\, b \land \forall x[\forall y(F(x,y) \to y \notin b) \to \forall y(F(x,y) \to x \notin b)]$.

## 4. Realization of axioms 0 of $ZF_\varepsilon$

We define $|a \notin b|$ and $|a \subset b|$ in the following way:

$$|a \notin b| = \bigcap_{c \in Cl(b)} (|a \subset c|, |c \subset a| \to |c \notin b|)$$
$$|a \subset b| = \bigcap_{c \in Cl(a)} (|c \notin b| \to |c \notin a|)$$

which is a correct definition, by induction on $(rk(a) \cup rk(b), rk(a) \cap rk(b))$ ($rk(a)$ is the rank of $a$).

Then we have:

$$|a \notin b| = |\forall x(a = x \to x \notin b)| = |\forall x(a \subset x,\ x \subset a \to x \notin b)|;$$
$$|a \subset b| = |\forall x(x \notin b \to x \notin a)|.$$

Indeed

$$|\forall x(a \subset x,\ x \subset a \to x \notin b)| = \bigcap_{c}(|a \subset c|, |c \subset a| \to |c \notin b|)$$
$$= \bigcap_{c \in Cl(b)} (|a \subset c|, |c \subset a| \to |c \notin b|)$$

since $|c \notin b| = \Lambda$ when $c \notin Cl(b)$.

Therefore, we have

$$(I, I) \Vdash a \notin b \leftrightarrow \forall x(a = x \to x \notin b) \text{ and}$$
$$(I, I) \Vdash a \subset b \leftrightarrow \forall x(x \notin b \to x \notin a)$$

which is the desired result.

From these definitions, we get the following equivalences:

$$p \Vdash a \notin b \;\Leftrightarrow\; \forall x \forall \vec{r}[\vec{r} \Vdash a = x \to p\vec{r} \Vdash x \notin b];$$
$$q \Vdash a \subset b \;\Leftrightarrow\; \forall x \forall p[p \Vdash x \notin b \to qp \Vdash x \notin a].$$

or else

$$p \Vdash a \notin b \;\Leftrightarrow\; \forall \vec{r} \forall x \forall \pi[\vec{r} \Vdash a = x,\ (x, \pi) \in b \to p\vec{r}\pi \in \bot\!\!\!\bot];$$
$$q \Vdash a \subset b \;\Leftrightarrow\; \forall p \forall x \forall \pi[p \Vdash x \notin b,\ (x, \pi) \in a \to qp\pi \in \bot\!\!\!\bot].$$

With these definitions, we can find $\lambda$-terms which realize any given theorem of $ZF + AF$, since the axioms of $ZF + AF$ have been seen to be consequences of $ZF_\varepsilon$. Let us give two simple examples, namely theorems 1 and 4. We simply follow the proof of these theorems.

**Theorem 10.** *Let $\theta \in \Lambda$ such that $\theta p \succ p\theta\theta$. Then $\theta \,|\!\!\Vdash \forall x(x \subset x)$.*

The proof of $\theta \Vdash a \subset a$ is done by induction on $rk(a)$. Let $p \in \Lambda$, $p \Vdash x \notin a$; we must show that $\theta p \Vdash x \not\varepsilon a$. This is obvious if $rk(x) \geq rk(a)$, since $|x \not\varepsilon a| = \Lambda$. If $rk(x) < rk(a)$, we have $\theta \Vdash x \subset x$ by induction hypothesis, and therefore $(\theta, \theta) \Vdash x = x$. Since $p \Vdash x \notin a$, we deduce $p\theta\theta \Vdash x \not\varepsilon a$, and thus $\theta p \Vdash x \not\varepsilon a$ since $\theta p \succ p\theta\theta$ (lemma 7.).

Q.E.D.

**Notation.** The λ-term $\lambda f \lambda g \lambda x (f)(g)x$ is denoted by $f \circ g$.

**Lemma 11.** $\lambda r \lambda x\, r \circ x \Vdash \forall abc[a \subset b,\ \forall x(x \notin c \to x \notin b) \to a \subset c]$.

The proof is immediate, if we notice that $|a \subset b|$ is $|\forall x(x \notin b \to x \not\varepsilon a)|$, and $|a \subset c|$ is $|\forall x(x \notin c \to x \not\varepsilon a)|$.

Q.E.D.

It follows that $\lambda x\, \theta \circ x \Vdash \forall x(x \notin c \to x \notin b) \to b \subset c$ (put $a = b$ in Lemma 11).

**Theorem 12.** *Let* $\xi, \eta \in \Lambda$ *be such that* $\xi r p \vec{s} \succ (r)(\eta) p \vec{s}$ *and* $\eta p \vec{r} \vec{s} \succ p . r_1 \circ \xi s_1 . s_2 \circ \xi r_2$. *Then* $\xi \,|\!\!\Vdash \forall xyz[x \subset y, z \notin y \to z \notin x]$ *and* $\eta \,|\!\!\Vdash \forall xyz[y \notin z, y = x \to x \notin z]$.

We prove, by induction on $rk(a)$ that:

$\xi \Vdash \forall yz[a \subset y, z \notin y \to z \notin a]$ and $\eta \Vdash \forall yz[y \notin z, y = a \to a \notin z]$.

1. Let us suppose that $r \Vdash a \subset y$, $p \Vdash z \notin y$, and $\vec{s} \Vdash z = z'$; we want to show $\xi r p \vec{s} \Vdash z' \not\varepsilon a$. This is clear when $rk(z') \geq rk(a)$, since $|z' \not\varepsilon a| = \Lambda$. If $rk(z') < rk(a)$, we have $\eta p \vec{s} \Vdash z' \notin y$ by the induction hypothesis. But $r \Vdash a \subset y$ and $\eta p \vec{s} \Vdash z' \notin y$, thus $(r)(\eta) p \vec{s} \Vdash z' \not\varepsilon a$, which gives the desired result by Lemma 7 , since $\xi r p \vec{s} \succ (r)(\eta) p \vec{s}$.

2. Let us suppose that $p \Vdash y \notin z$, $\vec{r} \Vdash y = a$ and $\vec{s} \Vdash a = y'$; we want to show $\eta p \vec{r} \vec{s} \Vdash y' \not\varepsilon z$. But we have $r_1 \Vdash y \subset a$ and $s_1 \Vdash a \subset y'$. By 1, we get $\xi s_1 \Vdash \forall z[z \notin y' \to z \notin a]$. From Lemma 11, it follows that $r_1 \circ \xi s_1 \Vdash y \subset y'$. In the same manner, we have $s_2 \Vdash y' \subset a$ et $r_2 \Vdash a \subset y$. From 1, we get $\xi r_2 \Vdash \forall z[z \notin y \to z \notin a]$. From Lemma 11, it follows that $s_2 \circ \xi r_2 \Vdash y' \subset y$.

We have proved that $(r_1 \circ \xi s_1, s_2 \circ \xi r_2) \Vdash y = y'$. Since $p \Vdash y \notin z$, we have:

$$p . r_1 \circ \xi s_1 . s_2 \circ \xi r_2 \Vdash y' \not\varepsilon z,$$

which gives the desired result by lemma 7, since $(\eta) p \vec{r} \vec{s} \succ p . r_1 \circ \xi s_1 . s_2 \circ \xi r_2$.

Q.E.D.

## 5. Definition of ∈ and ⊂ by means of ε

This section is not used in the sequel, and may be skipped at first reading. It is devoted to a method of *defining* the formulas $x \in y$ and $x \subset y$ by means of $\varepsilon$, which is due to H. Friedman [2], and which was pointed out to me by G. Gonthier. We will use an improvement due to him of the proof in [2].

The advantage of this method is that it does not make use of the foundation axiom. Its drawback is that the λ-terms obtained in this way for axioms 0 of $ZF_\varepsilon$ are much more complicated than with the preceding method. It is the reason why we do not use it in the following sections.

It is interesting to notice that, with this method, we can define the notion of *forcing* in set theory *without using the axiom of foundation*.

We consider a first order theory, which we call $ZF^-$, *which is written with the only relation symbol* $\varepsilon$. Its axioms are the axioms 2 to 7 of the theory $ZF_\varepsilon$, but, of course, in the axiom schemes 2, 5, 6 and 7, the variable formula $F$ is now written with the only relation symbol $\varepsilon$.

Therefore, the theory $ZF^-$ is essentially the theory $ZF$ *without extensionality*. We neither assume the foundation axiom.

We shall show below, following H. Friedman [2], that this theory is equiconsistent with $ZF$. As a corollary of this proof, we obtain two formulas $\mathsf{C}(x, y)$ and $\mathsf{E}(x, y)$ with two free variables, written with the only relation symbol $\varepsilon$, such that

$ZF^- \vdash \forall x\forall y[\mathsf{C}(x, y) \leftrightarrow (\forall z\,\varepsilon\, x)\mathsf{E}(z, y)]$ and

$ZF^- \vdash \forall x\forall y[\mathsf{E}(x, y) \leftrightarrow (\exists z\,\varepsilon\, y)(\mathsf{C}(x, z) \wedge \mathsf{C}(z, x)]$

Therefore, if we define $|x \in y| = |\mathsf{E}(x, y)|$ and $|x \subset y| = |\mathsf{C}(x, y)|$, then *axioms 0 of* $ZF_\varepsilon$ *are realized* : indeed, we have already realized the axioms of $ZF^-$ (when we realized axioms 2 to 7 of $ZF_\varepsilon$, in section 3) and we know that realizability is compatible with classical deduction.

We begin by defining a predicate of equality $\equiv$ in $ZF^-$. Let $x \equiv y$ be the formula $\forall z(x\,\varepsilon\, z \to y\,\varepsilon\, z)$ (*Leibniz equality*). Then we have :

$$a \equiv b \to (F(a) \to F(b)) \text{ for every formula } F(x) \text{ with parameters.}$$

Indeed, if $a \equiv b$ and $F(a)$, take $c$ such that $a\,\varepsilon\, c$ by the pairing axiom. Then take $d$ such that $x\,\varepsilon\, d \leftrightarrow x\,\varepsilon\, c \wedge F(x)$ by the comprehension scheme. Then $a\,\varepsilon\, d$, therefore $b\,\varepsilon\, d$, and thus we get $F(b)$.
Now, if we take for $F(x)$ the formula $x \equiv a$, we obtain $a \equiv b \to b \equiv a$. Therefore, $\equiv$ is an equivalence relation which satisfy the axioms of equality.

We define now the following formulas:

$a \subseteq b$ is $(\forall x\,\varepsilon\, a)\, x\,\varepsilon\, b$ ($a$ is a subset of $b$);

$c \sim \{a, b\}$ is $\forall x(x\,\varepsilon\, c \leftrightarrow x \equiv a \vee x \equiv b)$ (given $a$ and $b$, $c$ is *some* pair $\{a, b\}$);

$b \sim \cup a$ is $\forall x(x\,\varepsilon\, b \leftrightarrow (\exists y\,\varepsilon\, a)\, x\,\varepsilon\, y)$ (given $a$, $b$ is *some* union of all the elements of $a$);

$b \sim \{x\,\varepsilon\, a\ ;\ F(x)\}$ is $\forall x(x\,\varepsilon\, b \leftrightarrow x\,\varepsilon\, a \wedge F(x))$.

**Lemma 13.** *i)* $ZF^- \vdash \forall a\exists b(b \sim \cup a)$.
*ii)* $ZF^- \vdash \forall a\forall b\exists c(c \sim \{a, b\})$.
*iii)* $ZF^- \vdash \forall a\exists b(b \sim \{x\,\varepsilon\, a\ ;\ F(x)\})$.

i) Follows immediately from the union axiom and the comprehension scheme.
ii) Follows immediately from the pairing axiom and the comprehension scheme, applied to the formula $x \equiv a \vee x \equiv b$.
iii) It is the comprehension scheme.

Q.E.D.

**Lemma 14.** $ZF^- \vdash \forall a\exists b(a \subseteq b \wedge (\forall x\,\varepsilon\, b)(\forall y\,\varepsilon\, x)\, y\,\varepsilon\, b)$ *(every set is a subset of some transitive set).*

By Lemma 13(i), we have $ZF^- \vdash \forall x\exists y(y \sim \cup x)$. Therefore, it follows from the infinity scheme that, for every set $a$, there exists a set $b$ such that $a\,\varepsilon\,b$ and $(\forall x\,\varepsilon\,b)(\exists y\,\varepsilon\,b)(y \sim \cup x)$. Let $c$ be such that $c \sim \cup b$. Then $a \subseteq c$ and $c$ is transitive : if $x'\,\varepsilon\,x\,\varepsilon\,c$, we have $x\,\varepsilon\,y\,\varepsilon\,b$, so there exists $z\,\varepsilon\,b$ such that $z \sim \cup y$. Since $x'\,\varepsilon\,x\,\varepsilon\,y$, we have $x'\,\varepsilon\,z$ and $z\,\varepsilon\,b$, and therefore $x'\,\varepsilon\,c$.

Q.E.D.

Taking $a$ such that $b\,\varepsilon\,a$ and $c\,\varepsilon\,a$ by the pairing axiom, we deduce that, given any two sets $b, c$, there exists a transitive set $d$ such that $b\,\varepsilon\,d$ and $c\,\varepsilon\,d$.

For every set $u$, we define the reflexive and symmetric binary relation $\simeq_u$ in the following way : $x \simeq_u y$ is $x \equiv y \vee (\exists a\,\varepsilon\,u)(x\,\varepsilon\,a \wedge y\,\varepsilon\,a)$.

Let $D(u)$ be the formula : $\forall x\forall y[x \simeq_u y \rightarrow (\forall x'\,\varepsilon\,x)(\exists y'\,\varepsilon\,y)x' \simeq_u y']$.

Then, we define the binary relation $\simeq$ : $x \simeq y$ is the formula $\exists u(D(u) \wedge x \simeq_u y)$. The relation $\simeq$ is clearly symmetric. It is also reflexive, as can be seen by taking for $u$ an empty set : then we have $x \simeq_u y \leftrightarrow x \equiv y$, and thus $D(u)$.

**Lemma 15.** *Let $R(x, y)$ be a reflexive and symmetric relation such that $\forall x\forall y[R(x, y) \rightarrow (\forall x'\,\varepsilon\,x)(\exists y'\,\varepsilon\,y)R(x', y')]$. Then $R(x, y) \rightarrow x \simeq y$.*

Suppose $R(x_0, y_0)$; let $A$ be a transitive set such that $x_0, y_0\,\varepsilon\,A$ (Lemma 14). Let $B$ be a set such that $(\forall x, y\,\varepsilon\,A)(\exists z\,\varepsilon\,B)(z \sim \{x, y\})$ (which is obtained by lemma 13(ii) and the collection scheme). Let $u \sim \{z\,\varepsilon\,B; (\forall x, y\,\varepsilon\,z)(x, y\,\varepsilon\,A \wedge R(x, y))\}$, which is obtained by the comprehension scheme. Then we have:

$$(\star) \qquad x \simeq_u y \leftrightarrow (x \equiv y) \vee (x, y\,\varepsilon\,A \wedge R(x, y)).$$

Indeed, if $x \simeq_u y$ et $x \not\equiv y$, we have $x, y\,\varepsilon\,z\,\varepsilon\,u$, thus $x, y\,\varepsilon\,A \wedge R(x, y)$ by definition of $u$. Conversely, if $x, y\,\varepsilon\,A \wedge R(x, y)$, there exists $z\,\varepsilon\,B$ such that $z \sim \{x, y\}$, and we have $z\,\varepsilon\,u$ by definition of $u$ (we have $R(x, x)$, $R(y, y)$, $R(x, y)$ and $R(y, x)$ because $R$ is reflexive and symmetric) thus $x \simeq_u y$.

It follows that we have $x_0 \simeq_u y_0$. Therefore, it is sufficient to prove $D(u)$ in order to deduce $x_0 \simeq y_0$. But, if $x \simeq_u y$ and $x \not\equiv y$, we have $x, y\,\varepsilon\,A$ and $R(x, y)$. If $x'\,\varepsilon\,x$, by hypothesis on $R$, there exists $y'\,\varepsilon\,y$ such that $R(x', y')$. Since $A$ is transitive, we have $x', y'\,\varepsilon\,A$, and therefore $x' \simeq_u y'$ by $(\star)$.

Q.E.D.

**Theorem 16.** *i) We have $x \simeq y \leftrightarrow (\forall x'\,\varepsilon\,x)(\exists y'\,\varepsilon\,y)(x' \simeq y') \wedge (\forall y'\,\varepsilon\,y)(\exists x'\,\varepsilon\,x)(x' \simeq y')$.*
*ii) The relation $\simeq$ is an equivalence relation.*

i) Proof of $\rightarrow$ : obvious by definition of $\simeq$.

Proof of $\leftarrow$ : let us define

$$R(x, y) \equiv (\forall x'\,\varepsilon\,x)(\exists y'\,\varepsilon\,y)(x' \simeq y') \wedge (\forall y'\,\varepsilon\,y)(\exists x'\,\varepsilon\,x)(x' \simeq y').$$

We check the hypothesis of Lemma 15: $R$ is clearly reflexive and symmetric. If we have $R(x, y)$ and $x'\,\varepsilon\,x$, then there exists $y'\,\varepsilon\,y$ such that $x' \simeq y'$. But we have just shown (proof of $\rightarrow$) that $x' \simeq y' \rightarrow R(x', y')$. Therefore we have $(\forall x'\,\varepsilon\,x)(\exists y'\,\varepsilon\,y)R(x', y')$.

From Lemma 15, we get $R(x, y) \rightarrow x \simeq y$, which is the desired result.

ii) It is sufficient to prove that $\simeq$ is transitive. Let us define $R(x, y)$ by the formula $\exists z(x \simeq z \wedge z \simeq y)$. We check the hypothesis of Lemma 15: $R$ is clearly reflexive and symmetric. If $R(x, y)$ and $x' \,\varepsilon\, x$, then $x \simeq z$ and $z \simeq y$. Thus, there exists $z' \,\varepsilon\, z$ such that $x' \simeq z'$, and $y' \,\varepsilon\, y$ such that $z' \simeq y'$. Therefore we get $R(x', y')$.
From Lemma 15, we have $R(x, y) \to x \simeq y$, which is the desired result.

Q.E.D.

We can now write the two formulas:

$\mathsf{E}(x, y) : (\exists y' \,\varepsilon\, y)(x \simeq y')$ and
$\mathsf{C}(x, y) : (\forall x' \,\varepsilon\, x)\mathsf{E}(x', y)$.

Then $\mathsf{C}(x, y)$ is the formula $(\forall x' \,\varepsilon\, x)(\exists y' \,\varepsilon\, y)\, x' \simeq y'$, and therefore $x \simeq y$ is equivalent to $\mathsf{C}(x, y) \wedge \mathsf{C}(y, x)$ by theorem 16. Therefore, we have $\mathsf{E}(x, y) \leftrightarrow (\exists y' \,\varepsilon\, y)(\mathsf{C}(x, y') \wedge \mathsf{C}(y', x))$.

We have $x \,\varepsilon\, y \to \mathsf{E}(x, y)$ since $\simeq$ is reflexive. Therefore, if we define $x \in y$ by $\mathsf{E}(x, y)$ and $x \subset y$ by $\mathsf{C}(x, y)$, it is easy to show that the axioms of $ZF$ (without foundation) are satisfied : you only have to repeat the proof, already done, that the axioms of $ZF$ are consequences of $ZF_\varepsilon$, beginning at the comprehension scheme.

## 6. Typed λ-calculus in $ZF$

We add the following symbols of function to the language of $ZF_\varepsilon$: $\cup$, $\mathscr{P}$ (unary symbols), $\{\}$ (binary symbol), $\phi_F$, $\psi_F$, $\chi_F$ (for each formula $F$), the arity of which depends on $F$ : if $F$ is written $F(x, x_1, \ldots, x_n)$ with a particular variable $x$ ($x_1, \ldots, x_n$ are *parameters*), then $\phi_F$ has the arity $n + 1$. For brevity, we write $F(x)$ for $F(x, x_1, \ldots, x_n)$, and $\phi_F(a)$ for $\phi_F(a, x_1, \ldots, x_n)$. In the same way, if $F$ is written $F(x, y, x_1, \ldots, x_n)$ with two particular variables $x$ and $y$ (we write it $F(x, y)$), then $\psi_F$ is of arity $(n + 1)$ (we write $\psi_F(a)$ for $\psi_F(a, x_1, \ldots, x_n)$) ; the same for $\chi_F$.
We take the typing rules of the $\lambda_c$-calculus (at the end of section 2), with the sixth rule modified in the following way:

6. $x_1 : A_1, \ldots, x_n : A_n \vdash t : \forall x\, A \;\Rightarrow\; x_1 : A_1, \ldots, x_n : A_n \vdash t : A[\tau/x]$
for every term $\tau$ built with the function symbols $\cup$, $\mathscr{P}$, $\{\}$, $\phi_F$, $\psi_F$, $\chi_F$.

We add the following rules, one for each axiom of $ZF_\varepsilon$; we use the symbol $\vdash_\varepsilon$ to denote this new system of types; $x$ is a λ-variable; $a, b, y, z$ are set theoretic variables:

0. Equality and extensionality axioms
$x : a \notin b \vdash_\varepsilon x : \forall z(a \subset z, z \subset a \to z \not\varepsilon\, b)$ and
$x : \forall z(a \subset z, z \subset a \to z \not\varepsilon\, b) \vdash_\varepsilon x : a \notin b$ ;
$x : a \subset b \vdash_\varepsilon x : \forall z(z \notin b \to z \not\varepsilon\, a)$ and $x : \forall z(z \notin b \to z \not\varepsilon\, a) \vdash_\varepsilon x : a \subset b$.

1. Foundation scheme
$\vdash_\varepsilon \mathsf{Y} : \forall a[\forall z(F(z) \to z \not\varepsilon\, a), F(a) \to \bot] \to \forall a(F(a) \to \bot)$
(for every formula $F(z, x_1, \ldots, x_n)$).

2. Comprehension scheme
$x : z \not\varepsilon\, \phi_F(a) \vdash_\varepsilon x : F(z) \to z \not\varepsilon\, a$ and $x : F(z) \to z \not\varepsilon\, a \vdash_\varepsilon x : z \not\varepsilon\, \phi_F(a)$
(for every formula $F(z, x_1, \ldots, x_n)$).

3. Pairing axiom
$x : a \notin \{a, b\} \vdash_\varepsilon x : \bot$ and $x : b \notin \{a, b\} \vdash_\varepsilon x : \bot$.

4. Union axiom
$x : y \notin z \to z \notin a \vdash_\varepsilon x : y \notin \cup a \to z \notin a$.

5. Power set scheme
$x : \phi_F(a) \notin \mathscr{P}(a) \vdash_\varepsilon x : \bot$ (for every formula $F(z, x_1, \ldots, x_n)$).

6. Collection scheme
$x : \forall z(F(y, z) \to z \notin \psi_F(a)) \vdash_\varepsilon x : \forall z(F(y, z) \to y \notin a)$
(for every formula $F(y, z, x_1, \ldots, x_n)$).

7. Infinity scheme
$x : a \notin \chi_F(a) \vdash_\varepsilon x : \bot$;
$x : \forall z(F(y, z) \to z \notin \chi_F(a)) \vdash_\varepsilon x : \forall z(F(y, z) \to y \notin \chi_F(a))$
(for every formula $F(y, z, x_1, \ldots, x_n)$).

From the above, it follows that theorem 8 remains true with these new typing rules. In particular:

**Theorem 17.** *If $A$ is a closed formula and $\vdash_\varepsilon t : A$, then $t \mid\mid\!\!\vdash A$.*

**Remark.** i) In this system of types, for every formula $A$ we have:
$x : \bot \vdash_\varepsilon \lambda x_1 \ldots \lambda x_n\, x : A$ for some integer $n$.
This is easily proved by induction on $A$, remembering that $\bot$ is $\forall x \forall y(x \notin y)$: for an atomic formula $A$, this is trivial if $A$ is $t \notin u$, and this follows from rules 0 above if $A$ is $t \notin u$ or $t \subset u$. The cases where $A \equiv B \to C$ or $A \equiv \forall x\, B$ are trivial.
But, since $|\bot| \subset |A|$ for every formula $A$, we might use the following simpler rule:
$x : \bot \vdash_\varepsilon x : A$ for every formula $A$
and the theorem 17 remains valid.
ii) In this type system, the axioms of $ZF_\varepsilon$ are " inhabited " by very simple $\lambda$-terms, in fact $\lambda x\, x$ or Y. But this is no longer the case for the axioms of $ZF + AF$, since these axioms are *theorems* of $ZF_\varepsilon$ which are not completely trivial. For example, the power set axiom of $ZF$ can be written as $\forall x(x \subset a \to x \in \mathscr{P}(a))$, and it appears that no intuitionistic $\lambda$-term (i.e. not involving CC) realizes it.

## 7. Normalization properties

It is easy to see that no general normalization theorem is possible for this typed $\lambda$-calculus. Consider, for example, the following simple theorem, which uses only the comprehension scheme :

**Theorem 18.** *Let $F(y)$ be the formula $y \notin y$, and $\delta = \lambda x(x)x$. Then:*
$\vdash_\varepsilon \delta\delta : \forall x(\phi_F(x) \notin x)$.

Let $b$ be $\phi_F(a)$; then, we have $x : y \notin b \vdash_\varepsilon x : y \notin y \to y \notin a$. Therefore $x : b \notin b \vdash_\varepsilon x : b \notin b \to b \notin a$. Thus, $x : b \notin b \vdash_\varepsilon xx : b \notin a$, and therefore $\vdash_\varepsilon \delta : b \notin b \to b \notin a$. It follows that $\vdash_\varepsilon \delta : b \notin b$, and thus $\vdash_\varepsilon \delta\delta : b \notin a$.

Q.E.D.

In fact, it can be proved that, if any $\lambda$-term $\tau$ is such that $\vdash_\varepsilon \tau : \forall x(\phi_F(x) \notin x)$, this typing being obtained without using the foundation scheme, then $\tau$ has the same reduction behaviour as $\delta\delta$.

Nevertheless, the important fact is that *this typed λ-calculus leads to correct computations*, as far as data types are concerned. This is shown by the following theorems, about booleans and integers.

Consider first two symbols of constant 0 and 1, that we add to the language of $ZF_\varepsilon$. The formula $\forall X(1 \notin X, 0 \notin X \to x \notin X)$ is denoted by $Bool(x)$ (read " $x$ is a Boolean ").

**Theorem 19.** *If* $\vdash_\varepsilon \tau : Bool(1)$*, then for any λ-terms* $t, u$ *and any stack* $\pi$*, we have* $\tau t u \pi \succ_c t\pi$*. In other words,* $\tau$ *behaves like the boolean* $\lambda x \lambda y\, x$*. Of course, the same result holds for the formula* $Bool(0)$*.*

We take a model $\mathscr{U}$ such that $0 \neq 1$. Define $\perp\!\!\!\perp = \{\xi \in \Lambda\Pi \,;\, \xi \succ_c t\pi\}$, and $X = \{(1, \pi)\}$. Then $t \Vdash 1 \notin X$, and every λ-term realizes $0 \notin X$. From theorem 17., we get $\tau \Vdash Bool(1)$. It follows that $\tau t u \Vdash 1 \notin X$, which means that $\tau t u \pi \in \perp\!\!\!\perp$.
Q.E.D.

Consider now a symbol of constant 0, and a unary function symbol $s$, that we add to the language of $ZF_\varepsilon$. The formula $\forall X[\forall y(y \notin X \to sy \notin X), 0 \notin X \to x \notin X]$ is denoted by $Int(x)$ (read " $x$ is an integer ").

A simple method for computing classical integers has been given by M. Parigot, in the framework of second order logic and $\lambda\mu$-calculus. The following theorem shows that it remains valid in the typed λ-calculus in $ZF$.

**Theorem 20.** *Let* $n \in \mathbb{N}$ *and* $\tau \in \Lambda$*. If* $\vdash_\varepsilon \tau : Int(s^n 0)$*, then* $\tau$ *represents the classical Church integer* $n$ *in the sense of [8, 9]. In particular,* $((\tau)\lambda f\, f \circ \sigma)\phi t \pi \succ_c ((\phi)(\sigma)^n t)\pi$ *for every λ-terms* $\sigma, \phi, t$ *and every stack* $\pi$*.*

Let us only prove the last assertion. Take a model $\mathscr{U}$ in which the interpretation of $s$ and 0 are such that $sy \neq 0$ and $sy = s^{k+1}0 \to y = s^k 0$ for all $y$. Define $\perp\!\!\!\perp = \{\xi \in \Lambda\Pi \,;\, \xi \succ_c ((\phi)\sigma^n t)\pi\}$ and $X = \{(0, \sigma^n t\pi), \ldots (s^k 0, \sigma^{n-k} t\pi), \ldots, (s^n 0, t\pi)\}$.

Therefore, we have $\phi \Vdash 0 \notin X$. Let us show that $\lambda f\, f \circ \sigma \Vdash \forall y(y \notin X \to sy \notin X)$ : this is clear if $sy \neq 0, \ldots, s^n 0$, since then $|sy \notin X| = \Lambda$. If $sy = s^j 0$, then $j = k+1$ et $y = s^k 0 (0 \leq k < n)$. Suppose that $u \Vdash y \notin X$ ; thus, we have $((u)\sigma^{n-k} t)\pi \in \perp\!\!\!\perp$. But, if we set $v = (\lambda f\, f \circ \sigma)u$, we have $((v)\sigma^{n-k-1} t)\pi \succ_c ((u)\sigma^{n-k} t)\pi$, and therefore $((v)\sigma^{n-k-1} t)\pi \in \perp\!\!\!\perp$. This shows that $v \Vdash s^{k+1} 0 \notin X$, and we have proved that $\lambda f\, f \circ \sigma \Vdash s^k 0 \notin X \to s^{k+1} 0 \notin X$.

From theorem 17., we get $\tau \Vdash Int(s^n 0)$. It follows that $(\tau \lambda f\, f \circ \sigma)\phi \Vdash s^n 0 \notin X$, and therefore $(\tau \lambda f\, f \circ \sigma)\phi t \pi \in \perp\!\!\!\perp$, which is the desired result.
Q.E.D.

## References

1. Clint, M., Hoare, C.A.: Program proving: Jumps and functions. Acta informatica 1, 214–224 (1972)
2. Friedman, H.: The consistency of classical set theory relative to a set theory with intuitionistic logic. Journal of Symb. Logic, **38**(2), 315–319 (1973)

3. Friedman, H.: Classically and intuitionistically provably recursive functions. In: Higher set theory. Springer Lect. Notes in Math., **669**, 21–27 (1977)
4. Girard, J.-Y.: Une extension de l'interprétation de Gödel à l'analyse. In: Proc. 2nd Scand. Logic Symp. p. 63–92. North Holland Pub. Co. (1971)
5. Girard, J.-Y.: A new constructive logic: classical logic. Mathematical Structures in Computer Science, **1**, 255–296 (1991)
6. Griffin, T.: A formulæ-as-type notion of control. In Conference Record of the 17th A.C.M. Symposium on principles of Programming Languages (1990)
7. Jech, T.J.: Set theory. Academic Press (1978)
8. Krivine, J.-L.: Classical logic, storage operators and second order λ-calculus. Ann. of Pure and Appl. Log. **68**, 53–78 (1994)
9. Krivine, J.-L.: A general storage theorem for integers in call-by-name λ-calculus. Theor. Comp. Sc. **129**, 79–94 (1994)
10. Krivine, J.-L.: Théorie des ensembles. Cassini, éd. (1998)
11. Parigot, M.: $\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction. Proc. Logic Progr. and Autom. Reasoning, St Petersbourg. L.N.C.S. **624**, 190–201 (1992)