A Realizability Model for CZF validating the Negation of the Power Set Axiom

Thomas Streicher
TU Darmstadt (Germany)

Motivation

Observation
Usual *realizability models* for *Type* or *Set Theory* are *impredicative*!

Question
Can one - without restricting the meta-theory - construct realizability models for CZF that are not fully impredicative, i.e. validate e.g. $\neg$Pow or *all sets are subcountable*,?

Answer
Yes, by a modification of the *Aczel construction* !
However, the model still validates *full separation*, i.e. a theory with the same strength as Second Order Arithmetic.

CZF (Aczel, Myhill)

formulated in the language of FOL with equality and a binary base predicate $\in$. The axioms of CZF are Extensionality, Pairing, Union, Infinity, $\in$-Induction, *Bounded** Separation and

Collection (strong)
$\Big((\forall x{\in}a)(\exists y)\,\varphi\Big) \Rightarrow (\exists b)\ \mathbb{M}(x{:}a, y{:}b)\,\varphi$

Subset Collection (needed for existence of function spaces b^a)
$\forall a, b\ \exists c\ \forall \vec{u}\ \Big((\forall x{\in}a)(\exists y{\in}b)\varphi(x, y, \vec{u})\Big) \Rightarrow (\exists d{\in}c)\ \mathbb{M}(x{:}a, y{:}d)\,\varphi(x, y, \vec{u})$

where $\mathbb{M}(x{:}a, y{:}b)\,\varphi(x, y, \dots)$ stands for

$$(\forall x{\in}a)(\exists y{\in}b)\varphi(x, y, \dots) \wedge (\forall y{\in}b)(\exists x{\in}a)\varphi(x, y, \dots)$$

*A formula is *bounded* iff all its quantifications are of the form $(\forall x{\in}a)$ or $(\exists x{\in}a)$.

Review of the Aczel Construction

In MLTT with W-types and one universe U (without W-types) one can form the type $V = (W A{:}U)A$ of well-founded trees which are U-branching in the sense that the sons of a node are indexed by a type in U (or, alternatively, V is the initial solution of the type equation $V \cong (\Sigma A{:}U)V^A$). The elements of V are generated by the rule

$$\frac{A \in U \qquad f : A \to V}{\mathrm{sup}(A, f) \in V}$$

NB The notation $\mathrm{sup}(A, f)$ is merely historical! Better think of $\mathrm{sup}(A, f)$ as $\{f(a) \mid a \in A\}$. Thus V is generated by transfinitely iterating the functor $\mathcal{E}_U(X) = (\Sigma A{:}U)X^A$ instead of the (covariant) powerset functor $\mathcal{P}$ (à la H. Friedman '73 and Ch. McCarty '80).

Review of the Aczel Construction (ctd.)

Exploiting the inductive nature of V one can define binary predicates $=_V, \in_V : V \times V \to Prop$ by *transfinite recursion* on V

- $\mathsf{sup}(A, f) =_V \mathsf{sup}(B, g) \equiv$
  $\Big((\forall i{:}A)(\exists j{:}B)\ f(i) =_V g(j)\Big) \wedge \Big((\forall j{:}B)(\exists i{:}A)\ f(i) =_V g(j)\Big)$

- $b \in_V \mathsf{sup}(A, f) \equiv (\exists i{:}A)\ b =_V f(i)$.

These relations take values in $Prop$ as $Prop$ is assumed to be closed under universal and existential quantification over sets in U.

NB Only the definition of $=_V$ requires transfinite recursion. The relation $\in_V$ is defined *explicitly* in terms of $=_V$.

What is Prop ?

Aczel's choice for Prop is U which – by assumption – is closed under products and disjoint sums of families indexed by elements of U.

As MLTT validates

AC $\quad (\Pi x{:}A)(\Sigma y{:}B)C(x,y) \to (\Sigma f{:}B^A)(\Pi x{:}A)C(x,f(x))$

he could show that

Theorem (Aczel)
The structure $(V, =_V, \in_V)$ validates all axioms of CZF when interpreting logic via propositions as types in U.

Warning In general $(Qx{:}V)\varphi(x) \notin \mathit{Prop}$ for $\varphi : V \to \mathit{Prop}$ and $Q \in \{\forall, \exists\}$ simply because U is not closed under products and sums of families indexed by V (as $V \notin U$).

Our Plan

As models for our type theory we take $\mathbf{Asm}(\mathcal{A})$ for arbitrary pca's $\mathcal{A}$.

We interpret $Prop$ as $\nabla(\mathcal{P}(\mathcal{A}))$, a *proof-irrelevant* universe of propositions (impredicative).

We will consider 2 interpretations of U:

(1) for $U = \nabla(\mathbf{Mod}(\mathcal{A}))$ we have $V \models \mathsf{CZF} + \neg\mathsf{Pow}$

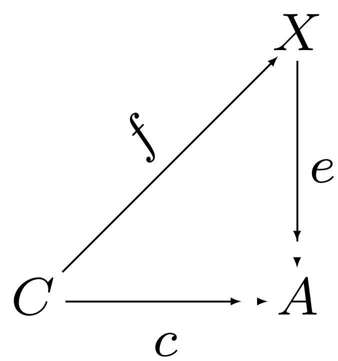
(2) for $U = \nabla(\mathbf{Asm}_\kappa(\mathcal{A}))$ we have $V \models \mathsf{IZF}$

where κ is some strongly inaccessible cardinal.

Problem For neither choice of U we get AC simply because $Prop$ is proof-irrelevant.

Projective Cover Axiom

In $\mathbf{Asm}(\mathcal{A})$ every object A has a projectice cover, i.e. there exists a regular epi $c : C \twoheadrightarrow A$ such that for every regular epi $e : X \twoheadrightarrow A$



for some $f : C \to X$.

This holds even *internally* giving rise to the following

Projective Cover Axiom (PCA)

$$(\forall A{:}U)(\exists C{:}U)(\exists c{:}A^U)\ \ c \text{ surj.} \wedge$$
$$(\forall X{:}U_1)(\forall e{:}A^X)\ e \text{ surj.} \Rightarrow (\exists f{:}X^C)\ e{\circ}f{=}c$$

where U_1 is some universe containing U as an element.

Projective Cover Axiom (ctd.)

If U is $\nabla(\mathbf{Mod}(\mathcal{A}))$ or $\nabla(\mathbf{Asm}_\kappa(\mathcal{A}))$ for some strongly inaccessible cardinal κ then put $U_1 = \nabla(\mathbf{Asm}_{\kappa'}(\mathcal{A}))$ where κ' is a strongly inaccessible cardinal such that $\mathbf{Mod}(\mathcal{A}) \in V_{\kappa'}$ or $\mathbf{Asm}_\kappa(\mathcal{A}) \in V_{\kappa'}$.

Then PCA is realized "essentially by identity" :

Given A in $\mathbf{Asm}_\kappa(\mathcal{A})$ choose C as the partitioned assembly with $|C| = \{(x,a) \mid x \in |A| \text{ and } a \Vdash_A x\}$ and $b \Vdash_C (x,a)$ iff $b = a$. Choose $c : C \twoheadrightarrow A$ as the map with $c(x,a) = a$ (realized by identity). Suppose $e : X \to A$ and there is a realizer for "e surjective". Then there is a $b \in \mathcal{A}$ such that whenever $a \Vdash_A x$ there exists a $z \in e^{-1}(x)$ with $b{\cdot}a \Vdash_X z$. Thus, there is a map $f : C \to X$ with $e \circ f = c$ and $b \Vdash f$.

ECC + PCA proves $V \models \mathsf{CZF}$

The Extended Calculus of Constructions (ECC) proves that $V_U = (WA{:}U)A$ validates all axioms of CZF but Collection and Subset Collection. Moreover, we have

Theorem In ECC + PCA one can prove that V_U validates Collection and Subset Collection.

Using the LEGO Proof Assistent it can be formally checked that

(1) ECC $\vdash V_U \models$ IZ (where IZ is Intuitionistic Zermelo Set Theory)

(2) ECC + PCA $\vdash V_U \models$ IZF

(3) $\mathsf{MLU_2W} \vdash V_U \models$ CZF (avoid using $Prop \in U$ giving powersets!)

ECC + PCA proves $V \models \mathsf{CZF}$ (ctd.)

Proof :

For Collection suppose $a = \sup(A, f)$ and $(\forall x{\in}a)(\exists y)\varphi(x, y)$.
Then $(\forall i{:}A)(\exists y)\varphi(f(i), y)$. Let $c : C \twoheadrightarrow A$ be a projective cover as guaranteed by PCA. As we have $(\forall j{:}C)(\exists y)\varphi(f(c(j)), y)$ it follows by PCA that there is a map $g : C \to V_U$ with $(\forall j{:}C)\varphi(f(c(j)), g(j))$.
Thus, for $b = \sup(C, g)$ we have $(\forall x{\in}a)(\exists y{\in}b)\varphi(x, y)$ as desired.

For Subset Collection suppose $a = \sup(A, f)$ and $b = \sup(B, g)$.
Let $c : C \twoheadrightarrow A$ be a projective cover as guaranteed by PCA.
Put $c = \sup(B^C, \lambda h{:}B^C.\, \sup(C, g \circ h))$.
Suppose $(\forall x{\in}a)(\exists y{\in}b)\varphi(x, y, \vec{u})$. Then $(\forall j{:}C)(\exists y{\in}b)\varphi(c(j), y, \vec{u})$ and, thus, also $(\forall j{:}C)(\exists i{:}B)\varphi(c(j), g(i), \vec{u})$ from which it follows by PCA that there exists $h : C \to B$ with $(\forall j{:}C)\varphi(c(j), g(h(j)), \vec{u})$. Then for $d = \sup(C, g \circ h)$ we have $d \in c$ and $\mathbb{M}(x{:}a, y{:}d)\, \varphi(x, y, \vec{u})$ as desired. $\square$

Refuting the Powerset Axiom

Theorem For $\mathcal{A} = \mathcal{K}_1$, the first Kleene algebra (number realizability), and $U = \nabla(\mathbf{Mod}(\mathcal{K}_1))$ we have $V_U \models \mathsf{CZF} + \neg\mathsf{Pow}$.
Moreover V_U validates that every set is subcountable, i.e. can be enumerated by a subset of ω.
Alas, the full separation scheme is validated by V_U as well.

Proof :
All A in $\mathbf{Mod}(\mathcal{K}_1)$ have only countably many elements. Thus, any set of the form sup(A, f) can be enumerated by the ($\neg\neg$-stable) subset $I_A = \{n \in \omega \mid \exists x \in |A|.\ n \vdash_A x\}$ of ω. However, the powerset $\mathcal{P}(\omega)$ does not exist in V_U as there are uncountably many subsets of ω.
Alas, V_U validates the full separation scheme Sep because modest sets are closed under *arbitrary* subobjects. $\Box$

Refuting the Powerset Axiom (ctd.)

Addendum The above Theorem extends to all pca's $\mathcal{A}$ with $|\mathcal{A}| < \beth_\omega$, i.e. for *practically all* pca's!
If $\mathcal{A}$ has cardinality $< \beth_n$ then $\mathcal{P}^n(\omega)$ does not exist in V_U.

Remarkably $V_{\mathbf{Mod}(\mathcal{A})}$ validates $\neg\mathsf{Pow}$ although $\mathbf{Asm}(\mathcal{A})$ is a model of *impredicative* type theory hosting even a model of IZF, namely $V_{\mathbf{Asm}_\kappa(\mathcal{A})}$ for some strongly inaccessible cardinal κ.

The strength of CZF $+$ Sep is that of Second Order Arithmetic (according to M. Rathjen).

Can we get rid of Full Separation?

As full separation is certainly impredicative we would like to get rid of it. For this purpose one would have to

(1) identify a universe U in $\mathbf{Asm}(\mathcal{A})$ not closed under subobjects

or

(2) construct a non-impredicative model of type theory with W-types that hosts a universe U.

(1) is hopeless if U is required to be closed under finite sums.

(2) is also a problem for the following reasons.

Can we get rid of Full Separation? (ctd.)

Lietz and TS have shown that for a typed pca $\mathcal{T}$ (e.g. some (standard) model of Gödel's T)

(1) $\mathbf{Asm}(\mathcal{T})$ is a model of predicative Martin-Löf Type Theory

(2) $\mathbf{Asm}(\mathcal{T})$ is *genuinely predicative*, i.e. does not admit a generic mono, if and only if $\mathcal{T}$ is *genuinly typed*, i.e. does not have a universal type of which all other types can be obtained as retracts.

Although there are plenty of genuinely impredicative models $\mathbf{Asm}(\mathcal{T})$ none of them is known to host a(n appropriate) universe.
The natural candidate would be families of modest sets which satisfy all desired closure properties but admit a generic family if and only if $\mathcal{T}$ admits a universal type, i.e. $\mathbf{Asm}(\mathcal{T})$ is impredicative.

Predicative Models of a Weaker Theory

If one drops the Infinity axiom from CZF and replaces it by the weaker requirement that in the full subcategory of (small) sets there exists an initial orbit N (n.n.o. in small sets) then there exist plenty of genuinely predicative models for this weaker set theory called PAST.

S. Awodey & al. have shown that for every locally cartesian closed pretopos $\mathcal{E}$ with n.n.o. N (model of MLTT without universes) the category $\mathsf{Idl}(\mathcal{E})$ gives rise to a model of PAST when defining "small" as "representable" and taking $\mathsf{Yon}(N)$ for n.n.o. in sets. The category $\mathsf{Idl}(\mathcal{E})$ is defined as the full subcategory of $\widehat{\mathcal{E}} = \mathbf{Set}^{\mathcal{E}^{\mathrm{op}}}$ on objects which appear as *directed colimits of mono's of representables*. Thus, the full subcategory of (small) sets of $\mathsf{Idl}(\mathcal{E})$ is equivalent to $\mathcal{E}$ itself.

Istantiating $\mathcal{E}$ by $\mathbf{Asm}(\mathcal{T})$ for some genuinely typed pca $\mathcal{T}$ gives rise to genuinely predicative models of PAST (with same strength as HA).

Comparison with Algebraic Set Theory

In Joyal and Moerdijk's *Algebraic Set Theory* (CUP 1995) they have constructed models of IZF in models for intuitionistic FOL with quotient types (so called *Heyting pretoposes*) endowed with a class $\mathcal{S}$ of *small maps* which are close to universes in the type-theoretic sense. The only difference is that they do not postulate a generic family for $\mathcal{S}$ but only a *weakly generic* one, i.e. a family $El : E \to U$ in $\mathcal{S}$ such that for every $a : A \to I$ in $\mathcal{S}$ there exists a regular epi $e : J \twoheadrightarrow I$ such that $e^*a \cong f^*El$ for some $f : J \to U$.

In more "logical" terms "weakly generic" means that $A \to I$ is in $\mathcal{S}$ iff $(\forall i{:}I)(\exists a{:}U)\ A_i \cong El(a)$.

Joyal and Moerdijk construct "initial ZF-algebras" like Aczel taking $V = (W A{:}U)El(A)$ (and then taking the quotient by extensional equality $=_V$ although there is no need for it!).

Comparison with AST (ctd.)

J.&M. show that every realizability topos and every Grothendieck topos hosts a class $\mathcal{S}$ of small maps giving rise to an initial ZF-algebra providing a model for IZF.

For realizability toposes RT($\mathcal{A}$) the W-type $V = (W\,A{:}U)El(A)$ stays within $\mathbf{Asm}(\mathcal{A})$ and only the quotient $V_{/=_V}$ leads out of it. At least when choosing $U = \mathbf{Asm}_\kappa(\mathcal{A})$ as we do. Their choice of U is more complicated because ignoring $\mathbf{Asm}(\mathcal{A})$ they prefer to work in the wider category RT($\mathcal{A}$) (obtained from $\mathbf{Asm}(\mathcal{A})$ by adding quotients). However, there is no need for this unless one insists on taking quotients!

For Grothendieck toposes one can construct universes $\mathcal{S}$ which even admit a generic family (see TS *Universes in Toposes* (2004) based on joint work with M. Hofmann) but do not validate the Projective Cover Axiom.

Comparison with AST (ctd.)

Instead the universes constructed in Grothendieck toposes validate the following

Type-Theoretic Collection Axiom (J.&M.'95)
$(\forall A{:}U)(\forall X{:}U_1)(\forall e{:}A^X)$ e surj. $\Rightarrow (\exists C{:}U)(\exists f{:}X^C)\ e \circ f$ surj.

meaning that for small A covered by $e : X \twoheadrightarrow A$ with X possibly big there exists $f : C \to X$ such that C is small and $e \circ f$ is still a cover, i.e. *every cover of a small type admits a small subcover*.

I have checked in LEGO that

$$\text{ECC} + \text{TTCA} \vdash V_U \models \text{IZF}$$

thus providing a purely type-theoretic account of J.&M.'s Algebraic Set Theory.

Comparison with AST (ctd.)

Proof idea for ECC + TTCA $\vdash V \models$ Coll

Suppose $a = \text{sup}(A, f)$ and $(\forall x{\in}a)(\exists y)\varphi(x, y)$.
Then $X := (\Sigma i{:}A)(\Sigma y{:}V)\varphi(f(i), y) \in U_1$ and $\pi_1 : X \twoheadrightarrow A$. From TTCA it follows that there exists $h : C \twoheadrightarrow X$ with $C \in U$ and $\pi_1 \circ h$ surjective. Then for $c = (C, \pi_1{\circ}\pi_2{\circ}f)$ one easily shows that $(\forall x{\in}a)(\exists y{\in}c)\varphi(x, y)$ as desired.

Inspecting the proof we actually see that

$$\text{MLU}_2\text{W} + \text{TTCA} \vdash V \models \text{Coll}$$

Predicative AST

If one tries to verify that $\mathsf{MLU_2W} + \mathsf{TTCA} \vdash V \models \mathsf{CZF}$ one runs into problems with showing that $\mathsf{MLU_2W} + \mathsf{TTCA} \vdash V \models \mathsf{SubColl}$.

Thus, one has to introduce the following *family version* of TTCA

$\mathsf{TTCA_{fam}}$ (implied by Moerdijk and Palmgren's AMC)

$$(\forall A{:}U)(\exists I{:}U)(\exists C{:}U^I)$$
$$(\forall X{:}U_1)(\forall e{:}A^X)\ e \text{ surj.} \Rightarrow (\exists i{:}I)(\exists f{:}X^{C_i})\ e{\circ}f \text{ surj.}$$

for which we have $\mathsf{MLU_2W} + \mathsf{TTCA_{fam}} \vdash V \models \mathsf{SubColl}$ and thus

$$\mathsf{MLU_2W} + \mathsf{TTCA_{fam}} \vdash V \models \mathsf{CZF}$$

as desired.

Predicative AST (ctd.)

Proof : Suppose $a = \mathsf{sup}(A, f)$ and $b = \mathsf{sup}(B, g)$.

Let $I \in U$ and $C \in U^I$ as guaranteed by $\mathsf{TTCA}_{\mathsf{fam}}$ for A.
Put $c = \mathsf{sup}\Big((\Sigma i{:}I)B^{C_i}, \lambda(i,h).\,\mathsf{sup}(C_i, g{\circ}h)\Big)$.

Suppose $(\forall x{\in}a)(\exists y{\in}b)\varphi(x, y, \vec{u})$.
Then $(\forall j{:}A)(\exists k{:}B)\varphi(f(j), g(k), \vec{u})$.
For $X := (\Sigma j{:}A)(\Sigma k{:}B)\varphi(f(j), g(k), \vec{u})$ we have $\pi_1 : X \twoheadrightarrow A$.
By $\mathsf{TTCA}_{\mathsf{fam}}$ there exist $i \in I$ and $h \in X^{C_i}$ with $\pi_1 \circ h : C_i \twoheadrightarrow A$.
Then $d = \mathsf{sup}(C_i, g{\circ}\pi_1{\circ}\pi_2{\circ}h) \in c$ and $\mathbb{M}(x{:}a, y{:}d)\,\varphi(x, y, \vec{u})$. $\square$

Summary

- *Without restricting the meta-theory* we have constructed a realizability model for CZF + ¬Pow (+Sep).

- Getting rid of full separaration seems to be related to the problem of finding genuinely predicative models of MLTT *with universes* which is a difficult open problem.
  However, for the weaker predicative set theory PAST (same strength as HA) there are plenty of genuinely predicative models.

- Joyal and Moerdijk's Algebraic Set Theory can be understood as as a variant of the Aczel construction. As $Prop$ is proof-irrelevant the lack of Axiom of Choice has to be compensated by adding "non-logical" axioms like PCA or $\mathrm{TTCA}_{(\mathrm{fam})}$ to type theory.