50 years after forcing, the Curry-Howard correspondence gives new models of ZF

Jean-Louis Krivine

PPS Group, University Paris-Diderot, CNRS

krivine@pps.univ-paris-diderot.fr

Institut Henri Poincaré, Paris, April 2014

Introduction

The topic of these talks is a technique called *classical realizability*,
which gives rise to new models of set theory, which I call *realizability models*.
It was made possible by the discovery by Tim Griffin, in 1990,
of the interpretation of the *excluded middle* by means of a *control instruction.*

I want to insist on the importance and strangeness of this discovery
which connects one of the oldest mode of mathematical reasoning
with a very sophisticated programming instruction.
What could Euclid know about the use of continuations in SCHEME ?
This is at least as surprising as the Gödel incompleteness theorem,
and like this theorem, it has certainly deep philosophical implications.

Introduction

The realizability models of ZF are interesting for several reasons :

- They are the first new models of ZF, fifty years after Cohen's forcing.
- They use thoroughly computer science methods :
  λ-calculus and combinatory logic, virtual machines, environments,
  technical programming instructions and methods, etc.
- Conversely, they give new insights about programming,
  by extending the Curry-Howard correspondence to set-theoretical proofs.
  We have to solve what I call the *specification problem* :
  what is the specification associated with a given theorem ?
  The aim is to obtain, in this way, useful secure programs.

Introduction

- These models also give us new insights about set theory :
  They emphasize the role of the *extensionality axiom*.
  This axiom is, by far, the most difficult to handle,
  much more than the excluded middle (given Griffin's result).
  Indeed, it is the only one for which no program can be found.
- They suggest that the only natural axiom of choice is *dependent choice* :
  indeed, up to now, in every non trivial example, *DC is true and AC is false*.
  Therefore, it is not wise to consider ZFC as the standard set theory.

Introduction

Forcing is a particular (in fact degenerate) case of classical realizability.

The *realizability models* of ZF are *much more* complicated than *forcing models* :

they are not an extension of the ground model ;

the ordinals and even *the integers* are changed ;

the axiom of choice *is not* preserved, only dependent choice may be.

The main tools are :

- Syntax : ZF_ε set theory which is a conservative extension of ZF ;

we introduce a strong membership relation ε which lacks extensionality ;
indeed, extensionality axiom cannot be directly realized.

- Semantics : Realizability algebra which is a three-sorted extension

of the well known combinatory algebra ; indeed, we have to manage
not only programs, but also environments and machine execution.

Realizability algebras

It is a 3-sorted first order structure, which consists of :

- *Three sets* : Λ the set of *terms* (programs), Π the set of *stacks* (environments),
  $\Lambda \star \Pi$ the set of *processes* (executable).
- *Six distinguished terms* : B, C, I, K, W, cc (*elementary combinators*).
- *Four operations* :
  Application : $\Lambda \times \Lambda \to \Lambda$ denoted $(\xi)\eta$, (or often $\xi\eta$) where ξ, η are terms ;
  Push : $\Lambda \times \Pi \to \Pi$ denoted $\xi . \pi$, where π is a stack ;
  Continuation : $\Pi \to \Lambda$ denoted k_π ;
  Process : $\Lambda \times \Pi \to \Lambda \star \Pi$ denoted $\xi \star \pi$.
- *A preorder on processes*, denoted $\succ$ (*execution*)
- *A distinguished subset* $\perp\!\!\!\perp$ of $\Lambda \star \Pi$ such that : $p \notin \perp\!\!\!\perp, p \succ p' \Rightarrow p' \notin \perp\!\!\!\perp$.
- *A distinguished subset* PL of Λ (*proof-like terms*) such that :
  B, C, I, K, W, cc $\in$ PL ; $\xi, \eta \in \mathrm{PL} \Rightarrow \xi\eta \in \mathrm{PL}$; $(\forall \xi \in \mathrm{PL})(\exists \pi \in \Pi)(\xi \star \pi \notin \perp\!\!\!\perp)$.

Axioms of realizability algebra

The preorder $\succ$ represents *execution in a weak head reduction machine* :

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

Remark. The usual set {K,S} of combinators does not work to interpret *weak head reduction* of λ-calculus.

A Curry-style translation of λ-calculus

A *c-term* is a term of the language of realizability algebras
built with variables $x, y, \ldots,$ elementary combinators and application.
Each closed c-term has a value in Λ which is *proof-like*.
Examples : *integers* in combinatory logic.
$\sigma = (\mathsf{BW})(\mathsf{B})\mathsf{B}$ (the *successor*) ; $\underline{0} = \mathsf{KI}$; $\underline{n+1} = (\sigma)\underline{n}$
Let t be a c-term and x a variable ; define inductively a c-term written $\Lambda x\, t$:

- $\Lambda x\, t = (\mathsf{K})\, t$ if x is not in t
- $\Lambda x\, x = \mathsf{I}$
- $\Lambda x\, tu = (\mathsf{C}\Lambda x\, t)\, u$ if x is in t but not in u
- $\Lambda x\, tx = t$ if x is not in t
- $\Lambda x\, tx = (\mathsf{W})\Lambda x\, t$ if x is in t
- $\Lambda x(t)(u)v = \Lambda x(\mathsf{B})\, tuv$ if x is in uv

We now define our translation of λ-calculus, by setting : $\lambda x\, t = \Lambda x(\mathsf{I})\, t$.

A Curry-style translation of λ-calculus

The rewriting of $\Lambda x\, t$ is finite because :

- no combinator is introduced inside t, but only in front of it ;
- the only changes in t are : moving parentheses, erasing occurrences of x ;
- each rule decreases the part of t which is under Λx ;
- except for the last rule, this decrease is *strict* ;
- the last rule can be applied consecutively only finitely many times because the length of the argument strictly decreases (from $(u)v$ to v).

Weak head reduction

Theorem. Let $t[x_1,\ldots,x_n]$ be a c-term and $\xi_1,\ldots,\xi_n \in \Lambda$. Then

$\lambda x_1 \ldots \lambda x_n\, t \star \xi_1 . \ldots . \xi_n . \pi \succ t[\xi_1/x_1,\ldots,\xi_n/x_n] \star \pi.$

Easily proved, by induction on the length of the rewriting of t.

The usual KS -translation does not satisfy the theorem. For instance :

$\lambda x(x)xx \star \xi . \pi \equiv ((\mathsf{S})(\mathsf{S})\mathsf{I}\,\mathsf{I})\,\mathsf{I} \star \xi . \pi \succ \mathsf{S}\,\mathsf{I}\,\mathsf{I} \star \xi . \mathsf{I}\xi . \pi \succ \xi \star \mathsf{I}\xi . \mathsf{I}\xi . \pi$ instead of $(\xi)\xi\xi \star \pi$.

The above Curry-style translation gives :

$\lambda x(x)xx \star \xi . \pi \equiv (\mathsf{W})(\mathsf{W})(\mathsf{B})(\mathsf{B})\mathsf{I} \star \xi . \pi \succ \mathsf{B} \star \mathsf{BI} . \xi . \xi . \xi . \pi \succ (\xi)\xi\xi \star \pi$

We use λ-calculus only as a convenient way of writing c-terms.

Combinatory algebra is a very low level programming language
(it compares with *machine language*)

λ-calculus is of somewhat higher level (it compares with *assembly language*).

The formal system for ZF_ε

We use first order logic with the only connectives $\top, \bot, \to, \forall$, some function symbols, three binary relation symbols $\not\varepsilon, \notin, \subseteq$ and the usual rules of natural deduction :

- $x_1{:}A_1, \ldots, x_n{:}A_n \vdash x_i{:}A_i$
- $x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}A \to B, \quad x_1{:}A_1, \ldots, x_n{:}A_n \vdash u{:}A \quad \Rightarrow \quad x_1{:}A_1, \ldots, x_n{:}A_n \vdash (t)u{:}B$
- $x_1{:}A_1, \ldots, x_n{:}A_n, x{:}A \vdash t{:}B \quad \Rightarrow \quad x_1{:}A_1, \ldots, x_n{:}A_n \vdash \lambda x\, t{:}A \to B$
- $x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}A \quad \Rightarrow \quad x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}\forall x\, A$ (x is not in $A_1, \ldots, A_n$)
- $x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}\forall x\, A \quad \Rightarrow \quad x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}A[\tau/x]$
  (τ is a *ℓ-term* of ZF_ε, i.e. a term built with variables and function symbols)
- $x_1{:}A_1, \ldots, x_n{:}A_n \vdash \mathsf{cc}{:}((A \to B) \to A) \to A$ (law of Peirce)
- $x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}\bot \quad \Rightarrow \quad x_1{:}A_1, \ldots, x_n{:}A_n \vdash t{:}A$

Notation. We write $F_1, \ldots, F_k \to F$ for $F_1 \to (F_2 \to \cdots \to (F_k \to F) \cdots)$
and $\exists x\{F_1, \ldots, F_k\}$ for $\forall x(F_1, \ldots, F_k \to \bot) \to \bot$.

Axioms of ZF$_\varepsilon$ set theory

The axioms of ZF$_\varepsilon$ essentially say that ε is a well founded relation and that its extensional collapse $\in$ satisfies ZF.

- Foundation scheme : $\forall\vec{z}\big(\forall x\big((\forall y\,\varepsilon\,x)F[y,\vec{z}] \to F[x,\vec{z}]\big) \to \forall a\,F[a,\vec{z}]\big)$
  for every formula $F[x,\vec{z}]$.
- Collapse : $\forall x\forall y\big(x \in y \leftrightarrow (\exists z\,\varepsilon\,y)\{x \subseteq z, z \subseteq x\}\big)$; $\forall x\forall y\big(x \subseteq y \leftrightarrow (\forall z\,\varepsilon\,x)z \in y\big)$
- Comprehension scheme : $\forall\vec{z}\forall a\exists b\forall x(x\,\varepsilon\,b \leftrightarrow (x\,\varepsilon\,a \wedge F[x,\vec{z}]))$
- Pairing : $\forall a\forall b\exists x\{a\,\varepsilon\,x, b\,\varepsilon\,x\}$
- Union : $\forall a\exists b(\forall x\,\varepsilon\,a)(\forall y\,\varepsilon\,x)\,y\,\varepsilon\,b$
- Power set : $\forall a\exists b\forall x(\exists y\,\varepsilon\,b)\forall z(z\,\varepsilon\,y \leftrightarrow (z\,\varepsilon\,a \wedge z\,\varepsilon\,x))$
- Collection scheme : $\forall\vec{z}\forall a\exists b(\forall x\,\varepsilon\,a)\big(\exists y\,F[x,y,\vec{z}] \to (\exists y\,\varepsilon\,b)F[x,y,\vec{z}]\big)$
- Infinity scheme : $\forall\vec{z}\forall a\exists b\big\{a\,\varepsilon\,b, (\forall x\,\varepsilon\,b)\big(\exists y\,F[x,y,\vec{z}] \to (\exists y\,\varepsilon\,b)F[x,y,\vec{z}]\big)\big\}$

A conservative extension of ZF. But, unlike ZF, function symbols are essential.

Realizability models of ZF$_\varepsilon$

We start with an ordinary model $\mathscr{M}$ of ZFC, called the *ground model*.

Its elements are called *individuals* (to avoid the word *set*, as far as possible).

The formulas of ZF (i.e. without $\not\varepsilon$) are interpreted in $\mathscr{M}$ (*true or false*).

The *realizability model* $\mathscr{N}$ has the *same domain* as $\mathscr{M}$.

The function symbols have the same interpretation as in $\mathscr{M}$.

The formulas of ZF$_\varepsilon$ are interpreted in $\mathscr{N}$, but *with truth values in* $\mathscr{P}(\Pi)$.

Although $\mathscr{M}$ and $\mathscr{N}$ have the same domain (which means that
the quantifier $\forall x$ describes the same domain for both)
$\mathscr{N}$ has *more individuals* than $\mathscr{M}$ because some of them are *not named*.

For instance, in the "thread model" below, there are necessarily
non standard integers in $\mathscr{N}$, i.e. integers which are not named in $\mathscr{M}$.

Therefore, realizability models *are not* forcing models.

Realizability models of ZF_ε

For each closed formula F of ZF_ε with parameters $a_1, \ldots, a_n$ in $\mathcal{M}$
we define its *truth value* $|F| \subset \Lambda$ and its *falsity value* $\|F\| \subset \Pi$.
$\xi \in |F|$ is read *ξ realizes F* and is written $\xi \Vdash F$.
These values are connected by the relation : $\xi \in |F| \Leftrightarrow (\forall \pi \in \|F\|)(\xi \star \pi \in \perp\!\!\!\perp)$
so that we only need to define the falsity value $\|F\|$, by induction :

- F is atomic ;

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

$\|a \subseteq b\|, \|a \notin b\|$ are defined by induction on the ranks of a, b :

$\|a \subseteq b\| = \bigcup_c \{\xi \bullet \pi;\ \xi \in \Lambda,\ \pi \in \Pi,\ (c,\pi) \in a,\ \xi \Vdash c \notin b\}$;

$\|a \notin b\| = \bigcup_c \{\xi \bullet \xi' \bullet \pi;\ \xi, \xi' \in \Lambda,\ \pi \in \Pi,\ (c,\pi) \in b,\ \xi \Vdash a \subseteq c,\ \xi' \Vdash c \subseteq a\}$.

- $F \equiv A \to B$; then $\|F\| = \{\xi \bullet \pi\ ;\ \xi \Vdash A,\ \pi \in \|B\|\}$
- $F \equiv \forall x\, A$; then $\|F\| = \bigcup_a \|A[a/x]\|$

Realizability models of ZF_ε

The following *adequacy lemma* is an essential tool.

Theorem. If $x_1 : A_1, \ldots, x_n : A_n \vdash t : A$ and $\xi_1 \Vdash A_1, \ldots, \xi_n \Vdash A_n$ then $t[\xi_1/x_1, \ldots, \xi_n/x_n] \Vdash A$. In particular, if $\vdash t : A$, then $t \Vdash A$.

We say that *the model $\mathcal{N}$ realizes F* if there is a *proof-like term θ* s.t. $\theta \Vdash F$.

Notation : $\mathcal{N} \Vdash F$ or even $\Vdash F$.

By adequacy, the class of realized formulas is closed by classical deduction.

Moreover, it is *coherent*, i.e. $\perp$ *is not realized* because :

For every proof-like term θ, there is a stack π such that $\theta \star \pi \notin \perp\!\!\!\perp$

Indeed, this is an axiom of realizability algebras.

Remark. If $\perp\!\!\!\perp \neq \emptyset$ i.e. $\xi \star \pi \in \perp\!\!\!\perp$, then $\mathrm{k}_\pi \xi \Vdash \perp$; thus, *any formula has realizers*.

Theorem. The axioms of ZF_ε , and thus also the axioms of ZF, are realized.

Therefore, the realizability model gives an ordinary model of ZF_ε and ZF.

We can obtain, in this way, *relative consistency results.*

Forcing and parallel or

The ordered sets used in forcing are degenerate cases of realizability algebras :

$\Lambda = \Pi = \Lambda \star \Pi$ is a meet-semi-lattice with a greatest element I ;

the binary operations *application, push, process* are all identical with the meet ;

the unary operation of *continuation* is the identity ;

the elementary combinators *B, C, I, K, W,* cc are all identical with *I*.

The corresponding realizability models are the *forcing models*,

which have been deeply investigated since 1963.

We will not consider them here, because they have *no programming content*.

They are characterized by the :

Theorem. A realizability algebra gives only forcing models iff there is a *parallel or*, i.e. a proof-like term e such that :

$$\xi \star \pi \in \perp\!\!\!\perp \text{ or } \eta \star \pi \in \perp\!\!\!\perp \;\Rightarrow\; \mathsf{e} \star \xi \centerdot \eta \centerdot \pi \in \perp\!\!\!\perp.$$

Equality

In the realizability model we have two notions of *equality* :

- The *strong* or *Leibniz* equality $x = y$ which is $\forall z(x \not\varepsilon z \to y \not\varepsilon z)$.

We have $\Vdash \forall x \forall y(x = y, F[x] \to F[y])$ for *every* formula F of ZF_ε.

- The *extensional* equality $x \simeq y$, which is $x \subseteq y, y \subseteq x$.

We have $\Vdash \forall x \forall y(x \simeq y, F[x] \to F[y])$ for every formula F *of ZF* (i.e. without the symbol $\not\varepsilon$).

Each function symbol f on $\mathscr{M}$ extends immediately to $\mathscr{N}$, with the same values on *named* individuals. ZF_ε remains satisfied with the extended language.
On the other hand, to satisfy ZF, we must check that f is *compatible with* $\simeq$:

$$\Vdash \forall x \forall y(x \simeq y \to f x \simeq f y)$$

or else $$\Vdash \forall x \forall y(x \subseteq y, y \subseteq x \to f x \subseteq f y)$$

Equality

In order to compute more easily with Leibniz equality, we introduce the symbol $\neq$:

$\|a \neq b\| = \Pi = \|\bot\|$ if $a = b$; $\|a \neq b\| = \emptyset = \|\top\|$ if $a \neq b$.

Then $x = y$ is defined as $x \neq y \to \bot$. It is equivalent with Leibniz equality ; indeed :

Theorem.

i) $\mathsf{I} \Vdash \forall z(a \notin z \to b \notin z), a \neq b \to \bot$;

ii) $\lambda x \lambda y(\mathrm{cc})\lambda k(x)(k)y \Vdash (a \neq b \to \bot) \to \forall z(a \notin z \to b \notin z)$.

i) Let $\xi \Vdash \forall z(a \notin z \to b \notin z), \eta \Vdash a \neq b$ and $\pi \in \Pi$. We must show $\xi \star \eta \centerdot \pi \in \perp\!\!\!\perp$.

If $a \neq b$, then $\|\forall z(a \notin z \to b \notin z)\| = \|\top \to \bot\|$ (take $z = \{b\} \times \Pi$).

Therefore $\xi \Vdash \top \to \bot$ and we are done.

If $a = b$, then $\eta \Vdash \bot$, thus $\eta \Vdash a \notin z$;

take $z = \{(b, \pi)\}$, then $\pi \in \|b \notin z\|$ and $\eta \centerdot \pi \in \|a \notin z \to b \notin z\|$. Thus $\xi \star \eta \centerdot \pi \in \perp\!\!\!\perp$.

Equality

ii) Let $\xi \Vdash a \neq b \to \bot,\ \ \eta \Vdash a \notin z$ and $\pi \in \|b \notin z\|$.

We must show $(\mathsf{cc})\lambda k(\xi)(k)\eta \star \pi \in ⫫$, i.e. $\xi \star \mathsf{k}_\pi \eta \,.\, \pi \in ⫫$.

If $a \neq b$, then $\xi \Vdash \top \to \bot$ and we are done.

If $a = b$, then $\eta \star \pi \in ⫫$, and therefore $\mathsf{k}_\pi \eta \Vdash \bot$. Thus $\mathsf{k}_\pi \eta \,.\, \pi \in \|\bot \to \bot\|$.

But $\xi \Vdash \bot \to \bot$, hence $\xi \star \mathsf{k}_\pi \eta \,.\, \pi \in ⫫$.

Q.E.D.

Preservation of well-foundedness

Theorem. Let f be a function symbol such that the relation $f(y,x)=1$ is well founded in the ground model $\mathcal{M}$. Then :

$\mathsf{Y} \Vdash \forall x\big(\forall y(F[y] \to f(y,x) \neq 1), F[x] \to \bot\big) \to \forall x(F[x] \to \bot\big)$

with $\mathsf{Y} = \mathsf{AA}$ and $\mathsf{A} = \lambda x \lambda f(f)(x)xf$ (Turing fixed point combinator).

Therefore, the relation $f(y,x)=1$ is well founded in the realizability model.

Proof. Let $\xi \Vdash \forall x(\forall y(F[y] \to f(y,x) \neq 1), F[x] \to \bot)$, $\eta \Vdash F[a]$ and $\pi \in \Pi$.

We show $\mathsf{Y} \star \xi . \eta . \pi \in \perp\!\!\!\perp$ by induction on a

following the well founded relation $f(y,x)=1$.

Since $\mathsf{Y} \star \xi . \eta . \pi \succ \xi \star \mathsf{Y}\xi . \eta . \pi$, we need to show $\xi \star \mathsf{Y}\xi . \eta . \pi \in \perp\!\!\!\perp$.

Now, $\xi \Vdash \forall y(F[y] \to f(y,a) \neq 1), F[a] \to \bot$, so that it suffices to show

$\mathsf{Y}\xi \Vdash \forall y(F[y] \to f(y,a) \neq 1)$, i.e. $\mathsf{Y}\xi \Vdash F[b] \to f(b,a) \neq 1$ for every b.

Let $\zeta \Vdash F[b]$ and $\varpi \in \| f(b,a) \neq 1 \|$. Thus, we have $f(b,a)=1$

and therefore $\mathsf{Y} \star \xi . \zeta . \varpi \in \perp\!\!\!\perp$ by induction hypothesis. Q.E.D.

The axioms of ZF$_\varepsilon$ are realized

Foundation. $\curlyvee \Vdash \forall x\big(\forall y(F[y] \to y \not\varepsilon x), F[x] \to \bot\big) \to \forall x(F[x] \to \bot\big)$.

In the ground model $\mathcal{M}$, define a function symbol

$$f(y,x) = 1 \text{ iff } \text{rank}(y) < \text{rank}(x).$$

We have $\|y \not\varepsilon x\| \neq \emptyset \Rightarrow \|f(y,x) \neq 1\| = \Pi$; thus $\|y \not\varepsilon x\| \subset \|f(y,x) \neq 1\|$.

Hence the result, by the theorem above. Q.E.D.

Collapse. $\Vdash \forall x \forall y[x \subseteq y \leftrightarrow (\forall z \varepsilon x) z \in y]$; $\Vdash \forall x \forall y[x \in y \leftrightarrow (\exists z \varepsilon y)\{x \subseteq z, z \subseteq x\}]$

Indeed, we have :

$\|a \subseteq b\| = \|\forall z(z \notin b \to z \not\varepsilon a)\|$ and $\|a \notin b\| = \|\forall z(a \subseteq z, z \subseteq a \to z \not\varepsilon b)\|$

This follows immediately from the definition of $\|a \subseteq b\|$ and $\|a \notin b\|$:

$\|a \subseteq b\| = \bigcup_c \{\xi \cdot \pi;\ \xi \in \Lambda,\ \pi \in \Pi,\ (c,\pi) \in a,\ \xi \Vdash c \notin b\}$;

$\|a \notin b\| = \bigcup_c \{\xi \cdot \xi' \cdot \pi;\ \xi, \xi' \in \Lambda,\ \pi \in \Pi,\ (c,\pi) \in b,\ \xi \Vdash a \subseteq c,\ \xi' \Vdash c \subseteq a\}$.

The axioms of ZF_ε are realized

Pairing. If $c = \{a,b\} \times \Pi$, then $\|a \notin c\| = \|b \notin c\| = \|\bot\|$; thus $I \Vdash a\,\varepsilon\,c$, $I \Vdash b\,\varepsilon\,c$.

Warning. In $\mathcal{N}$, c may have many other ε-elements than a, b.

An instance of a pair $\{a,b\}$ is $c' = \{(a, \mathsf{K}\,.\,\pi);\ \pi \in \Pi\} \cup \{(b, \underline{0}\,.\,\pi);\ \pi \in \Pi\}$. Indeed :

$\lambda x\, x\mathsf{K} \Vdash a\,\varepsilon\,c'$; $\lambda x\, x\underline{0} \Vdash b\,\varepsilon\,c'$; $\lambda x \lambda y \lambda z\, zxy \Vdash \forall x(x \neq a, x \neq b \to x \notin c')$.

Comprehension.

Given a set a and a formula $F[x]$, define $b = \{(u, \xi\,.\,\pi);\ (u,\pi) \in a,\ \xi \Vdash F[u]\}$;

then $\|u \notin b\| = \|F(u) \to u \notin a\|$ for every set u.

Therefore $\mathsf{I} \Vdash \forall x(x \notin b \to (F(x) \to x \notin a))$ and $\mathsf{I} \Vdash \forall x((F(x) \to x \notin a) \to x \notin b)$.

and so on ...

The axioms of ZF_ε have very simple realizers.

But it would be very difficult to realize directly the axioms of ZF,

because they have non trivial proofs in ZF_ε.

Type-like sets in $\mathcal{N}$

Define the function symbol $\daleth$ by $\daleth E = E \times \Pi$. Define the quantifier $\forall x^{\daleth E}$ by :
$\|\forall x^{\daleth E} A[x]\| = \bigcup_{a \in E} \|A[a/x]\|$; therefore $|\forall x^{\daleth E} A[x]| = \bigcap_{a \in E} |A[a/x]|$.

Let us see that this quantifier has the intended meaning $\forall x(x \varepsilon \daleth E \to A[x])$:

Theorem.

i) $\lambda x \lambda y\, yx \Vdash \forall x^{\daleth E} A[x] \to \forall x(\neg A[x] \to x \not\varepsilon \daleth E)$;

ii) cc $\Vdash \forall x(\neg A[x] \to x \not\varepsilon \daleth E) \to \forall x^{\daleth E} A[x]$.

i) Let $\xi \Vdash \forall x^{\daleth E} A[x]$, $\eta \Vdash \neg A[a]$ and $\pi \in \|a \not\varepsilon \daleth E\|$ i.e. $a \in E$.

Then $\xi \Vdash A[a]$; therefore $\lambda x \lambda y\, yx \star \xi . \eta . \pi \succ \eta \star \xi . \pi \in ⫫$.

ii) Let $\xi \Vdash \forall x(\neg A[x] \to x \not\varepsilon \daleth E)$, $a \in E$ and $\pi \in \|A[a]\|$;

then $\xi \Vdash \neg\neg A[a]$, $\mathsf{k}_\pi \Vdash \neg A[a]$; thus $\mathsf{cc} \star \xi . \pi \succ \xi \star \mathsf{k}_\pi . \pi \in ⫫$. Q.E.D.

For every set E of $\mathcal{M}$, the individual $\daleth E$ represents the *type* associated with E.

For instance $\daleth \mathbf{2}$ (resp. $\daleth \mathbb{N}$) is the type of *booleans* (resp. *integers*).

Type-like sets in $\mathcal{N}$

Let f, g be some terms built with the function symbols in the ground model $\mathcal{M}$.

If $\mathcal{M} \models f : E_1 \times \cdots \times E_k \to E$ then $\mathcal{N} \Vdash f : \daleth E_1 \times \cdots \times \daleth E_k \to \daleth E$

(in fact, $\mathsf{I} \Vdash \forall x_1^{\daleth E_1} \cdots \forall x_k^{\daleth E_k}[f(x_1, \ldots, x_k) \not\varepsilon \daleth E \to \bot]$).

Moreover, if $\mathcal{M} \models (\forall x_1 \in E_1) \cdots (\forall x_k \in E_k)[f(x_1, \ldots, x_k) = g(x_1, \ldots, x_k)]$

then $\mathsf{I} \Vdash \forall x_1^{\daleth E_1} \cdots \forall x_k^{\daleth E_k}[f(x_1, \ldots, x_k) = g(x_1, \ldots, x_k)]$.

For instance, let $\wedge, \vee, \neg$ be the (trivial) boolean operations on the set $\mathbf{2} = \{0, 1\}$.

They give a structure of boolean algebra on $\daleth\mathbf{2}$ in the realizability model $\mathcal{N}$.

Remarks about $\daleth\mathbf{2}$.

- $|\forall x^{\daleth\mathbf{2}} F[x]| = |F[1]| \cap |F[0]|$; thus $\forall x^{\daleth\mathbf{2}} F[x]$ behaves like an *intersection type*.
- Every ε-element of $\daleth\mathbf{2}$ except 1 is empty ; indeed $\mathsf{I} \Vdash \forall x^{\daleth\mathbf{2}} \forall y (x \neq 1 \to y \not\varepsilon x)$.
- The boolean algebra $\daleth\mathbf{2}$ is trivial iff the realizability model is a *forcing model.*
- Only two ε-elements of $\daleth\mathbf{2}$ are *named* : 0 and 1.

Integers

Define the function symbol s in $\mathscr{M}$ by $s(a) = \{a\} \times \Pi = ℸ(\{a\})$ and $0 = \emptyset$.

$s(a)$ represents some singleton of a in the realizability model $\mathscr{N}$;

The following formulas are realized in $\mathscr{N}$:

$\forall x \forall y (sx = sy \to x = y)$; $\forall x (sx \neq 0)$;

$\forall x \forall y (x \simeq y \to sx \simeq sy)$.

Let us define $\tilde{\mathbb{N}} = \{(s^n 0, \underline{n} \centerdot \pi);\ n \in \mathbb{N}, \pi \in \Pi\}$;

$\tilde{\mathbb{N}}$ is the set of integers of the realizability model $\mathscr{N}$ (see below).

Since we have $ℸ\mathbb{N} = \{(s^n 0, \pi);\ n \in \mathbb{N}, \pi \in \Pi\}$, it follows that $\mathsf{I} \Vdash \tilde{\mathbb{N}} \subset ℸ\mathbb{N}$.

This inclusion is strict, except in the degenerate case of *forcing*.

Consider a *proof-like term* ν such that $\nu \Vdash s^n 0 \,\varepsilon\, \tilde{\mathbb{N}}$ in every realizability model ;

for instance, ν comes from a proof that $\mathrm{ZF}_\varepsilon \vdash \mathrm{int}(s^n 0)$.

Then ν is a program which computes the integer $\underline{n}$. Indeed, we have :

$\nu \star \kappa \centerdot \pi \succ \kappa \star \underline{n} \centerdot \pi$ for every term κ and stack π.

Integers

Define the quantifier $\forall x^{\text{int}}$ by $\|\forall x^{\text{int}} F[x]\| = \bigcup\{\underline{n}\cdot\pi;\ n \in \mathbb{N}, \pi \in \|F[s^n 0]\|\}$.

Remark. $\xi \Vdash \forall x^{\text{int}} F[x]$ implies $\xi\underline{n} \Vdash F[s^n 0]$ for each $n \in \mathbb{N}$ *(Kleene realizability)*.

We see, as before, that the quantifier $\forall x^{\text{int}}$ has the intended meaning which is $\forall x(x\,\varepsilon\,\tilde{\mathbb{N}} \to F[x])$.

$\tilde{\mathbb{N}}$ represents the set of integers of the model $\mathcal{N}$. Indeed :

Theorem. $\lambda x\, x\underline{0} \Vdash 0\,\varepsilon\,\tilde{\mathbb{N}}$; $\lambda f \lambda x(f)(\sigma)x \Vdash \forall x(sx \notin \tilde{\mathbb{N}} \to x \notin \tilde{\mathbb{N}})$;
$\mathsf{I} \Vdash \forall x^{\text{int}}(\forall y(F[sy] \to F[y]), F[x] \to F[0])$ for every formula $F[x]$.

The following theorem gives a characteristic property of recursive functions : *the image of an integer is an integer* and not only an element of $\beth\mathbb{N}$.

Theorem. Let $f : \mathbb{N}^k \to \mathbb{N}$ be a recursive function defined in $\mathcal{M}$. Then :
$\theta_f \Vdash \forall x_1^{\text{int}} \ldots \forall x_k^{\text{int}}(f(x_1,\ldots,x_k)\,\varepsilon\,\tilde{\mathbb{N}})$ for some proof-like term θ_f.

θ_f is a program which computes f. Indeed, if $\nu_i \Vdash n_i\,\varepsilon\,\tilde{\mathbb{N}}$, we have :
$\theta_f \star \nu_1\cdot\ldots\cdot\nu_k\cdot\kappa\cdot\pi \succ \kappa \star \underline{n}\cdot\pi$ with $n = f(n_1,\ldots,n_k)$.

Arithmetical formulas

Realizability models cannot change the truth of *arithmetical formulas*. :
Indeed, any arithmetical formula which is true in the ground model $\mathcal{M}$,
is realized (by a proof-like term). We have the following general result :

Theorem. Let $f : \mathbb{N}^{2k} \to \mathbf{2}$ be an arbitrary function such that :
$\mathcal{M} \models (\forall x_1 \in \mathbb{N})(\exists y_1 \in \mathbb{N}) \cdots (\forall x_k \in \mathbb{N})(\exists y_k \in \mathbb{N}) \big(f(x_1, y_1, \ldots, x_k, y_k) \neq 0\big)$.
Then, there is a proof-like term θ_k *which depends only on* k, such that :
$\theta_k \Vdash \forall x_1^{\gimel\mathbb{N}} \exists y_1^{\text{int}} \cdots \forall x_k^{\gimel\mathbb{N}} \exists y_k^{\text{int}} \big(f(x_1, y_1, \ldots, x_k, y_k) \neq 0\big)$.

Note that the quantifiers $\forall x_i$ are restricted, not to int, but to $\gimel\mathbb{N}$, which is stronger.
Also, since $f : \gimel\mathbb{N}^{2k} \to \gimel\mathbf{2}$ in the realizability model $\mathcal{N}$,
$f(x_1, y_1, \ldots, x_k, y_k) \neq 0$ does not mean $f(x_1, y_1, \ldots, x_k, y_k) = 1$
unless f is recursive and the quantifiers $\forall x_i$ are restricted to int.

The submodel of constructible sets

In the particular case of *forcing*, the model $\mathcal{N}$ contains the ground model $\mathcal{M}$ as a transitive submodel, with the same ordinals.

It follows that the *constructible universe* is the same for $\mathcal{M}$ and $\mathcal{N}$.

Therefore, arithmetical truth is trivially preserved (*absoluteness*) ;

by a theorem of J. Shoenfield, it is the same for Σ^1_2 and Π^1_2 formulas.

In the general case of *classical realizability*, it was recently shown [12] that the model $\mathcal{N}$ contains *an elementary extension* of the ground model $\mathcal{M}$, again as a transitive submodel, with the same ordinals.

Therefore, the absoluteness result remains true for Σ^1_2 and Π^1_2 formulas.

This may seem disappointing, if we look for independence results.

But, on the other hand, this shows :

Theorem. Any true Σ^1_3 formula is realized by some closed λ-term with cc.

Some examples

As you know, there is a wide variety of *forcing models.*
The notion of *realizability model* being much more general,
there is a much greater variety of realizability models.
But their structure is also much more complicated
and we have to invent completely new techniques to understand them.
We already obtained relative consistency results *impossible to get with forcing*.
But we are far from knowing how to fully exploit the realizability technique.

In the following, I consider two kinds of examples :

- Realizability algebras of terms, which I call *standard realizability algebras* and the particularly simple and interesting *thread model.*
- The usual models of λ-calculus (Scott domains, stable models, ...) are well known *combinatory algebras*.
  But it appears that, in fact, they are *realizability algebras.*

Standard realizability algebras

The terms and the stacks are *words* composed with the following alphabet :

- the elementary *combinators* B, C, I, K, W, cc, ς (this is a new one)
- the *symbols* k $\bullet$ ( ) [ ]
- a countable set Π_0 of *empty stacks*.

The sets Λ of *terms* and Π of *stacks* are defined as follows :

- each elementary combinator is a term ; each empty stack is a stack ;
- if ξ,η are terms, then $(\xi)\eta$ is a term (*application*, written also $\xi\eta$) ;
- if ξ is a term and π a stack, then $\xi\,\bullet\,\pi$ is a stack (*push*) ;
- if π is a stack, then $\mathsf{k}[\pi]$ is a term (*continuation*, written k_π).

A *process* is an ordered pair (ξ,π) with $\xi \in \Lambda, \pi \in \Pi$; it is written $\xi \star \pi$.

The four operations of *application, push, continuation, process*
are defined in the obvious way.

Execution of processes

Define the preorder $\succ$ on processes (*execution*) by the following rules :

$(\xi)\eta \star \pi \succ \xi \star \eta . \pi$

$\mathsf{I} \star \xi . \pi \succ \xi \star \pi$

$\mathsf{K} \star \xi . \eta . \pi \succ \xi \star \pi$

$\mathsf{W} \star \xi . \eta . \pi \succ \xi \star \eta . \eta . \pi$

$\mathsf{C} \star \xi . \eta . \zeta . \pi \succ \xi \star \zeta . \eta . \pi$

$\mathsf{B} \star \xi . \eta . \zeta . \pi \succ \xi \star (\eta)\zeta . \pi$

$\mathsf{cc} \star \xi . \pi \succ \xi \star \mathsf{k}_\pi . \pi$

$\mathsf{k}_\pi \star \xi . \varpi \succ \xi \star \pi$

$\varsigma \star \xi . \eta . \pi \succ \xi \star \underline{\mathsf{n}}_\eta . \pi$

where $\eta \longmapsto \mathsf{n}_\eta$ is a fixed (not necessarily recursive) enumeration of terms.

$\perp\!\!\!\perp$ is any set of processes such that $\xi \star \pi \in \perp\!\!\!\perp, \xi' \star \pi' \succ \xi \star \pi \Rightarrow \xi' \star \pi' \in \perp\!\!\!\perp$.

The *proof-like terms* are generated with the *seven combinators* B, C, I, K, W, cc, ς.

Non extensional and dependent choice

Standard realizability models satisfy a weak form of the axiom of choice.

Theorem. For each formula $F[x,y]$, we can define a function symbol f such that :

$$\mathcal{N} \Vdash \forall x(\exists y\, F[x,y] \to \exists n^{\text{int}} F[x, f(n,x)]).$$

The symbol f is not exactly a choice function,

but the choice is restricted to a *sequence*.

We obtain a true choice function ϕ (but no longer a *function symbol*) by setting :

$\phi(x) = f(n,x)$ for the first n such that $F[x, f(n,x)]$ if there is one ; else 0. Then :

$$\mathcal{N} \Vdash \forall x(\exists y\, F[x,y] \to F[x, \phi(x)])$$

This gives the axiom of choice in the realizability model $\mathcal{N}$ for ZF_ε, *but not for ZF*, because we cannot find a function ϕ which is *compatible with* $\simeq$.

This axiom is much weaker than choice, we call it *non extensional choice (NEC)*.

As we shall see below, it does not even imply the well ordering of $\mathbb{R}$.

Non extensional and dependent choice

Nevertheless, *it implies the axiom of dependent choice (DC)*. The proof is easy :
from $\forall x \exists y\, F[x,y]$, using NEC, we get a function ϕ such that $\forall x\, F[x, \phi x]$;
then, given a_0, we have the sequence $a_i = \phi^i(a_0)$ such that $F[a_i, a_{i+1}]$.
We prove the theorem in the following form :

Theorem. For each formula $F[x,y]$, we can define a function symbol f such that :

$$\lambda x(\mathsf{cc})(\varsigma)x \Vdash \forall x(\forall n^{\mathrm{int}} F[x, f(n,x)] \to \forall y\, F[x,y]).$$

Using the axiom of choice, define f in such a way that, for every individual a :
if there exists some b such that $\pi \in \|F[a,b]\|$, then $\pi \in \|F[a, f(\mathsf{n}_{\mathsf{k}_\pi}, a)]\|$.
Now, let $\xi \Vdash \forall n^{\mathrm{int}} F[a, f(n,a)]$ and $\pi \in \|\forall y\, F[a,y]\|$.
Then $\pi \in \|F[a, f(\mathsf{n}_{\mathsf{k}_\pi}, a)]\|$, thus $\xi \star \underline{\mathsf{n}}_{\mathsf{k}_\pi} \centerdot \pi \in \perp\!\!\!\perp$, by hypothesis on ξ,
and therefore $\varsigma \star \xi \centerdot \mathsf{k}_\pi \centerdot \pi \in \perp\!\!\!\perp$, by the execution rule of ς.
It follows that $\lambda x(\mathsf{cc})(\varsigma)x \star \xi \centerdot \pi \in \perp\!\!\!\perp$. Q.E.D.

The Boolean algebra $\beth 2$

The Boolean algebra $\beth 2$ is a very important object of the realizability model $\mathcal{N}$.
We call it the *characteristic Boolean algebra*.
It is trivial if, and only if, $\mathcal{N}$ is a *forcing model*.
It is rather difficult to handle because it is, in general, infinite (even atomless)
but only its obvious elements 0 and 1 are *named*.
It may be not well-orderable (see the *model of threads* below)
but there is always an *ultrafilter* on $\beth 2$, which is also a canonical object of $\mathcal{N}$ [12].

The Boolean algebra $\gimel 2$

When the realizability algebra is standard, $\gimel 2$ has a remarkable property :

$\gimel 2$ has a countable dense subset.

Theorem. There exists a function $\Delta : \mathbb{N} \to \mathbf{2}$ such that
$\lambda x \lambda y(\varsigma) y x x \Vdash \forall x^{\gimel 2}(x \neq 0 \to \exists n^{\text{int}}\{\Delta(n) \neq 0, (\Delta(n) \vee x) = x\})$.

Δ is defined as follows in $\mathcal{M}$: let $j \longmapsto \eta_j$ be the inverse of the given enumeration of Λ, which is $\eta \longmapsto \mathrm{n}_\eta$
(recall : the execution rule of the instruction ς is $\varsigma \star \xi . \eta . \pi \succ \xi \star \underline{\mathrm{n}}_\eta . \pi$). Then

$$\Delta(j) = 0 \Leftrightarrow \eta_j \Vdash \bot.$$

In $\mathcal{N}$, we have $\Delta : \gimel\mathbb{N} \to \gimel 2$; in particular $\Delta : \widetilde{\mathbb{N}} \to \gimel 2$.
The theorem says that every element $\neq 0$ of $\gimel 2$ has a lower bound $\Delta(n) \neq 0$ with $n \,\varepsilon\, \widetilde{\mathbb{N}}$.

$\daleth 2$ has a countable dense subset (proof)

Proof. Let $a \in \{0,1\}$, $\eta \Vdash a \neq 0$, $\xi \Vdash \forall n^{\text{int}}(\Delta(n) \neq 0 \to a \neq \Delta(n) \vee a)$ and $\pi \in \Pi$.

We must show $\lambda x \lambda y(\varsigma)yxx \star \eta . \xi . \pi \in \perp\!\!\!\perp$ i.e. $\varsigma \star \xi . \eta . \eta . \pi \in \perp\!\!\!\perp$ that is :

$$\xi \star \underline{\mathsf{n}}_\eta . \eta . \pi \in \perp\!\!\!\perp.$$

By hypothesis on ξ, it suffices to show $\underline{\mathsf{n}}_\eta . \eta . \pi \in \|\forall n^{\text{int}}(\Delta(n) \neq 0 \to a \neq \Delta(n) \vee a)\|$

i.e. by definition of the quantifier $\forall n^{\text{int}}$: $\eta . \pi \in \|\Delta(\mathsf{n}_\eta) \neq 0 \to a \neq \Delta(\mathsf{n}_\eta) \vee a\|$

This amounts to show : $\eta \Vdash \Delta(\mathsf{n}_\eta) \neq 0$ and $a = \Delta(\mathsf{n}_\eta) \vee a$

- Proof of $\eta \Vdash \Delta(\mathsf{n}_\eta) \neq 0$: trivial if $\Delta(\mathsf{n}_\eta) = 1$ because $\|\Delta(\mathsf{n}_\eta) \neq 0\| = \emptyset$;
  if $\Delta(\mathsf{n}_\eta) = 0$, then $\eta \Vdash \perp$, by definition of Δ.
- Proof of $a = \Delta(\mathsf{n}_\eta) \vee a$: obvious if $a = 1$; if $a = 0$, then $\eta \Vdash \perp$ (hypothesis on η) ;
  thus $\Delta(\mathsf{n}_\eta) = 0$ by definition of Δ, hence the result. Q.E.D.

The pseudo integers $\gimel\mathbf{n}$

In the ground model $\mathcal{M}$, we put, for each integer n :

$$\mathbf{n} = \{0, 1, \ldots, n-1\} = \{0, s0, \ldots, s^{n-1}0\}.$$

The functions $n \mapsto \mathbf{n}$ and $n \mapsto \gimel\mathbf{n}$ are defined in the realizability model $\mathcal{N}$ with domain $\gimel\mathbb{N}$.

We define the function $(m{<}n)$ from $(\gimel\mathbb{N})^2$ into $\gimel\mathbf{2}$, by setting, in $\mathcal{M}$, for $m, n \in \mathbb{N}$:

$(m{<}n) = 1$ if $m < n$ else $(m{<}n) = 0$.

The relation $(m{<}n) = 1$ is a strict (well founded, partial) order on $\gimel\mathbb{N}$ which is the usual order on the set $\widetilde{\mathbb{N}}$ of integers in $\mathcal{N}$.

The following formulas are realized :

$\forall x^{\gimel\mathbb{N}} \forall m^{\gimel\mathbb{N}} ((x{<}m) = 1 \leftrightarrow x \,\varepsilon\, \gimel\mathbf{m})$

$\forall m^{\gimel\mathbb{N}} \forall n^{\gimel\mathbb{N}} ((m{<}n) = 1 \to \gimel\mathbf{m} \subset \gimel\mathbf{n})$

$\forall m^{\gimel\mathbb{N}} \forall n^{\gimel\mathbb{N}}$(the application $(x, y) \longmapsto my + x$ is a bijection from $\gimel\mathbf{m} \times \gimel\mathbf{n}$ onto $\gimel(\mathbf{mn})$).

Injection of $\daleth\mathbf{n}$ into $\mathbb{R}$

The application $x \longmapsto \{n \,\varepsilon\, \tilde{\mathbb{N}};\ \Delta(n) \le x\}$ is, in $\mathcal{N}$, an injection of $\daleth\mathbf{2}$ into $\mathscr{P}(\tilde{\mathbb{N}})$ (the real line of the model $\mathcal{N}$). Therefore :

$\mathcal{N} \Vdash (\forall n^{\text{int}})(\exists f : (\daleth\mathbf{2})^n \to \mathbb{R})(f$ is injective).

By recurrence on n, we see that $(\daleth\mathbf{2})^n$ is equipotent with $\daleth(\mathbf{2^n})$.

Now, for each integer n, we have $n < 2^n$ and therefore $\daleth\mathbf{n} \subset \daleth(\mathbf{2^n})$. Thus :

$\mathcal{N} \Vdash (\forall n^{\text{int}})(\exists f : \daleth\mathbf{n} \to \mathbb{R})(f$ is injective).

We will now choose the set $\perp\!\!\!\perp$ such that, in the realizability model $\mathcal{N}$, $\daleth\mathbf{2}$ is infinite and the “cardinals” of $\daleth\mathbf{n}$ form a *strictly increasing sequence* (which means that there is no surjection of $\daleth\mathbf{n}$ onto $\daleth(\mathbf{n}+\mathbf{1})$).

Since $\daleth\mathbf{m} \times \daleth\mathbf{n}$ is equipotent with $\daleth(\mathbf{mn})$, it follows that :

neither $\daleth\mathbf{2}$ nor $\mathbb{R}$ are well ordered in $\mathcal{N}$.

The model of threads

Remark. If $\daleth 2$ is non trivial, then there are non standard integers in the model $\mathcal{N}$.

Indeed, let $a \varepsilon \daleth \mathbf{2}, a \neq 0,1$; there is an integer n such that $\Delta(n) \neq 0$ and $\Delta(n) \leq a$.

Thus $\Delta(n) \neq 0,1$; n is non-standard because $\Delta(m) = 0$ or 1 for each standard m.

Thus, the realizability model $\mathcal{N}$ we are looking for, has non-standard integers.

It cannot be a forcing model or an inner model.

We define now the simplest non trivial *coherent* realizability model. Let :

$n \longmapsto \pi_n$ be an enumeration of the *empty stacks*

$n \longmapsto \theta_n$ be a (not necessarily recursive) enumeration of the *proof-like terms*.

The *thread with number n* is the set of processes $\xi \star \pi$ such that $\theta_n \star \pi_n \succ \xi \star \pi$.

The only empty stack which appears in the terms of the n-th thread is π_n.

The model of threads

The simplest way to ensure a *coherent model* is to decide that $\theta_n \star \pi_n \in \perp\!\!\!\perp^c$

($\perp\!\!\!\perp^c$ is the complement of $\perp\!\!\!\perp$). Then, every thread must be in $\perp\!\!\!\perp^c$. Thus, we decide :

$\perp\!\!\!\perp^c$ is the union of all threads

Therefore $\xi \star \pi \in \perp\!\!\!\perp$ iff $\xi \star \pi$ never appears in any thread.

$\xi \Vdash \perp$ iff ξ never appears in head position in any thread.

Theorem. The following are satisfied in the model of threads :

i) There is a proof-like ω such that $\omega \mathrm{k}_\pi \xi \Vdash \perp$ or $\omega \mathrm{k}_\pi \xi' \Vdash \perp$ for any π, ξ, ξ' with $\xi \neq \xi'$.

ii) If $\zeta_0, \zeta_1, \zeta_2$ are distinct, then $\mathrm{k}_\pi \alpha \zeta_0 \Vdash \perp$ or $\mathrm{k}_\pi \alpha \zeta_1 \Vdash \perp$ or $\mathrm{k}_\pi \alpha \zeta_2 \Vdash \perp$ for any α, π.

i) Take $\omega = (\lambda x\, xx)\lambda x\, xx$ or (WI)(W)I.

ii) If the process $\alpha \star \pi$ appears twice in a thread, then the execution enters in a loop, and there will be no third appearance.

Q.E.D.

Consequences of (i)

We now consider any realizability model which satisfies properties (i) or (ii) (or both).

Theorem. If a realizability model $\mathcal{N}$ satisfies property (i), then :

- $\mathcal{N} \Vdash \beth\mathbf{2}$ is not countable
- $\mathcal{N} \Vdash \forall m^{\text{int}} \forall n^{\text{int}} (m < n \to$ there is no surjection from $\beth\mathbf{m}$ onto $\beth\mathbf{n}$).

Since there is an injection of $\beth\mathbf{n}$ into $\mathbb{R}$, it follows that :

there exists a sequence $X_n (n \geq 2)$ of infinite subsets of $\mathbb{R}$ such that

their "cardinals" are strictly increasing and $X_m \times X_n$ is equipotent with X_{mn}.

Dependent choice is true, but $\mathbb{R}$ *is badly not well orderable.*

The behaviour of cardinals of subsets of $\mathbb{R}$ is dramatically unusual ; for instance :

$\text{card}(X_5) < \text{card}(X_6) < \text{card}(X_7)$ and $\text{card}(X_5 \times X_7) < \text{card}(X_6 \times X_6)$.

These relative consistency results are *not obtainable with forcing.*

Consequences of (ii)

Theorem.

If a realizability model $\mathcal{N}$ satisfies property (ii), then it realizes the formulas :

- $\daleth\mathbf{2}$ is an atomless Boolean algebra.
- $\forall a^{\daleth\mathbf{2}} \forall b^{\daleth\mathbf{2}} (a \wedge b = 0, b \neq 0 \to$ there is no surjection from $a\daleth\mathbf{2}$ onto $b\daleth\mathbf{2}$).
- $\forall a^{\daleth\mathbf{2}} \forall b^{\daleth\mathbf{2}} (a < b \to$ there is no surjection from $a\daleth\mathbf{2}$ onto $b\daleth\mathbf{2}$).

$a\daleth\mathbf{2}$ is the ideal $\{x \,\varepsilon\, \daleth\mathbf{2};\ x \leq a\}$ of the boolean algebra $\daleth\mathbf{2}$.

We have an atomless Boolean algebra $\mathscr{B}$ of infinite subsets of $\mathbb{R}$ such that :

$X, Y \in \mathscr{B}, X \cap Y = \emptyset \Rightarrow$ card(X) and card(Y) are not comparable.

$X, Y \in \mathscr{B}, X \subset Y, X \neq Y \Rightarrow$ card$(X) <$ card(Y).

Thus, there is a family $(X_r)_{r \in \mathbb{R}}$ of subsets of $\mathbb{R}$ such that

$r < s \Rightarrow$ card$(X_r) <$ card(X_s).

Very far from the continuum hypothesis and the well ordering of $\mathbb{R}$.

$\beth 2$ is not equipotent with $\beth 4$

This is the key property to prove that $\mathbb{R}$ is not well ordered.

Theorem. Suppose there is a proof-like ω such that $\xi \neq \xi' \Rightarrow \omega\mathsf{k}_\pi\xi \Vdash \bot$ or $\omega\mathsf{k}_\pi\xi' \Vdash \bot$.
Then $\lambda x \lambda x'(\mathrm{cc})\lambda k(x')\lambda z(xzz)(\omega)kz \Vdash$

$$\forall x \forall y \forall y' \big(F(x,y), F(x,y'), y \neq y' \to \bot\big), \forall y^{\beth 4} \exists x^{\beth 2} F(x,y) \to \bot.$$

The formula F being arbitrary, this tells us that there is no surjection from $\beth 2$ onto $\beth 4$.
A similar proof would show that there is no surjection from $\widetilde{\mathbb{N}}$ onto $\beth 2$.
Since $\beth 4$ is equipotent with $(\beth 2)^2$ it follows that $\beth 2$ is not well ordered.

Proof. If this is false, there exist $\xi, \xi' \in \Lambda, \pi \in \Pi$ such that :

$\lambda x \lambda x'(\mathrm{cc})\lambda k(x')\lambda z(xzz)(\omega)kz \star \xi \,.\, \xi' \,.\, \pi \notin \perp\!\!\!\perp$;

$\xi \Vdash \forall x \forall y \forall y' \big(F(x,y), F(x,y'), y \neq y' \to \bot\big)$;

$\xi' \Vdash \forall y^{\beth 4} \neg \forall x^{\beth 2} \neg F(x,y)$.

$\beth 2$ is not equipotent with $\beth 4$

Therefore, we have $\xi' \star \eta \cdot \pi \notin \perp\!\!\!\perp$ with $\eta = \lambda z(\xi z z)(\omega)\mathsf{k}_\pi z$.

By hypothesis on ξ', we have $\eta \not\Vdash \forall x^{\beth 2} \neg F(x, i)$ for $i < 4$.

Thus, there exists $\delta_i \in \{0, 1\}$ such that $\eta \not\Vdash \neg F(\delta_i, i)$.

Then, there exist $\xi_i \in \Lambda$ and $\pi_i \in \Pi$ such that $\xi_i \Vdash F(\delta_i, i)$ and $\eta \star \xi_i \cdot \pi_i \notin \perp\!\!\!\perp$.

By definition of η, we get $\xi \star \xi_i \cdot \xi_i \cdot \omega\mathsf{k}_\pi \xi_i \cdot \pi_i \notin \perp\!\!\!\perp$.

By hypothesis on ξ, we have $\omega\mathsf{k}_\pi \xi_i \not\Vdash i \neq i$, i.e. $\omega\mathsf{k}_\pi \xi_i \not\Vdash \perp$ for every $i < 4$.

Now, the hypothesis of the theorem gives $\xi_i = \xi_j$ for every $i, j < 4$.

But, since $\delta_i < 2$, there exist $i, j < 4$, $i \neq j$ such that $\delta_i = \delta_j = \delta$.

Then, $\xi_i = \xi_j \Vdash F(\delta, i), F(\delta, j)$ and $\omega\mathsf{k}_\pi \xi_i \Vdash i \neq j$ since $\|i \neq j\| = \emptyset$.

Thus, by hypothesis on ξ, we have $\xi \star \xi_i \cdot \xi_i \cdot \omega\mathsf{k}_\pi \xi_i \cdot \pi_i \in \perp\!\!\!\perp$, which is a contradiction.

Q.E.D.

Denotational semantics and realizability algebra

In 1962, P. Cohen discovered his powerful method of *forcing*, which gives
a model of ZF set theory, from any ordered set P (the set of *conditions*).
D. Scott found that we can always take for P a *complete Boolean algebra*.
This gives the well known *Boolean-valued models*,
due also to P. Vopenka and R. Solovay.
Ten years later, the same D. Scott used *complete lattices*
to build models of *λ-calculus* and *combinatory logic*.
But complete lattices and complete Boolean algebras are very similar structures.
In this talk, we explain how to continue this story and close the loop :
starting with a model of λ-calculus, we can generally give it
a structure of *realizability algebra*, and thus obtain a *model of ZF*.

Denotational semantics

There exists a lot of *models of λ-calculus*, such as Scott domains, coherent and hypercoherent models, ... They are all *combinatory algebras*.

Thus, the combinators B, C, I, K, W and the operation of application are defined.

In order to obtain *realizability algebras*, we should define :

- the sets Π of stacks and $\Lambda \star \Pi$ of processes ;
- the combinator cc and the operation of continuation $\pi \mapsto \mathsf{k}_\pi$;
- the operations $(\xi, \pi) \mapsto \xi \,.\, \pi$ (push) and $(\xi, \pi) \mapsto \xi \star \pi$ (process).

T. Ehrhard has found a simple and elegant way to do this.

The construction of stacks was also found by T. Streicher.

There is also a natural way to define the *proof-like terms*.

Thus, in the usual models of λ-calculus, a much richer structure is hidden : they are, in fact, realizability algebras ; and it follows that *a model of set theory* is associated with each of them.

The coherent model

Since we don't want to get *forcing models*, we need to avoid *parallel or*.

Thus, our example will be the simplest *coherent model of λ-calculus*.

Let us recall (one of) its construction.

We first define the set $\mathcal{F}$ of (propositional) *formulas* as the smallest set such that :

$o \in \mathcal{F}$ where o is a fixed symbol ;

if $\alpha \in \mathcal{F}$ and a is a finite subset of $\mathcal{F}$, then $(a \to \alpha) \in \mathcal{F}$;

moreover, we identify $\emptyset \to o$ with o.

Each $\alpha \in \mathcal{F}$ has a unique normal form $\alpha = (a_1, \ldots, a_k \to o)$

with $k \in \mathbb{N}$ and $a_k \neq \emptyset$. Then $\alpha = (a_1, \ldots, a_k, \emptyset, \ldots, \emptyset \to o)$.

The *truth value* $|\alpha| \in \{0, 1\}$ of a formula α is defined by induction :

$|o| = 0$; $|a_1, \ldots, a_k \to o| = 1$ iff $(\exists \beta \in a_1 \cup \ldots \cup a_k)(|\beta| = 0)$.

The coherent model

If $\alpha = (a_1, \dots, a_k \to o), \beta = (b_1, \dots, b_k \to o)$ we define

$$\alpha \sqcap \beta = (a_1 \cup b_1, \dots, a_k \cup b_k \to o).$$

This operation is associative, commutative and idempotent ; o is neutral ;

it defines an order relation : $\alpha \le \beta \Leftrightarrow b_1 \subset a_1, \dots, b_k \subset a_k$.

Define a subset $\mathscr{W}$ of $\mathscr{F}$ (the *web*) by induction : $(a_1, \dots, a_k \to o) \in \mathscr{W}$ iff

for $1 \le i \le k$, $a_i \subset \mathscr{W}$ and $(\forall \beta, \gamma \in a_i)(\beta \ne \gamma \Rightarrow \beta \sqcap \gamma \notin \mathscr{W})$ (a_i is an *antichain* of $\mathscr{W}$).

$\mathscr{W}$ is a final segment of $\mathscr{F}$:

let $\alpha = (a_1, \dots, a_k \to o)$, $\beta = (b_1, \dots, b_k \to o)$, $\alpha \in \mathscr{W}, \alpha \le \beta$.

Then $b_i \subset a_i$ and a_i is an antichain of $\mathscr{W}$, thus so is b_i.

$\alpha, \beta \in \mathscr{W}$ are called *compatible* if $\alpha \sqcap \beta \in \mathscr{W}$; in symbols $\alpha \asymp \beta$.

If $\alpha_1, \dots, \alpha_n$ are pairwise compatible, then $\alpha_1 \sqcap \dots \sqcap \alpha_n \in \mathscr{W}$.

The combinatory algebra

We first recall the well known structure of *combinatory algebra* :

- Λ is the set of antichains of $\mathcal{W}$, i.e. $t \subset \mathcal{W}$ is a term iff $(\forall \alpha, \beta \in t)(\alpha \asymp \beta \to \alpha = \beta)$.
- $t\,u = \{\alpha \in \mathcal{W}\,;\, (\exists a \subset u)(a \to \alpha) \in t\}$; it follows that : $t\,u_1 \ldots u_k = \{\alpha \in \mathcal{W}\,;\, (\exists a_1 \subset u_1, \ldots, a_k \subset u_k)(a_1, \ldots, a_k \to \alpha) \in t\}$.
- I is the set of formulas $\{\alpha\} \to \alpha$ for $\alpha \in \mathcal{W}$.
- K is the set of formulas $\{\alpha\}, \emptyset \to \alpha$ for $\alpha \in \mathcal{W}$.
- C is the set of formulas $\{b, a \to \alpha\}, a, b \to \alpha$ where a and b are antichains.
- W is the set of formulas $\{a, b \to \alpha\}, a \cup b \to \alpha$ where $a \cup b$ is an antichain.
- B is the set of formulas $\{\{\alpha_1, \ldots, \alpha_k\} \to \alpha\}, \{(a_1 \to \alpha_1), \ldots, (a_k \to \alpha_k)\}, a_1 \cup \ldots \cup a_k \to \alpha$ where $\{\alpha_1, \ldots, \alpha_k\}$ and $a_1 \cup \ldots \cup a_k$ are antichains.

The realizability algebra

We now complete this structure to get a realizability algebra.

- Π is the set of filters of $\mathcal{W}$, i.e. $\pi \subset \mathcal{W}$ is a stack iff
  $\mathsf{o} \in \pi$; $(\forall \alpha, \beta \in \pi)\, \alpha \sqcap \beta \in \pi$; $\forall \alpha \forall \beta (\alpha \in \pi, \alpha \leq \beta \to \beta \in \pi)$.
- $t \centerdot \pi = \{a \to \alpha \,;\, a \subset t,\, \alpha \in \pi\}$.

Remark. Π *can be identified with* $\Lambda^{\mathbb{N}}$: *a sequence of terms* $(t_0, \ldots, t_k, \ldots)$ *corresponds with the filter* $\{(a_0, \ldots, a_k \to \mathsf{o}) \;;\, k \in \mathbb{N},\, a_0 \subset t_0, \ldots, a_k \subset t_k\}$.
Moreover, if $\pi = (t_0, \ldots, t_n, \ldots)$, *then* $t \centerdot \pi = (t, t_0, \ldots, t_n, \ldots)$.

- $\Lambda \star \Pi$ is $\{0, 1\}$ and $\perp\!\!\!\perp$ is $\{1\}$.
- If $t \in \Lambda, \pi \in \Pi$ then $t \star \pi \in \perp\!\!\!\perp$ iff $t \cap \pi \neq \emptyset$ (i.e. $t \cap \pi$ is a singleton).
- k_π is the set of formulas $(\{\alpha\} \to \mathsf{o})$ for $\alpha \in \pi$;
- cc is the set of formulas $\{a \to \alpha\} \to \alpha \sqcap \alpha_1 \sqcap \ldots \sqcap \alpha_k$
  with $a = \{\{\alpha_1\} \to \mathsf{o}, \ldots, \{\alpha_k\} \to \mathsf{o}\}$ and $\alpha \sqcap \alpha_1 \sqcap \ldots \sqcap \alpha_k \in \mathcal{W}$.
- PL is the set of $t \in \Lambda$ such that $|t| = 1$ i.e. $(\forall \alpha \in t)(|\alpha| = 1)$.

The realizability algebra

Lemma 1. $t \Vdash \top, \ldots, \top \to \bot$ iff $t = \{o\}$.

Indeed, $t \star \emptyset . \ldots . \emptyset . \{o\} \in \perp\!\!\!\perp \Rightarrow t = \{o\}$ QED

Lemma 2. If $t \in |\top, \bot \to \bot| \cap |\bot, \top \to \bot|$ then $t = \{o\}$.

We have $t \cap \emptyset . \{o\} . \{o\} \neq \emptyset$ and $t \cap \{o\} . \emptyset . \{o\} \neq \emptyset$; thus

$(\emptyset, a \to o) \in t$ and $(b, \emptyset \to o) \in t$ with $a, b \subset \{o\}$.

But these two formulas are compatible and therefore equal ; thus $a = b = \emptyset$. QED

It follows that there is no *parallel or* in PL ; therefore :

The model of ZF associated with this realizability algebra is *not a forcing model.*

T. Streicher told me he has shown that it satisfies the *dependent choice*.

Problem : does this model satisfies the axiom of choice ? (probably not).

Integers

In the sequel, we use truth values defined by subsets $|V|$ of Λ.

They may be used in formulas only before a $\to$.

If $|V| \subset \Lambda, \|A\| \subset \Pi$, we define $\|V \to A\| = \{t \cdot \pi \,;\; t \in |V|, \pi \in \|A\|\}$.

In particular $\|\neg V\| = \{t \cdot \pi \,;\; t \in |V|, \pi \in \Pi\}$.

Lemma 3. If $(\forall t \in \Lambda)(t \in |V| \Rightarrow \theta t \in |W|)$ then $\lambda x\, x \circ \theta \Vdash \neg W \to \neg V$.

We shall sometimes write $\theta \Vdash V \to W$ in such a case.

Now, define the formulas :

$\nu_0 = (\{\mathsf{o}\} \to \mathsf{o})\;;\; \nu_1 = (\emptyset, \{\mathsf{o}\} \to \mathsf{o})\;;\; \ldots\;;\; \nu_n = (\emptyset, \ldots, \emptyset, \{\mathsf{o}\} \to \mathsf{o})\;;\; \ldots\;;$

and the terms $\overline{n} = \{\nu_n\}$; $\mathsf{suc} = \{(\{\nu_0\} \to \nu_1), \ldots, (\{\nu_i\} \to \nu_{i+1}), \ldots\}$.

Define the unary predicate N by :

$|Nn| = \{\overline{n}\}$ if $n \in \mathbb{N}$; $|Nn| = \emptyset$ if $n \notin \mathbb{N}$.

Then we have easily $\lambda x(x)\overline{0} \Vdash \neg\neg N0$; $\mathsf{suc} \Vdash Nn \to N(n+1)$ for every n ;

i.e. $\lambda x\, x \circ \mathsf{suc} \Vdash \forall x(\neg N(x+1) \to \neg Nx)$.

We have shown : $\Vdash \forall x^{\mathrm{int}} \neg\neg Nx$.

Theorem 4. Let $u_n (n \in \mathbb{N})$ be any sequence of terms and define :
$\theta = \{(\{v_n\} \to \alpha)\ ;\ n \in \mathbb{N}, \alpha \in u_n\}$. Then $\theta \overline{n} = u_n$ for all $n \in \mathbb{N}$.
If every u_n is in PL, then $\theta \in$ PL.
We show that $\theta \in \Lambda_D$: if $(\{v_m\} \to \alpha) \asymp (\{v_n\} \to \beta)$ then $\{v_m, v_n\}$ is an antichain and therefore $m = n$; thus $\alpha, \beta \in u_m$; but $\alpha \asymp \beta$ and therefore $\alpha = \beta$.
$\theta\{v_n\} = u_n$ is obvious. QED

Define the unary predicate $\text{ent}(x)$ by :
$|\text{ent}(n)| = \{\underline{n}\}$ (Church integer) for $n \in \mathbb{N}$; $|\text{ent}(n)| = \emptyset$ if $n \notin \mathbb{N}$.
We already know (general theory) that $\text{ent}(x)$ is equivalent to $\text{int}(x)$.
Apply lemma 3 and theorem 4 above with $u_n = \{\underline{n}\}$.
This gives $\theta \Vdash Nn \to \text{ent}(n)$ and therefore $\lambda x\, x \circ \theta \Vdash \forall x(\neg \text{ent}(x) \to \neg Nx)$.
Finally we have shown that the predicates Nx, $\text{int}(x)$, $\text{ent}(x)$ are equivalent.
In the following, we use Nx which is the simplest.

Corollary. If $\theta_n \Vdash F(n)$, with $\theta_n \in$ PL for all $n \in \mathbb{N}$, then there exists $\theta \in$ PL such that $\theta \Vdash \forall n^{\text{int}} F(n)$.

Applying theorem 4, we get $\theta \underline{n} \Vdash F(n)$ for all $n \in \mathbb{N}$, thus $\theta \Vdash \forall n^{\text{int}} F(n)$. QED

By the above corollary, the set of formulas which are realized by a proof-like term is closed by the ω-rule.

Thus there exists a realizability model *which is an ω-model*.

Let $\mathscr{B} = \mathscr{P}(\Pi)$ be the Boolean algebra of truth values.

The order is defined by $\|A\| \leq \|B\| \Leftrightarrow (\exists \theta \in \text{PL})(\theta \Vdash A \to B)$.

Theorem. $\mathscr{B}$ is a countably complete Boolean algebra :

If $\|B(n)\|_{n \in \mathbb{N}}$ is a sequence of truth values, then $\inf_{n \in \mathbb{N}} \|B(n)\| = \|\forall x^{\text{int}} B(x)\|$.

Let $\|A\| \leq \|B(n)\|$ for every $n \in \mathbb{N}$. Then $\theta_n \Vdash A \to B(n)$ for some sequence $\theta_n \in$ PL.

By the previous corollary, we get $\theta \Vdash \|A \to \forall x^{\text{int}} B(x)\|$ i.e. $\|A\| \leq \|\forall x^{\text{int}} B(x)\|$.

Conversely, $\|\forall x^{\text{int}} B(x)\| \leq \|B(n)\|$ because $\lambda x(x)\underline{n} \Vdash \forall x^{\text{int}} B(x) \to B(n)$. QED

References

1. **S. Berardi, M. Bezem, T. Coquand** *On the computational content of the axiom of choice.* J. Symb. Log. 63, pp. 600-622, 1998.

2. **H.B. Curry, R. Feys** *Combinatory Logic.* North-Holland, 1958.

3. **T. Griffin.** *A formulæ-as-type notion of control.*
Conf. Record of the 17th A.C.M. Symp. on Principles of Progr. Languages, 1990.

3. **M. E. Hyland** *The effective topos.* The Brouwer Centenary Symposium (Noordwijkerhout, 1981), pp. 165–216, Stud. Log. Found. Math., 110, North-Holland, 1982.

4. **W. Howard** *The formulas–as–types notion of construction.* Essays on combinatory logic, λ-calculus, and formalism, Acad. Press, pp. 479–490, 1980.

5. **G. Kreisel.** *On the interpretation of non-finitist proofs I.*
J. Symb. Log. 16, pp. 248-267, 1951.

6. **G. Kreisel.** *On the interpretation of non-finitist proofs II.*
J. Symb. Log. 17, pp. 43-58, 1952.

References (cont.)

7. **J.-L. Krivine** *Typed lambda-calculus in classical Zermelo-Fraenkel set theory.*
Arch. Math. Log. 40, 3, pp. 189-205, 2001.

8. **J.-L. Krivine** *Dependent choices, ‘quote’ and the clock.*
Th. Comp. Sc. 308, pp. 259-276, 2003.

9. **J.-L. Krivine** *Realizability in classical logic.*
Panoramas et synthèses, Société Mathématique de France, 27, pp. 197-229, 2009.

10. **J.-L. Krivine** *Realizability algebras : a program to well order* $\mathbb{R}$.
Log. Methods in Comp. Sc. 7 (3:02) pp. 1-47, 2011.

11. **J.-L. Krivine** *Realizability algebras II : new models of ZF + DC*
Log. Methods in Comp. Sc. 8 (1:10) pp. 1-28, 2012.

12. http://www.pps.univ-paris-diderot.fr/~krivine/articles/Fondation.pdf

13. **A. Miquel** *Forcing as a program transformation.* LICS’11, p. 197-206, 2011.

Pdf files at http://www.pps.univ-paris-diderot.fr/~krivine