Realizing realizability results with classical constructions

Asaf Karagila

University of East Anglia

19 September 2019

Realizability Workshop 2019
CIRM

DISCLAIMER:

I do not know anything about realizability, other than that it is a thing. When I inevitably say something silly, *please* correct me.

Krivine used realizability methods to construct a model of set theory in which there is an increasing sequence of subsets $A_n \subseteq \mathbb{R}$ and:

1. ZF + DC hold.
2. $|A_m| <^* |A_n|$ if and only if $m < n$. $|X| \leqslant^* |Y| \iff \exists Y' \subseteq Y\, \exists f : Y' \twoheadrightarrow X$
3. For $n > 1$, A_n is uncountable.
4. $|A_n \times A_m| = |A_{nm}|$.

We will see today how to create such model using forcing, or rather symmetric extensions, and how our existing understanding of symmetric extensions allows us to easily obtain better results which were recently obtained by Krivine, Fontanella, and Geoffroy in the realizability settings.

These results appear in the paper “Realizing realizability results with classical constructions”, **arXiv:1905.08202**.

Forcing conventions:

1. A notion of forcing is a preordered set, $\mathbb{P}$, with a maximum, $\mathbb{1}$.
2. For $p, q \in \mathbb{P}$ we write $q \leqslant p$ to mean that q is *stronger* than p.
   We will also do our best to follow Goldstern's alphabet convention.
3. We use $\dot{x}$ to denote names, and a name is a set whose elements are $\langle p, \dot{y}\rangle$ where $p \in \mathbb{P}$ and $\dot{y}$ is also a name.
4. We use $\check{x}$ to denote the canonical name for x in the ground model:
   $\check{x} = \{\langle \mathbb{1}, \check{y}\rangle \mid y \in x\}$.
5. If $\{\dot{x}_i \mid i \in I\}$ is a family of names, we write $\{\dot{x}_i \mid i \in I\}^\bullet$ to mean the obvious name: $\{\langle \mathbb{1}, \dot{x}_i\rangle \mid i \in I\}$. Now $\check{x} = \{\check{y} \mid y \in x\}^\bullet$. This will also naturally extend to ordered pairs, sequences, etc.
6. If $\dot{x}$ is a name, we say that $\dot{y}$ *appears in* $\dot{x}$ if there is some condition p that $\langle p, \dot{y}\rangle \in \dot{x}$.

Let $\mathbb{P}$ be a notion of forcing, and let π be an automorphism of $\mathbb{P}$. Then we can define by recursion an action of π on the $\mathbb{P}$-names:

$$\pi\dot{x} = \{\langle \pi p, \pi\dot{y}\rangle \mid \langle p, \dot{y}\rangle \in \dot{x}\}.$$

Lemma (The Symmetry Lemma)

$$p \Vdash \varphi(\dot{x}) \iff \pi p \Vdash \varphi(\pi\dot{x}).$$

Proposition

If x is in the ground model, then $\pi\check{x} = \check{x}$.

Proof.

Note that $\pi\mathbb{1} = \mathbb{1}$ and use induction. $\square$

Definition

Let $\mathscr{G}$ be a group. We say that $\mathscr{F}$ is a *filter of subgroups* (on $\mathscr{G}$) if it is a filter on the lattice of subgroups of $\mathscr{G}$. Namely, $\mathscr{F}$ is a non-empty set of subgroups of $\mathscr{G}$ which is closed under intersections and supergroups.
$\mathscr{F}$ is a *normal filter* if whenever $\pi \in \mathscr{G}$ and $H \in \mathscr{F}$, then $\pi H \pi^{-1} \in \mathscr{F}$.

Definition

We say that $\langle \mathbb{P}, \mathscr{G}, \mathscr{F} \rangle$ is a *symmetric system* if $\mathbb{P}$ is a notion of forcing, $\mathscr{G}$ is a subgroup of $\mathrm{Aut}(\mathbb{P})$, and $\mathscr{F}$ is a normal filter of subgroups on $\mathscr{G}$.

Let us fix a symmetric system for now, $\langle \mathbb{P}, \mathscr{G}, \mathscr{F} \rangle$.

For a name $\dot{x}$ we define $\operatorname{sym}_{\mathscr{G}}(\dot{x}) = \{\pi \in \mathscr{G} \mid \pi\dot{x} = \dot{x}\}$. We say that $\dot{x}$ is $\mathscr{F}$*-symmetric* if $\operatorname{sym}_{\mathscr{G}}(\dot{x}) \in \mathscr{F}$. We say that $\dot{x}$ is *hereditarily* $\mathscr{F}$*-symmetric* if this holds hereditarily as well. We denote by $\mathsf{HS}_{\mathscr{F}}$ the class of all hereditarily $\mathscr{F}$-symmetric names.

Theorem

Let $G \subseteq \mathbb{P}$ be a V-generic filter, and let $M = \mathsf{HS}^G_{\mathscr{F}} = \{\dot{x}^G \mid \dot{x} \in \mathsf{HS}_{\mathscr{F}}\}$. Then M is a transitive class of $V[G]$, $V \subseteq M$, and $M \models \mathsf{ZF}$.

Such M is called a *symmetric extension*.

We will omit the subscripts whenever no confusion can occur, which is everywhere for our purpose.

We also have a forcing relation, $\Vdash^{\mathsf{HS}}$, with the usual truth lemma:

Theorem

The following are equivalent:

- $p \Vdash^{\mathsf{HS}} \varphi(\dot{x})$.
- *For every V-generic filter G such that $p \in G$, $\mathsf{HS}^G \models \varphi(\dot{x}^G)$.*

And we have a symmetry lemma relative to $\mathscr{G}$:

Lemma

Suppose that $\pi \in \mathscr{G}$, then

$$p \Vdash^{\mathsf{HS}} \varphi(\dot{x}) \iff \pi p \Vdash^{\mathsf{HS}} \varphi(\pi \dot{x}).$$

Example: The real numbers cannot be well-ordered

Let $\mathbb{P}$ be $\mathrm{Add}(\omega, \omega_1)$, so $p \in \mathbb{P}$ is a finite partial function from $\omega_1 \times \omega \to 2$. Next define $\mathscr{G}$ as the group of all permutations of ω_1. The action of $\mathscr{G}$ on $\mathbb{P}$ is given by

$$\pi p(\pi\alpha, m) = p(\alpha, m).$$

For $E \subseteq \omega_1$, let $\mathrm{fix}(E) = \{\pi \in \mathscr{G} \mid \pi \upharpoonright E = \mathrm{id}\}$. We take $\mathscr{F}$ to be the filter generated by $\{\mathrm{fix}(E) \mid E \in [\omega_1]^{<\omega_1}\}$.

For $\alpha < \omega_1$, define $\dot{a}_\alpha = \{\langle p, \check{m}\rangle \mid p(\alpha, m) = 1\}$, and $\dot{A} = \{\dot{a}_\alpha \mid \alpha < \omega_1\}^\bullet$.

Proposition

$\pi\dot{a}_\alpha = \dot{a}_{\pi\alpha}$, and consequently, $\pi\dot{A} = \dot{A}$ for all $\pi \in \mathscr{G}$. □

Corollary

$\mathrm{sym}(\dot{a}_\alpha) = \mathrm{fix}(\{\alpha\})$ and $\mathrm{sym}(\dot{A}) = \mathscr{G}$. Therefore $\dot{a}_\alpha$ and $\dot{A}$ are in HS. □

Continuing...

Proposition

Suppose that $\dot{x}$ is a name such that $\mathbb{1} \Vdash \dot{x} \subseteq \check{\omega}$. Then there is $\dot{x}_* \in$ HS such that $\mathbb{1} \Vdash \dot{x} = \dot{x}_*$.

Proof.

Since $\mathbb{P}$ is a c.c.c. forcing, for every n, there is a countable maximal antichain D_n such that $p \in D_n$ decides the truth value of $\check{n} \in \dot{x}$. Let $\dot{x}_*$ be defined as follows,

$$\dot{x}_* = \{\langle p, \check{n}\rangle \mid p \in D_n, p \Vdash \check{n} \in \dot{x}\}.$$

It is not hard to see that $\mathbb{1} \Vdash \dot{x} = \dot{x}_*$. As each D_n is countable, there is some $\alpha < \omega_1$ large enough such that every condition $p \in D_n$ only mentions ordinals below α. Therefore $\mathrm{fix}(\alpha) \subseteq \mathrm{sym}(\dot{x}_*)$. □

Finishing. . .

Theorem

$\mathbb{1} \Vdash^{\mathsf{HS}} \dot{\mathbb{R}}$ *cannot be well-ordered.*

Proof.

Suppose $\dot{f} \in \mathsf{HS}$ and $p \Vdash^{\mathsf{HS}} \dot{f}\colon \dot{\mathbb{R}} \to \check{\eta}$, where η is some ordinal. Let E be a large enough countable set so that $\operatorname{dom} p \subseteq E \times \omega$, and $\operatorname{fix}(E) \subseteq \operatorname{sym}(\dot{f})$.
Pick some $\alpha > \sup E$ and let $q \leqslant p$ be a condition such that for some ordinal γ, $q \Vdash \check{\gamma} = \dot{f}(\dot{a}_\alpha)$. Take $\beta > \alpha$ such that β is not mentioned in q, and let π be the 2-cycle $(\alpha\ \beta)$. Clearly, $\pi \in \operatorname{fix}(E)$, so $\pi\dot{f} = \dot{f}$ and $\pi p = p$. By the symmetry lemma tells us that $\pi q \Vdash \pi\check{\gamma} = \pi\dot{f}(\pi\dot{a}_\alpha) = \dot{f}(\dot{a}_\beta) = \check{\gamma}$. But it is easy to see that q and πq are compatible. So $q \cup \pi q \Vdash \dot{f}$ is not injective.
Therefore there is no condition that has an extension forcing that $\dot{f}$ is injective, for any $\dot{f}$. Therefore $\mathbb{1} \Vdash^{\mathsf{HS}} \dot{\mathbb{R}}$ cannot be well-ordered. $\square$

In fact a modification of this proof shows more: it shows that if $\dot{f} \in \mathsf{HS}$ and $p \Vdash^{\mathsf{HS}} \dot{f}\colon \dot{A} \to \check{\eta}$, then $p \Vdash^{\mathsf{HS}} \operatorname{rng}(\dot{f})$ is countable.

We could have taken a different permutation group, e.g. one that preserves a certain structure, and we could have taken a different filter of subgroups, e.g. one that is generated by pointwise stabilizers of non-stationary sets, and the resulting models would be different.

The main philosophy behind symmetric extensions (especially those given by adding Cohen reals) is that we can add a copy of a structure and preserve it with our automorphisms, and that will produce what is (usually) a non-well ordered set with the structure we preserve.

If you want to have it, preserve it!

Definition

Dependent Choice (DC) states that if X is a non-empty set, R is a binary relation on X such that $\operatorname{dom} R = X$, then there is a function $f\colon \omega \to X$ such that $f(n)\ R\ f(n+1)$.

The following are equivalents of DC:

1. In every partial order there is a maximal element or an infinite chain.
2. Every tree of height ω has a maximal node or a branch.
3. Well-founded relations are exactly those without decreasing infinite chains.
4. And many *many* others.

Definition

Let κ be an infinite cardinal. DC_κ is the statement that if $\langle X, \leqslant\rangle$ is a partial order, and every chain of order type $< \kappa$ has an upper bound, then there is a maximal element, or a chain of order type κ. $\mathsf{DC}_{<\kappa}$ means $\forall\lambda < \kappa : \mathsf{DC}_\lambda$.

Definition

Suppose that $M \subseteq V$ are models of ZF with the same ordinals. We say that M is κ-closed in V if whenever $\alpha < \kappa$ and $f\colon \alpha \to M$ is a function in V, then $f \in M$.

Theorem

Suppose that $M \subseteq V$ such that $V \models \mathsf{ZF} + \mathsf{DC}_{<\kappa}$ and M is κ-closed, then $M \models \mathsf{DC}_{<\kappa}$. □

Theorem

Suppose that $\langle \mathbb{P}, \mathscr{G}\, \mathscr{F}\rangle$ is a symmetric system such that $\mathscr{F}$ is a κ-complete filter of groups. If $\mathbb{P}$ is κ-closed or has κ-c.c., then $\mathbb{1} \Vdash^{\mathsf{HS}} \mathsf{DC}_{<\kappa}$.

Corollary

Suppose that $\langle \mathrm{Add}(\omega, \lambda), \mathscr{G}, \mathscr{F}\rangle$ is a symmetric system, then $\mathsf{DC}_{<\kappa}$ holds in the symmetric extension, where κ is the completeness of $\mathscr{F}$.

Definition

For a set X, AC_X states that if $\{A_x \mid x \in X\}$ is a family of non-empty sets, then it admits a choice function. AC denotes $\forall X : \mathsf{AC}_X$ and $\mathsf{AC}_{\mathsf{WO}}$ denotes $\forall \alpha \in \mathrm{Ord} : \mathsf{AC}_\alpha$.

We have a condition that guarantees a symmetric extension to preserve AC_X (including X which are generically added) and in particular $\mathsf{AC}_{\mathsf{WO}}$. It is overly technical for this talk, but here is a “simplified” version.

Theorem

Suppose that $\langle \mathrm{Add}(\omega, X), \mathscr{G}, \mathscr{F}\rangle$ is a symmetric system such that $\mathscr{G}$ is a group of permutations of X acting on the forcing naturally, and $\mathscr{G}$ is transitive on X, and suppose that $\mathscr{F}$ is given by $\mathrm{fix}(E)$ where $E \in [X]^{\leqslant\kappa}$ for some infinite κ. Then $\mathbb{1} \Vdash^{\mathsf{HS}} \mathsf{AC}_{\dot X} \wedge \mathsf{AC}_{\mathsf{WO}}$, where $\dot X$ is the canonical name for the added reals.

So in our example a few slides ago, $\mathbb{1} \Vdash^{\mathsf{HS}} \mathsf{AC}_{\dot A}$ and $\mathsf{AC}_{\mathsf{WO}}$, and DC. This will also be true for the construction we will present now.
(Note: $\mathsf{AC}_{\mathsf{WO}}$ implies DC, but not $\mathsf{DC}_{\aleph_1}$. So we will still want to have nice closure properties for $\mathscr{F}$.)

Let X be $\omega_1 \times \mathbb{Q}$ let and $\prec$ denote the lexicographic order. Let $\mathbb{P}$ denote $\operatorname{Add}(\omega, X)$. We let $\mathscr{G}$ be the automorphism group of the linear order $\langle X, \prec\rangle$. Note that this action is "very" transitive. Finally, $\mathscr{F}$ is generated by $\{\operatorname{fix}(E) \mid E \in [X]^{<\omega_1}\}$. Of course, $\mathscr{F}$ is $\aleph_1$-closed, so $\mathsf{AC}_{\mathsf{WO}}$ and DC will hold at the symmetric extension.

For $x \in X$, let $\dot{a}_x$ denote the canonical name of the real on the xth coordinate. And as before, $\dot{A} = \{\dot{a}_x \mid x \in X\}^\bullet$. And $1 \Vdash^{\mathsf{HS}} \mathsf{AC}_{\dot{A}}$.

Proposition

$\pi\dot{a}_x = \dot{a}_{\pi x}$, and therefore $\pi\dot{A} = \dot{A}$ for any $\pi \in \mathscr{G}$.

Corollary

$\dot{a}_x, \dot{A} \in \mathsf{HS}$. $\dot{\prec} = \{\langle \dot{a}_x, \dot{a}_y\rangle^\bullet \mid x \prec y\}^\bullet \in \mathsf{HS}$.

And it is easy to see that $\mathbb{1} \Vdash^{\mathsf{HS}}$ "$\dot{\prec}$ is a linear order on $\dot{A}$". Even more, since we have countable supports, $\mathbb{1} \Vdash^{\mathsf{HS}}$ "Every subset of $\dot{A}$, bounded in $\dot{\prec}$, can be embedded into $\check{\mathbb{Q}}$". Why did we need the order, though?

Krivine's proof (in *Realizability Algebras II*) proceeds with the following steps:

1. Prove that $\gimel\mathbf{m} \subseteq \gimel\mathbf{n}$ is an increasing sequence of sets with the wanted properties.
2. Prove that $\gimel\mathbf{2}$ has a natural Boolean algebra structure.

So A_n, for Krivine, is simply $\gimel\mathbf{n}$.

We suggest to think about this as somehow a Boolean-valued ultrapower. In effect we are constructing something which "feels like" an ultrapower of $\mathbb{N}$. One natural way to think about this in the case of forcing is using names. We consider names—*symmetric names*—for natural numbers.

This line of thought is not very straightforward, and required quite some work. However, we arrived at a reasonable definition for A_n that works. The key difficulty is to ensure that our A_n's can be encoded, uniformly, as a set of real numbers. Otherwise we gained nothing.

This is where the linear order comes in handy.

Definition

We say that a function $f\colon A \to \omega$ is *based* if it is weakly decreasing, and $f^{-1}(n)$ admits a smallest element for each $n \in \operatorname{rng} f$. We call $\min f^{-1}(n)$ the base point of n.

Proposition

If f is a based function, then f has a canonical name in HS. *Moreover, there is a uniform way to code f into a real number.*

The reason is simple: If f is based, then knowing its base points and their values is enough in order to know f. This information is finite, and therefore can be uniformly coded by finitely many reals in A.

In other words, given a “pre-based function”, i.e. $F\colon X \to \omega$, we can define a name $\dot{f}_F$ for a based function which would be its copy in the full generic extension (where A and X are isomorphic).

Moreover, by its essentially finiteness, we can show that every name for a based function must be eventually equal to $\dot{f}_F$ for some “pre-based function”.

Explicitly defining $\dot{f}_F$, where F is pre-based, is helpful,

$$\dot{f}_F = \{\langle \dot{a}_x, \check{n}\rangle^\bullet \mid F(x) = n\}^\bullet.$$

It is now easy to see that $\dot{f}_F \in$ HS, and that $\pi\dot{f}_F = \dot{f}_{F\circ\pi}$. Note that $F \circ \pi$ is also pre-based, since π is an order automorphism.

We note define $\dot{A}_n = \{\dot{f}_F \mid F\colon X \to n \text{ is pre-based}\}^\bullet$. It is very easy to verify now that $\pi\dot{A}_n = \dot{A}_n$ for all n. Therefore $\dot{A}_n \in$ HS, and $\langle \dot{A}_n \mid n < \omega\rangle^\bullet \in$ HS as well. Moreover, we have:

- $\dot{A}_m \subseteq \dot{A}_n$ for $m < n$. This is trivial.
- $1 \Vdash^{\mathsf{HS}} |\dot{A}_n \times A_m| = |\dot{A}_{nm}|$. This is less trivial, but goes through a simple argument:
  Suppose that F, G are two pre-based functions into n and m respectively, define $H(x) = F(x) \cdot m + G(x)$, then H is pre-based and goes into $m \cdot n$. This translation is uniform, so it can be copied to the symmetric names. The idea behind Krivine's proof is somehow similar.
- $1 \Vdash^{\mathsf{HS}} |\dot{A}_m| \nleq^* |\dot{A}_n|$ if $n < m$. This is not trivial at all. But let us try and sketch a proof anyway.

Sketch of Proof that $1 \Vdash^{\mathsf{HS}} |\dot{A}_m| \nleq^* |\dot{A}_n|$ when $n < m$.

Suppose that $p \Vdash^{\mathsf{HS}} \dot{F} \colon \dot{A}_n \to \dot{A}_m$. There is some countable E which supports $\dot{F}$, i.e. $\pi \in \operatorname{fix}(E)$ satisfy $\pi\dot{F} = \dot{F}$, and we may assume that $\pi p = p$ too.

Note that only countably many based functions can even have base points in E. In particular, there is a function $\dot{f}_m$ which admits m base points, and none of them lie in E. Assume now towards contradiction that p forced that $\dot{F}$ is surjective. This means that there is some $q \leqslant p$ and some $\dot{f}_n$ which is in $\dot{A}_n$ such that $q \Vdash^{\mathsf{HS}} \dot{F}(\dot{f}_n) = \dot{f}_m$.

But $n < m$, so there is at least one base point of f_m which is not a base point of f_n. Say $\dot{a}_x$. We can find an automorphism of X, $\pi \in \operatorname{fix}(E)$, which moves x, but does not move any of the base points of f_n or other base points of f_m. This is because every bounded interval of X is isomorphic to $\mathbb{Q}$.

Moreover, q is finite, so we can do this in a way that ensures that πq is compatible with q. Again, this is due to the very nice properties of $\mathbb{Q}$.

Sketch of Proof continued…

So we have that:

1. $\pi \in \mathrm{fix}(E)$.
2. πq is compatible with q.
3. $\pi \dot{f}_n = \dot{f}_n$.
4. $\pi \dot{f}_m \neq \dot{f}_m$.

But $q \cup \pi q$ forces that $\pi \dot{f}_m = \pi \dot{F}(\pi \dot{f}_n) = \dot{F}(\dot{f}_n) = \dot{f}_m$. And this is a contradiction, so p cannot force that $\dot{F}$ is surjective. And the proof is complete

Suppose now that GCH holds in the ground model, then for every regular κ, there is a universal linear order η_κ of size κ which has nice model theoretic properties like $\mathbb{Q}$. Taking $X = \kappa^+ \times \eta_\kappa$ and generating $\mathscr{F}$ using $\{\mathrm{fix}(E) \mid E \in [X]^{\leqslant\kappa}\}$ we immediately get DC_κ to hold.

But what about $\beth 2$ being a Boolean algebra? Certainly this is not the case that A_2 is a Boolean algebra.

Indeed, we do not know how to reconcile this with Krivine's construction. We do note that the interval algebra of A (with its version of $\prec$) might serve as a suitable candidate. This would require a deeper and better understanding of the $\beth$ function.

To make matter worse, in Krivine's third model, there is a set of real numbers with a linear order $\prec$ satisfying similar properties to A in this model, except that $|A \times A| = |A|$ and $|\mathbb{R}| \leqslant^* |\omega_1 \times A|$. In that model $\beth 2$ is a Boolean algebra with 4 elements. So the $\beth$ function remains mysterious at this time.

It might be interesting to note that using AC_A in the symmetric extension we can in fact prove that $|\mathbb{R}| \leqslant^* |\omega_1 \times A|$. But we can also prove that A is in fact A_2 in our sequence of sets. So $|A_2 \times A_2| = |A_4|$ while $|A_2| <^* |A_4|$.

On the other hand, we get a model where we embed not only the countable atomless Boolean algebra, but $\mathcal{P}(\omega)$ itself. Moreover, we do this without collapsing cardinals. So you win some, and you lose some.

Where do we go now?

1. We need to better understand the $\gimel$ function and how it interacts with the symmetric constructions.
2. We need to better understand the properties of the new reals in Krivine's models. Are they all Cohen over the ground model, for example?
3. We need to better understand the structure of realizability models:
    1. Do they satisfy the Boolean Prime Ideal theorem?
    2. What about other weak versions of AC?
    3. Are there other significant set theoretic axioms that always hold or fail in realizability models, e.g. $V = L(x)$ or SVC which states that AC can be forced (with a set-forcing)?
    4. Is there a way to make these fail?
4. What about results such as Solovay's model, or other type of "classical consistency results"? Can these be obtained via realizability methods?

Thank you for your attention!

(and your corrections.)