,,

La réalisabilité: de Curry Howard au Forcing

Laura Fontanella
laura.fontanella@gmail.com
https://www.i2m.univ-amu.fr/perso/laura.fontanella/

October 6, 2020

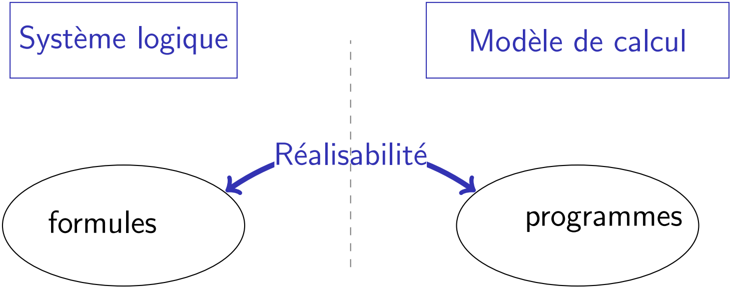
Objectif de la réalisabilité:

On cherche à interpréter les formules d'un système logique dans un modèle de calcul, afin d'extraire le contenu calculatoire des preuves mathématiques.

Kleene 1945

Interprétation des formules de l'arithmétique de Heyting par des ensembles (d'indices) de fonctions récursives.

De Curry Howard au Forcing



De Curry Howard au Forcing

Système logique

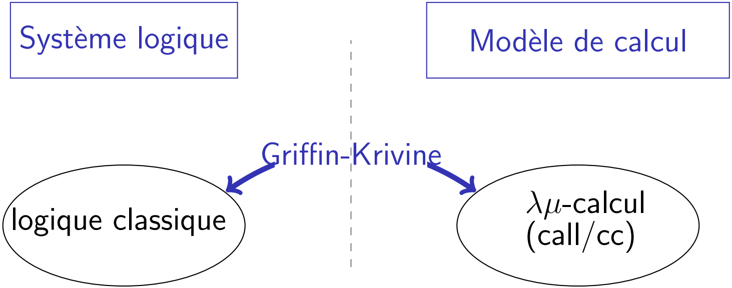
Modèle de calcul

Curry-Howard

logique intuitionniste

λ-calcul simplément typé

De Curry Howard au Forcing



De Curry Howard au Forcing

Système logique | Modèle de calcul

Krivine

théorie des ensembles | $\lambda\mu$-calcul enrichi

Forcing en bref

Cohen 1963: Indépendance de l'hypothèse du continuum de la théorie des ensembles ZF.

Forcing: technique pour construire des modèles de ZFC et montrer des résultats d'indépendance (ou de cohérence)

$$p \Vdash \varphi$$

Moralement, on attribue une probabilité p à chaque énoncé φ de la théorie des ensembles.

$$\text{Théorie} := \{\varphi \ : \ 1 \Vdash \varphi\}$$

forme une théorie cohérente

La réalisabilité classique en bref

En réalisabilité classique on travaille avec des processus $\xi * \pi$ où ξ est un terme du $\lambda\mu$-calcul enrichi et π est une pile.

- Λ l'ensemble des termes ($\lambda\mu$- termes) qui jouent le rôle de "témoins de vérité"
- Π l'ensemble des piles qui jouent le rôle de "témoins de fausseté"

Donc à toute formule φ on associe

- une valeur de vérité $|\varphi| \subseteq \Lambda$
- une valeur de fausseté $||\varphi|| \subseteq \Pi$

qui sont définies simultanément par induction sur la formule:

$\xi \in |\varphi|$ si ξ est "incompatible" avec toute pile dans $||\varphi||$ (où $||\varphi||$ sera défini plus tard)

Algèbres de réalisabilité

Pour construire un modèle de réalisabilité pour la théorie des ensembles on définit une algèbre de réalisabilité

Les ingrédients d'une algèbre de réalisabilité

- Λ l'ensemble des termes
- Π l'ensemble des piles
- $\mathcal{R}$ l'ensemble des réalisateurs/quasi-preuves
- $\prec_K$ la rélation d'execution sur les processus, qui défini la machine de Krivine
- $\perp\!\!\!\perp$ le pôle, qui définit les processus "incompatibles"

Termes et piles

L'ensemble des termes et l'ensemble des piles sont définies par la grammaire suivante (modulo α-équivalence)

$$
\begin{array}{llcll}
\lambda\mu\textbf{-terms} & t, u & ::= & x & \text{(variable)} \\
 & & \mid & tu & \text{(application)} \\
 & & \mid & \lambda x.t & \text{(abstraction, où } x \text{ est une variable} \\
 & & & & \text{et } t \text{ un } \lambda\mu\text{-term)} \\
 & & \mid & cc & \text{(call-with-current-continuation)} \\
 & & \mid & k_\pi & \text{(constante de continuation,où } \pi \text{ est une pile)} \\
 & & \mid & \xi_\gamma & \text{(instructions spéciales)} \\
 & & & & \\
\textbf{Stacks} & \pi & ::= & \omega_\gamma & \text{(piles atomiques)} \\
 & & \mid & t \bullet \pi & \text{(où } t \text{ est un } \lambda\mu\text{-term clos et } \pi \text{ une pile)}
\end{array}
$$

L'application est associative à gauche: $tu_1 u_2 \dots u_n$ signifie $(\dots((tu_1)u_2)\dots)u_n$

Les processus et les réalisateurs

Un processus est un couple $(\xi, \pi) \in \Lambda \times \Pi$ noté $\xi * \pi$. L'ensemble des processus est noté $\Lambda * \Pi$.

L'ensemble des réalisateurs/quasi-preuves, noté $\mathcal{R}$ est l'ensemble de tous les $\lambda\mu$-termes clos qui ne contiennent aucune occurrence de la constante de continuation.

Spoiler alert: c'est les termes "fiables", le modèle de réalisabilité $\mathcal{N}$ est défini par les formules qui sont réalisées par ces termes.

$$\mathcal{N} \models \varphi \iff \exists \xi \in \mathcal{R}(\xi \Vdash \varphi)$$

La machine de Krivine

La relation d'execution $\prec_K$ est un pre-ordre sur l'ensemble des processus tel que

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

Selon le contexte on peut rajouter des règles d'évaluation pour les instructions spéciales.

Le pole

Le pole noté $\perp\!\!\!\perp$ est un segment final de l'ensemble des processus.

un terme ξ et une pile π sont "incompatibles" si $\xi * \pi \in \perp\!\!\!\perp$

Condition de cohérence
Un réalisateur ne peut pas être incompatible avec toute pile

$$\forall \xi \in \mathcal{R} \exists \pi \in \Pi (\xi * \pi \notin \perp\!\!\!\perp)$$

Algèbres de réalisabilité vs Forcing

Un ensemble de forcing est un cas particulier d'algèbre de réalisabilité, en effet à partir d'une algèbre de Boole $(\mathbb{B}, 0, 1, \leq, \vee, \neg)$ on peut définire une algèbre de réalisabilité comme suit:

- Λ est l'ensembles de $\lambda\mu$-termes sans instructions supplémentaires
- Π contient une pile atomique pour chaque condition de B
- Pour définir $\prec$, on interprète les termes et les piles à l'aide de la fonction suivante $\tau : \Lambda \cup \Pi \to \mathbb{B}$:
  - $\tau(p) := p$, pour toute pile atomique p
  - $\tau(t \bullet \pi) := \tau(t) \wedge \tau(\pi)$, pour tout terme t et toute pile π
  - $\tau(x) := \tau(cc) := 1$, pour toute variable x
  - $\tau(tu) := \tau(t) \wedge \tau(u)$, pour tout $\lambda\mu$-terms t, u
  - $\tau(\lambda x.t) := \tau(t)$, pour toute variable x et tout terme t
  - $\tau(k_\pi) := \tau(\pi)$, pour tout π
- On définit $t_1 * \pi_1 \succ t_2 * \pi_2$ ssi $\tau(t_1) \wedge \tau(\pi_1) \leq \tau(t_2) \wedge \tau(\pi_2)$
- On définit $\perp\!\!\!\perp$ comme l'ensemble de tous les processus tels que $\tau(t) \wedge \tau(\pi) = 0$.

Algèbre de réalisabilité vs Forcing

...moralement:

- $\Lambda = \Pi = \mathbb{B}$
- $pq = p \bullet q = p * q = p \wedge q$
- $k_p = p$
- R=$\{1\}$
- $p \succ q \iff p \leq q$ (i.e. $p \wedge q = p$)
- $\perp\!\!\!\perp = \{0\}$

La théorie des ensembles non extensionnelle

Pour réaliser les axiomes de la théorie des ensembles, on travaille avec une version *non extensionnelle* de ZF.

On considère deux relations d'appartenance:

- $\in$ l'appartenance usuelle extensionnelle
- ε l'appartenance non extensionnelle

... et deux relations d'égalité:

- $\simeq$ l'égalité extensionnelle $x \simeq y \iff \forall z(z \in x \iff z \in y)$
- $=$ l'identité de Leibniz, i.e. deux ensembles sont identique ssi ils satisfont les mêmes énoncés

On définit alors la théorie ZF_ε qui est une extension conservative de ZF.

La théorie des ensembles non extensionnelle ZF_ε

0. **Axiome d'extensionnalité:**

$$\forall x \forall y [x \in y \iff \exists z \varepsilon y \ (x \simeq z)];$$
$$\forall x \forall y [x \subseteq y \iff \forall z \varepsilon x \ (z \in y)].$$

1. **Axiome de la paire:** $\forall a \ \forall b \ \exists x \ (a \ \varepsilon \ x \wedge b \ \varepsilon \ x)$.
2. **Axiome de la reunion:** $\forall a \ \exists b \ \forall x \varepsilon a \ \forall y \varepsilon x \ (y \ \varepsilon \ b)$.
3. **Axiome des parties:** pour toute formule $F(x, z_1, \ldots, z_n))$

$$\forall a \ \exists b \ \forall z_1 \ldots \forall z_n \ \exists y \varepsilon b \ \forall x \ (x \ \varepsilon \ y \iff (x \ \varepsilon \ a \wedge F(x, z_1, \ldots, z_n)))$$

4. **Axiome de remplacement:** pour toute formules $F(x, y, z_1, \ldots, z_n)$,

$$\forall z_1 \ldots \forall z_n \ \forall a \ \exists b \ \forall x \varepsilon a \ (\exists y \ F(x, y, z_1, \ldots, z_n) \Rightarrow \exists y \varepsilon b \ F(x, y, z_1, \ldots, z_n))$$

5. **Axiome de fondation:** pour toute formules $F(x, z_1, \ldots, z_n)$,

$$\forall z_1 \ldots \forall z_n \ \forall a \ (\forall x \ (\forall y \ \varepsilon \ x \ (F(y, z_1, \ldots, z_n) \Rightarrow F(x, z_1, \ldots, z_n))) \Rightarrow F(a, z_1, \ldots, z_n))$$

6. **Axiome de l'infini:** for every formula $F(x, y, z_1, \ldots, z_n)$,

$$\forall z_1 \ldots \forall z_n \ \forall a \ \exists b \ (a \ \varepsilon \ b \wedge \forall x \varepsilon b \ (\exists y \ F(x, y, z_1, \ldots, z_n) \Rightarrow \exists y \varepsilon b \ F(x, y, z_1, \ldots, z_n)))$$

Ground model et langage de réalisabilité

On se donne un modèle $\mathcal{M}$ de *ZFC* appelé ground model, l'algèbre de réalisabilité $\mathcal{A}$ est définie dans ce modèle.

Le langage de réalisabilité

C'est une extension du langage de ZF_ε où on rajoute:

- un nouveau symbole de constant pour chaque élément de $\mathcal{M}$
- un nouveau symbol de fonction pour chaque fonction-classe définissable à paramètres dans $\mathcal{M}$

Les valeurs de vérité et de fausseté

Pour toute formule φ du langage de réalisabilité ZF_ε on définit par induction la valeur de vérité de φ, notée $|\varphi|$ et sa valeure de fausseté notée $||\varphi||$.

- $|\varphi| = \{t \in \Lambda;\ \forall \pi \in \|\varphi\|\ (t * \pi \in \perp\!\!\!\perp)\}$
- $\|\top\| = \emptyset,\ \|\bot\| = \Pi,$
- $\|a \not\in\!\!\!\!\!\!\: \varepsilon\ b\| = \{\pi \in \Pi;\ (a, \pi) \in b\}$
- $\|a \subseteq b\|$ et $\|a \notin b\|$ sont définies simultanément:
  - $\|a \subseteq b\| = \{t \bullet \pi;\ (t, \pi) \in \Lambda \times \Pi,\ (c, \pi) \in a \text{ and } t \in |c \notin b|\}$
  - $\|a \notin b\| = \{t \bullet t' \bullet \pi;\ (t, t', \pi) \in \Lambda \times \Lambda \times \Pi,\ (c, \pi) \in b,\ \ t \in |a \subseteq c|,\ \ t' \in |c \subseteq a|\},$
- $\|A \Rightarrow B\| = \{t \bullet \pi; (t, \pi) \in \Lambda \times \Pi,\ \ t \in |A|, \pi \in \|B\|\},$
- $\|\forall x A\| = \{\pi \in \Pi;\ \exists a(\pi \in \|A[a/x]\|)\},$

On écrit $t \Vdash \varphi$ pour $t \in |\varphi|$.

Le modèle de réalisabilité

Les théorèmes suivants montrent que l'ensemble des énoncés qui sont réalisés forme une théorie classique cohérente qui contient ZF_ε

Lemme d'adéquation (Krivine RA2)

Si A est une formule de ZF_ε, alors $\vdash t : A$ implique $t \Vdash A$.

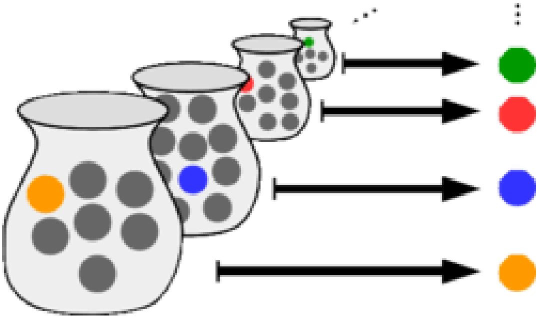
Théoreme (Krivine RA2)

- La loi de Peirce est réalisée, i.e. pour toute pair de formules A, B, on a $cc \Vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$.
- Les axiomes de ZF_ε sont réalisés.
- $\perp$ n'est pas réalisé ssi la condition de cohérence sur $\mathcal{R}$ est respectée.

... on appelle modèle de réalisabilité n'importe quel modèle de cette théorie cohérente. On notera par $\mathcal{N}_\varepsilon$ le modèle de réalisabilité vu comme un modèle de ZF_ε et par $\mathcal{N}_\in$ le modèle de ZF correspondant.

L'Axiome du Choix

Peut-on réaliser l'axiome du choix?

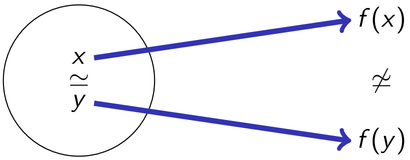


L'axiome du choix non extensionnel

On peut réaliser l'axiome du choix non extensionnel, NEAC
(par exemple en rajoutant l' instruction 'quote')

NEAC: Existence d'une fonction de choix non extensionnelle c-à-d.

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



Réaliser l'axiome du choix

Krivine 2004

En utilisant NEAC, on peut réaliser DC

$$AC \iff \forall \kappa \in Ord\ (AC_\kappa)$$
$$DC = AC_\omega$$

Fontanella Geoffroy 2020

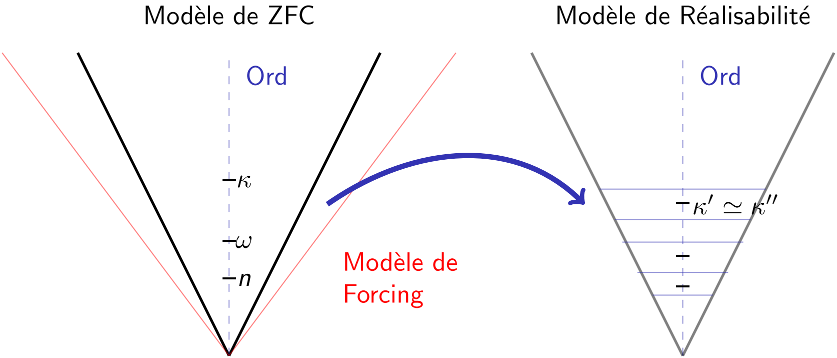
Pour tout cardinal κ, on peut construire un modèle de réalisabilité pour $ZF + AC_\kappa$

L'axiome du choix restreint

L'axiome du choix restreint, AC_κ

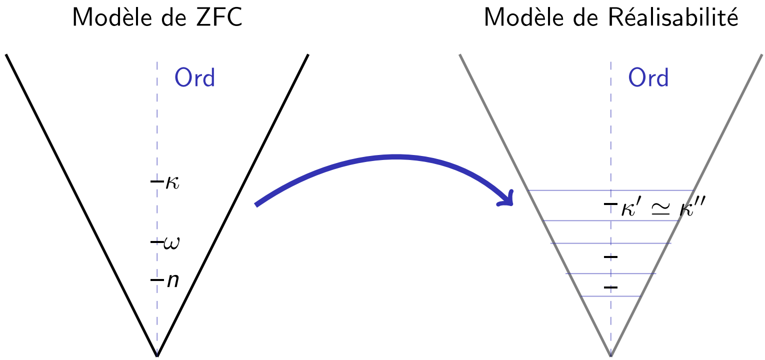
Soit X un ensemble non vide et R une relation binaire sur X telle que pour tout $\alpha < \kappa$ et toute R-chaine $s = (s_\beta)_{\beta<\alpha}$ de longueur α peut etre prolongée (i.e. il existe un élément $y \in X$ tel que $s_\beta \ R \ y$ pour tout $\beta < \alpha$), alors il existe une R-chaine de longueur κ.

Position du problème



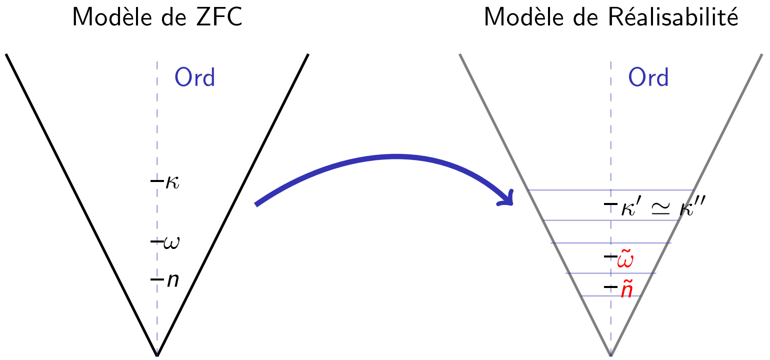
Contrairement au Forcing les ordinaux du modèle de réalisabilité n'ont à priori aucun rapport avec les ordinaux du modèle de depart. On trouve sur les modèle de réalisabilité $\mathcal{N}_\varepsilon$ des classes d'ordinaux $\simeq$-équivalents. Pour réaliser AC il faudrait définire une fonction de choix sur tous ces ordinaux.

Position du problème



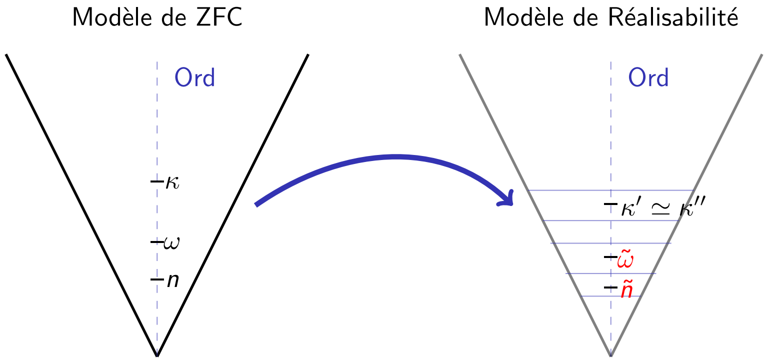
On peut réaliser assez facilement NEAC, donc pour réaliser AC il suffirait de choisir des représentants pour chaque classe d'équivalence, d'appliquer NEAC sur ces représentants et d'assigner aux autres ordinaux la même valeure que leur représentant.

Position du problème



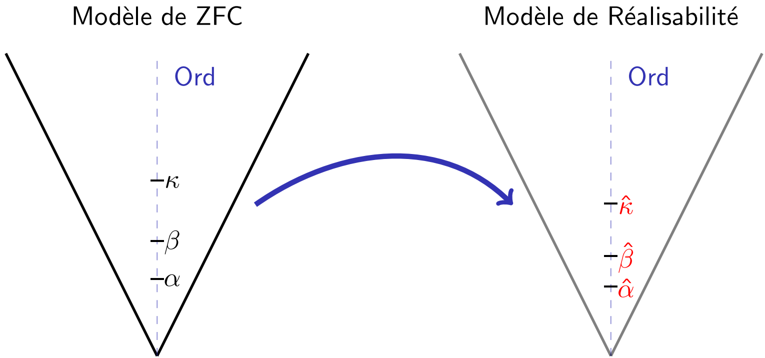
On peut "représenter" les entiers assez facilement par exemple en les intégrant au $\lambda\mu$-termes puis on utilisant l'instruction supplémentaire 'quote' (Krivine RA2). On réalise ainsi $AC_\omega = DC$.

Position du problème



Pour les ordinaux transfinis la situation est un peu plus complèxes (on n'a pas de λ-termes pour ces ordinaux).

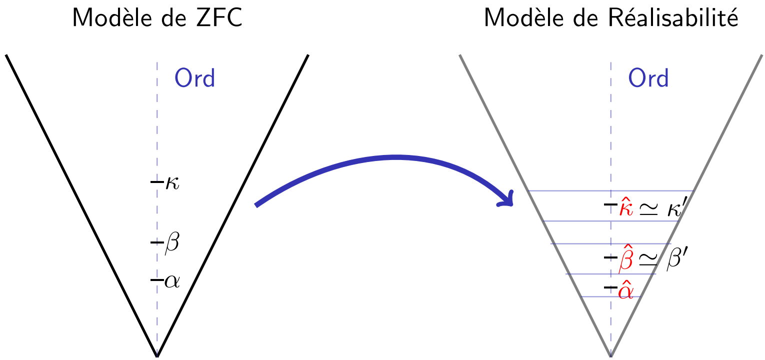
Fontanella Geoffroy 2020



Fontanella Geoffroy 2020

À partir d'un modèle $\mathcal{M}$ de ZF avec une fonction de choix globale on peut définir pour tout cardinal κ de $\mathcal{M}$ un modèle de réalisabilité où κ a un représentant $\hat{\kappa}$ tel que $ZF + AC_{\hat{\kappa}}$ est réalisé

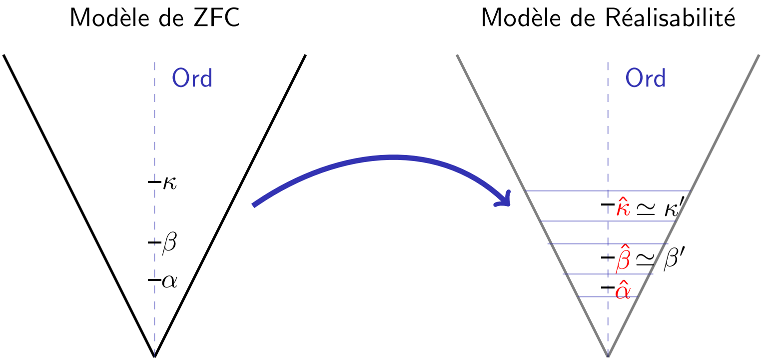
Fontanella Geoffroy 2020



Sketch - les représentants

- On se donne une algèbre qui contient κ termes
- On rajoute une intruction χ qui "réalise l'ordre total sur ces termes"
- À partir de ces termes on définit pour tout ordinal $\alpha \leq \kappa$ dans le ground model un ensemble $\hat{\alpha}$
- On montre que les ordinaux chapeaux "représentent" leur contrepart du ground model.

Fontanella Geoffroy 2020



Sketch - on réalise $AC_{\hat{\kappa}}$

- $\hat{\kappa}$ admet un $=$-unique représentant de chacune de ses $\simeq$-classes d'éléments
- NEAC entraine une fonction de choix non extensionnelle sur ces représentants
- on attribue la même valeur aux autres éléments de la même classe
- ainsi on réalise $AC_{\hat{\kappa}}$

Réaliser l'Axiome du Choix

Théorème (Krivine, en preparation)

Il existe un modèle de réalisabilité pour l'axiome du choix

Réaliser l'Axiome du Choix

Théorème (Krivine, en preparation)

Il existe un modèle de réalisabilité pour l'axiome du choix

Mais...

... on montre qu'il existe un réalisateur pour AC, mais on ne sait pas lequel.

Réaliser l'Axiome du Choix

Théorème (Krivine, en preparation)

Il existe un modèle de réalisabilité pour l'axiome du choix

Mais...

... on montre qu'il existe un réalisateur pour AC, mais on ne sait pas lequel.

De plus, en utilisant un théorème de Toschimichi Usuba, on peut montrer que le modèle de Krivine pour AC est en réalité une "petite" extension d'un modèle de ZFC, c'est à dire qu'on peut obtenir ce modèle par des méthodes classiques de théorie des ensembles.