The evolution of the concept of proof trough realizability

Laura Fontanella

Université Paris Est Créteil
Laboratoire LACL
IUT Sénart Fontainebleau

October 28, 2021

What is a mathematical proof?

What is a mathematical proof?

Proofs are algorithms

What is a mathematical proof?

Proofs are algorithms : realizability

from constructive mathematics to the axiom of choice

Kleene

BHK interpretation

Proofs as functions : ex. a proof of $P \to Q$ is a function f that converts a proof of P into a proof of Q

Computability theory

The study of *computable* functions

Kleene 1945

Proofs are *computable functions* $\to$ Development of Realisability: interpretation of Heyting arithmetic by sets of (indexes) of recursive functions

Realisability

Goal:

To extract the computational content of mathematical proofs. A theory/logical system is interpreted in a model of computation by establishing a correspondence between formulae and programs in a way that is compatible with the rules of deduction.

Exemple: a realizer of $A \Rightarrow B$ is a program which applied to a realizer of A returns a realizer of B

Realisability

Goal:

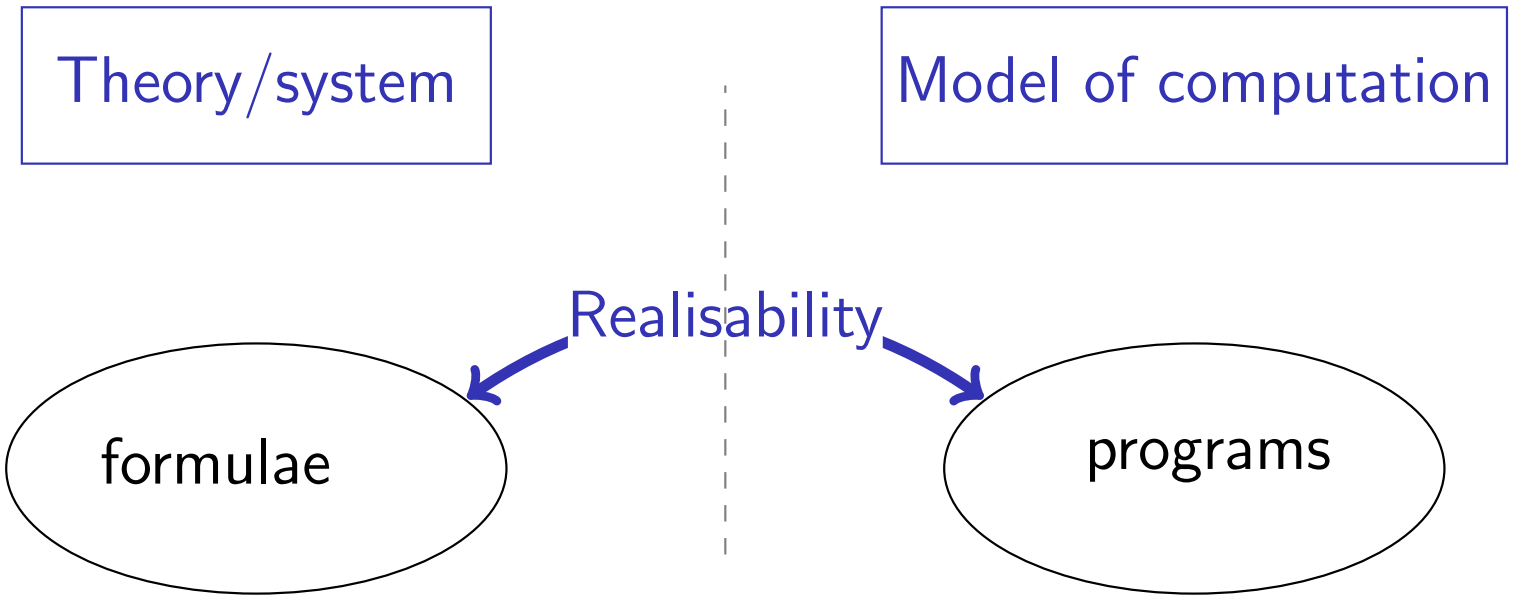
To extract the computational content of mathematical proofs. A theory/logical system is interpreted in a model of computation by establishing a correspondence between formulae and programs in a way that is compatible with the rules of deduction.

Exemple: a realizer of $A \Rightarrow B$ is a program which applied to a realizer of A returns a realizer of B

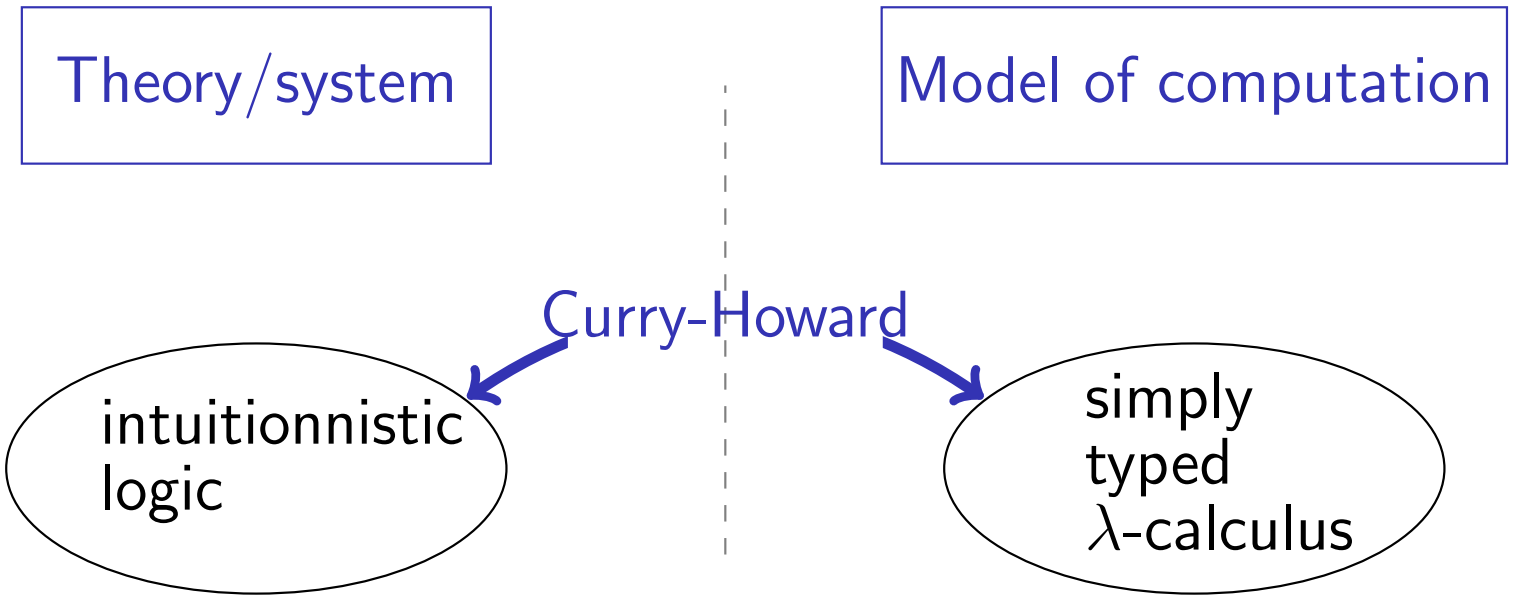
Programs extraction

When a formula A is provable it is possible to extract from every proof of A, a program that realizes it (analogous to programs-extraction in proofs assistants such as Coq).

From Curry Howard to classical realizability



From Curry Howard to classical realizability



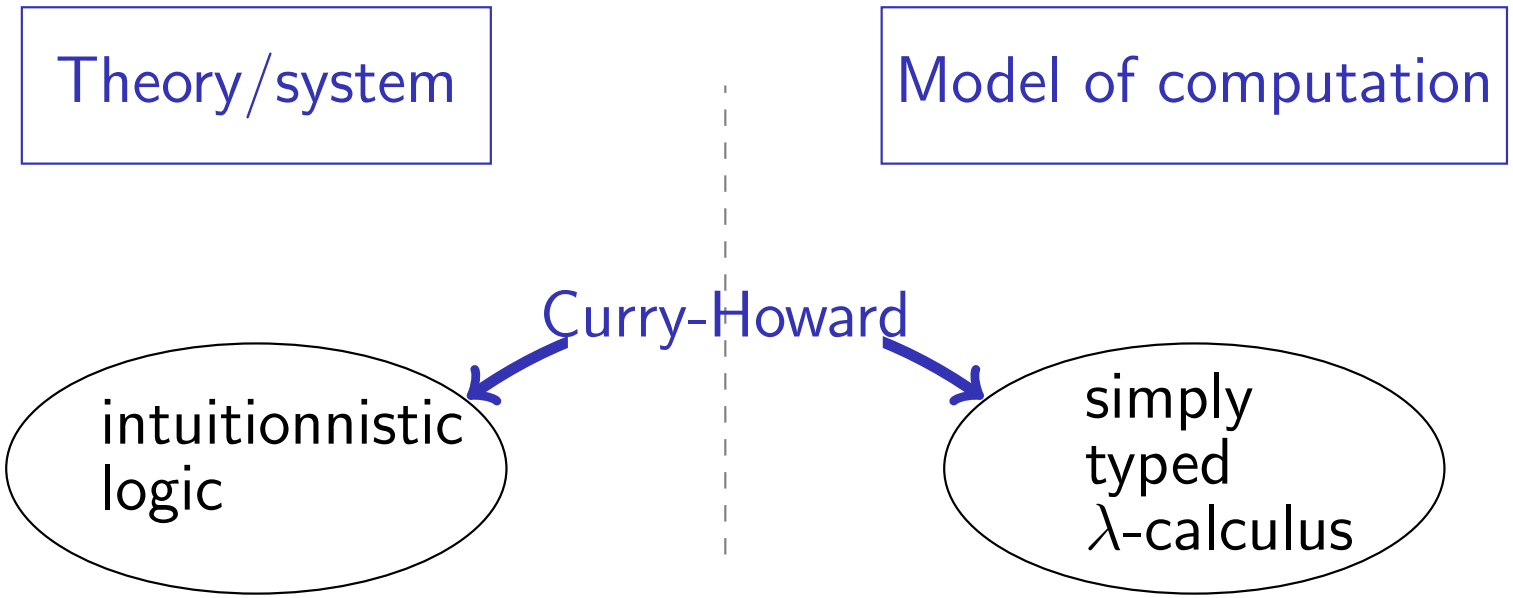
Curry-Howard isomorphism

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{B \Rightarrow A,\ C \Rightarrow B,\ C \vdash B \Rightarrow A}}{B \Rightarrow A,\ C \Rightarrow B,\ C \vdash A}}{B \Rightarrow A,\ C \Rightarrow B \vdash C \Rightarrow A}}{B \Rightarrow A \vdash (C \Rightarrow B) \Rightarrow C \Rightarrow A}}{\vdash (B \Rightarrow A) \Rightarrow (C \Rightarrow B) \Rightarrow C \Rightarrow A}}{B \Rightarrow A,\ C \Rightarrow B,\ C \vdash C \Rightarrow B \qquad B \Rightarrow A,\ C \Rightarrow B,\ C \vdash C}}{B \Rightarrow A,\ C \Rightarrow B,\ C \vdash B}$$

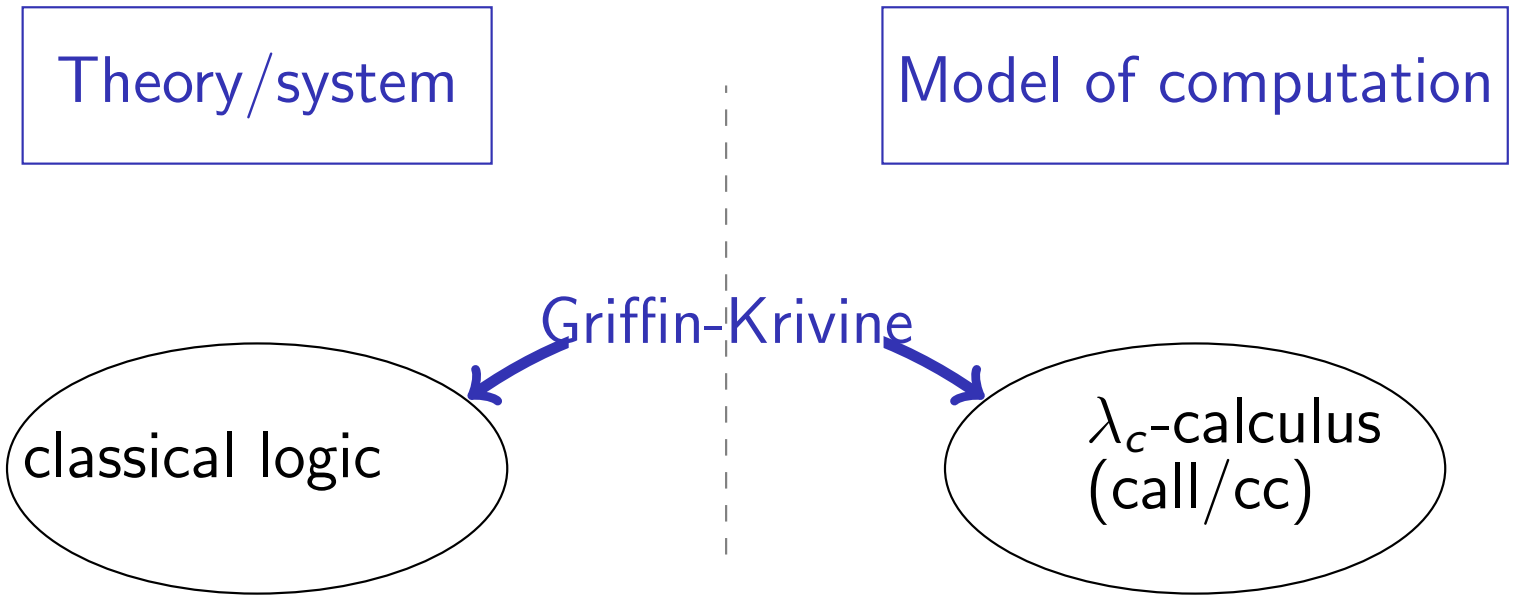
Curry-Howard isomorphism

$$\dfrac{\dfrac{\dfrac{\dfrac{x : B \Rightarrow A, y : C \Rightarrow B, z : C \vdash x : B \Rightarrow A \qquad \dfrac{x : B \Rightarrow A, y : C \Rightarrow B, z : C \vdash y : C \Rightarrow B \qquad x : B \Rightarrow A, y : C \Rightarrow B, z : C \vdash z : C}{x : B \Rightarrow A, y : C \Rightarrow B, z : C \vdash yz : B}}{x : B \Rightarrow A, y : C \Rightarrow B, z : C \vdash x(yz) : A}}{x : B \Rightarrow A, y : C \Rightarrow B \vdash \lambda z.x(yz) : C \Rightarrow A}}{x : B \Rightarrow A \vdash \lambda y.\lambda z.x(yz) : (C \Rightarrow B) \Rightarrow C \Rightarrow A}}{\vdash \lambda x.\lambda y.\lambda z(yz) : (B \Rightarrow A) \Rightarrow (C \Rightarrow B) \Rightarrow C \Rightarrow A}$$

From Curry Howard to classical realizability



From Curry Howard to classical realizability



How to realize classical logic?

Classical realizability

We assign to each formula φ

- a **"truth value"** $|\varphi|$ which is a set of programs (λ_c-terms)
- a **"falsity value"** $||\varphi||$ which is a set of stacks

Classical realizability

We assign to each formula φ

- a **"truth value"** $|\varphi|$ which is a set of programs (λ_c-terms)
- a **"falsity value"** $||\varphi||$ which is a set of stacks

No stack is in $||\top||$, every stack is in $||\bot||$

Classical realizability

We assign to each formula φ

- a **"truth value"** $|\varphi|$ which is a set of programs (λ_c-terms)
- a **"falsity value"** $||\varphi||$ which is a set of stacks

No stack is in $||\top||$, every stack is in $||\bot||$

$$||\varphi \Rightarrow \psi|| = \{\xi \cdot \pi;\ \xi \in |\varphi| \text{ and } \pi \in ||\psi||\}$$

Classical realizability

We assign to each formula φ

- a **"truth value"** $|\varphi|$ which is a set of programs (λ_c-terms)
- a **"falsity value"** $||\varphi||$ which is a set of stacks

No stack is in $||\top||$, every stack is in $||\bot||$

$$||\varphi \Rightarrow \psi|| = \{\xi \cdot \pi;\ \xi \in |\varphi| \text{ and } \pi \in ||\psi||\}$$

$\xi \in |\varphi|$ if ξ is "incompatible" with every stack in $||\varphi||$

Classical realizability

We assign to each formula φ
- a **"truth value"** $|\varphi|$ which is a set of programs (λ_c-terms)
- a **"falsity value"** $||\varphi||$ which is a set of stacks

$$\text{No stack is in } ||\top||, \text{ every stack is in } ||\bot||$$
$$||\varphi \Rightarrow \psi|| = \{\xi \cdot \pi;\ \xi \in |\varphi| \text{ and } \pi \in ||\psi||\}$$
$$\xi \in |\varphi| \text{ if } \xi \text{ is "incompatible" with every stack in } ||\varphi||$$

We denote by $\perp\!\!\!\perp$ the set of "incompatible processes" $\xi * \pi$.
We write $\xi \Vdash \varphi$ for $\xi \in |\varphi|$.

Classical realizability

We select a set $\mathcal{R}$ of "trustful programs"

$$\text{Theory} := \{\varphi \,:\, \exists \xi \in \mathcal{R}\ \xi \Vdash \varphi\}$$

forms a coherent theory closed by natural deduction

Theorem

$cc \Vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (Peirce's Law)

Classical realizability

We select a set $\mathcal{R}$ of "trustful programs"

$$\text{Theory} := \{\varphi \,:\, \exists \xi \in \mathcal{R}\ \xi \Vdash \varphi\}$$

forms a coherent theory closed by natural deduction

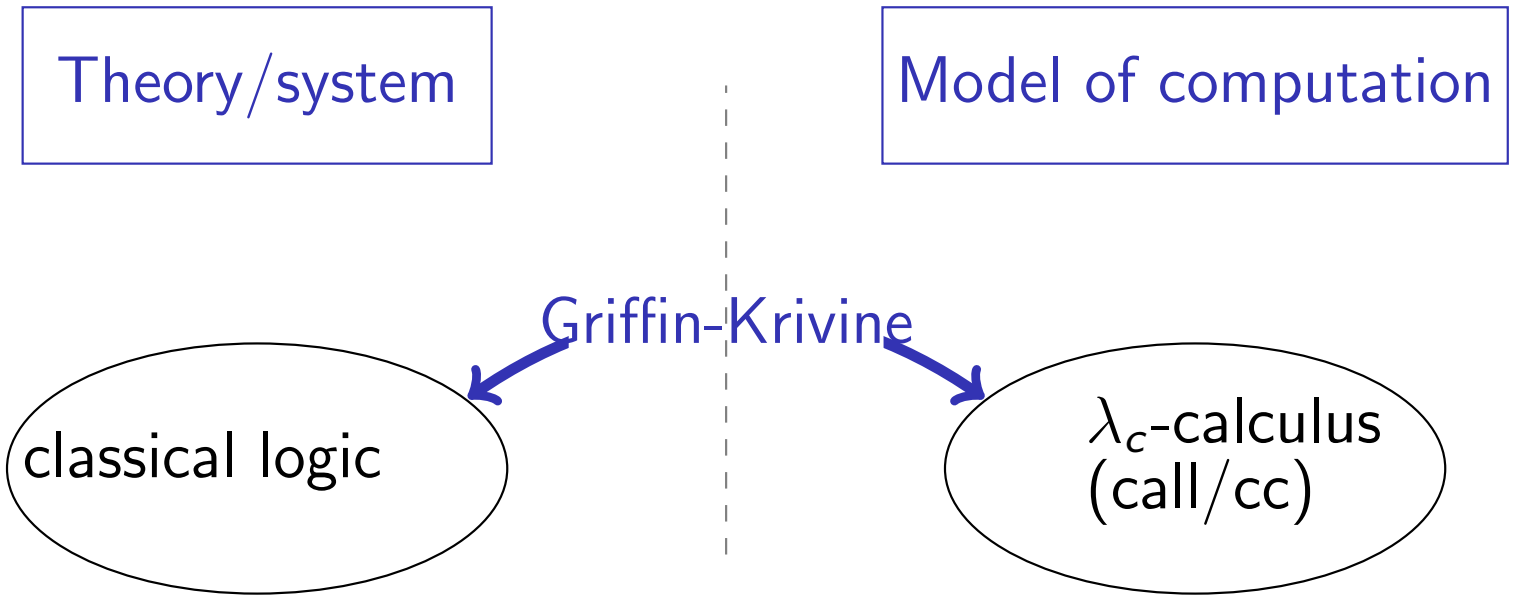
Theorem
$cc \Vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (Peirce's Law)

Any formula in the Theory can be computed in Krivine's abstract machine.

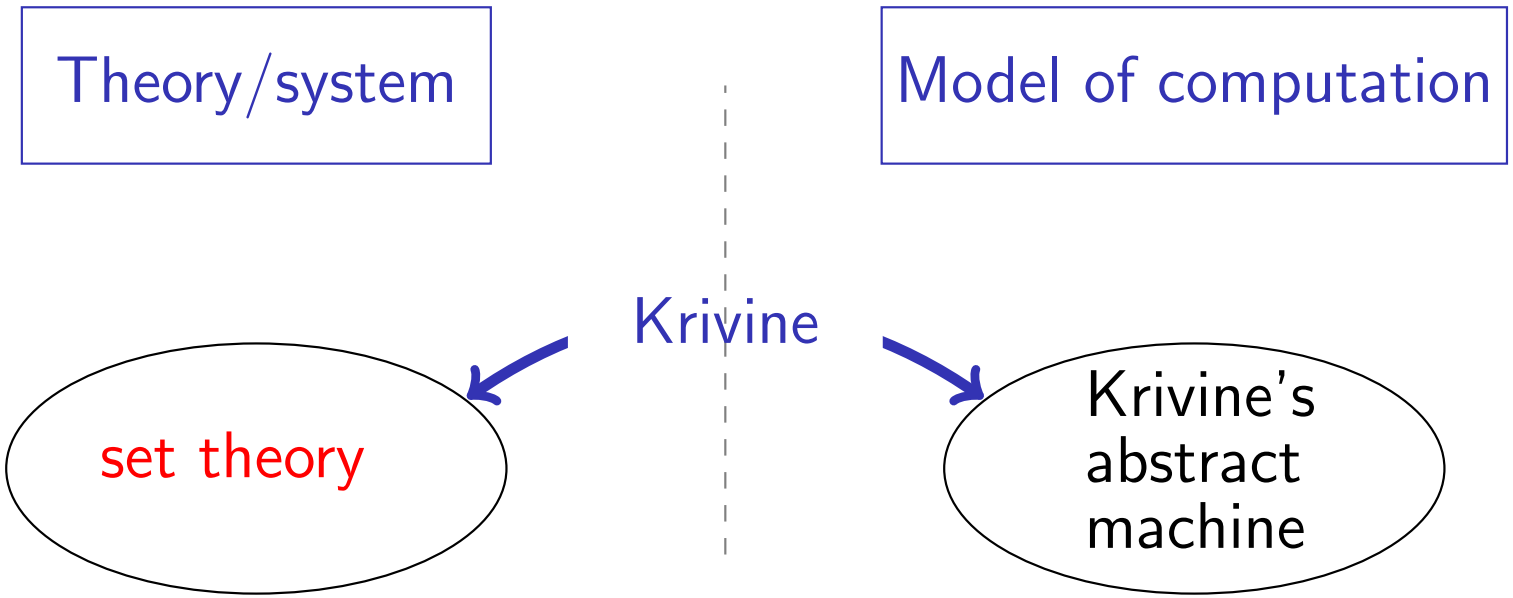
Krivine's machine

$$
\begin{array}{rcll}
tu * \pi & \succ_K & t * u \bullet \pi & (\text{push}) \\
\lambda x.t * u \bullet \pi & \succ_K & t[x := u] * \pi & (\text{grab}) \\
cc * t \bullet \pi & \succ_K & t * k_\pi \bullet \pi & (\text{save}) \\
k_{\pi'} * t \bullet \pi & \succ_K & t * \pi' & (\text{restore})
\end{array}
$$

From Curry Howard to classical realizability



From Curry Howard to classical realizability



How to realize ZF set theory?

Non extensional set theory

In order to realize the axioms of set theory, we work with a *non-extensional* version of ZF, called $\mathrm{ZF}_{\varepsilon}$.

We consider, two membership relations:

- $\in$ the usual extensional one
- ε a (strict) non-extensional one

Non extensional set theory

In order to realize the axioms of set theory, we work with a *non-extensional* version of ZF, called ZF_ε.

We consider, two membership relations:

- $\in$ the usual extensional one
- ε a (strict) non-extensional one

... and two equality relations

- $\simeq$ the usual extensional one $x \simeq y \iff \forall z(z \in x \iff z \in y)$
- $=$ Leibniz identity, i.e. two sets are identical if the satisfy the same formulae

The realizability relation

We define the two truth values $|\varphi|$ and $||\varphi||$.

- no stack is in $||\top||$, every stack is in $||\bot||$
- $||a \notin b|| = \{\pi \text{ stack } ;\ (a, \pi) \in b\}$
- $||a \subseteq b|| = \{\xi \cdot \pi;\ \exists c (c, \pi) \in a \text{ and } \xi \Vdash c \notin b\}$
- $||a \notin b|| = \{\xi \cdot \xi' \cdot \pi;\ \exists c (c, \pi) \in b \text{ and } \xi \Vdash a \subseteq c \text{ and } \xi' \Vdash c \subseteq a\}$
- $||\varphi \Rightarrow \psi|| = \{\xi \cdot \pi;\ \xi \Vdash \varphi \text{ and } \pi \in ||\psi||\}$
- $||\forall x \varphi|| = \bigcup_a ||\varphi[a/x]||$

$\xi \in |\varphi| \iff \forall \pi \in ||\varphi|| (\xi \star \pi \in \perp\!\!\!\perp)$

$\xi \Vdash \varphi$ means $\xi \in |\varphi|$

The realizability model

$$\text{Theory} := \{\varphi \,:\, \exists \xi \in \mathcal{R}\ \xi \Vdash \varphi\}$$

forms a coherent theory closed by natural deduction which contains $\mathrm{ZF}_{\in}$

The realizability model

$$\text{Theory} := \{\varphi \,:\, \exists \xi \in \mathcal{R}\ \xi \Vdash \varphi\}$$

forms a coherent theory closed by natural deduction which contains ZF_ε, but ZF_ε is a conservative extension of ZF, hence the Theory induces a model of ZF.

The realizability model

$$\text{Theory} := \{\varphi \,:\, \exists \xi \in \mathcal{R}\ \xi \Vdash \varphi\}$$

forms a coherent theory closed by natural deduction which contains ZF_ε, but ZF_ε is a conservative extension of ZF, hence the Theory induces a model of ZF.

Exemple: the identity realizes the axiom of pairing; the axiom of foundation is realized by Turing fixed point combinator; ...

The Axiom of Choice

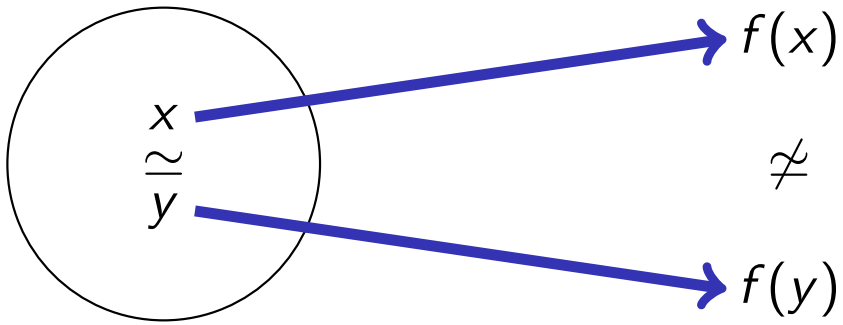
Can we realize the axiom of choice?

Non extensional axiom of choice

We can easily realize a non extensional version of AC, called NEAC
(by many different programs, for instance by the instruction 'quote')

NEAC: existence of a *non-extensional* choice function, i.e.

$$\begin{array}{lcl} x = y & \Rightarrow & f(x) = f(y), \text{ but} \\ x \simeq y & \not\Rightarrow & f(x) \simeq f(y) \end{array}$$



Realizing fragments of AC

Krivine 2003

DC can be realized (using NEAC)

Realizing fragments of AC

Krivine 2003

DC can be realized (using NEAC)

Fontanella Geoffroy 2020

Uncountable versions of AC can be realized

Realizing the full Axiom of Choice

Theorem (Krivine 2021)

There is a realizability model for the Axiom of Choice (and more)

Realizing the full Axiom of Choice

Theorem (Krivine 2021)

There is a realizability model for the Axiom of Choice (and more)

but...

... one can show that there is a realizer for AC, but we don't know which one.

Conclusions

- The proofs as algorithms/programs paradigm was developed within logical intuitionnism

Conclusions

- The proofs as algorithms/programs paradigm was developed within logical intuitionnism
- Realizability is the implementation of this paradigm

Conclusions

- The proofs as algorithms/programs paradigm was developed within logical intuitionnism
- Realizability is the implementation of this paradigm
- The paradigm and Kleene's realizability were developed as part of a broader research in constructive mathematics

Conclusions

- The proofs as algorithms/programs paradigm was developed within logical intuitionnism
- Realizability is the implementation of this paradigm
- The paradigm and Kleene's realizability were developed as part of a broader research in constructive mathematics
- ...but realizability evolved to include classical logic, set theory and even the axiom of choice

Thank you