Categoricity Results for Second-Order ZF in Dependent Type Theory

Dominik Kirst and Gert Smolka

Saarland University, Saarbrücken, Germany
{kirst,smolka}@ps.uni-saarland.de

Abstract. We formalise the axiomatic set theory second-order ZF in the constructive type theory of Coq assuming excluded middle. In this setting we prove Zermelo's embedding theorem for models, categoricity in all cardinalities, and the correspondence of inner models and Grothendieck universes. Our results are based on an inductive definition of the cumulative hierarchy eliminating the need for ordinals and transfinite recursion.

1 Introduction

Second-order ZF is different from first-order ZF in that the replacement axiom quantifies over all relations at the class level. This is faithful to Zermelo's [22] informal view of axiomatic set theory and in sharp contrast to the standard first-order axiomatisation of ZF (cf. [8,6]). The difference between the two theories shows in the possibility of artificial and counterintuitive models of first-order ZF that are excluded by the more determined second-order ZF [17].

Zermelo [22] shows in an informal higher-order setting a little noticed embedding theorem saying that given two models of second-order ZF one embeds isomorphically into the other. From Zermelo's paper it is clear that different models of second-order ZF differ only in the height of their cumulative hierarchy and that higher models admit more Grothendieck universes [20] (i.e., sets closed under all set constructions).

The present paper studies second-order ZF in the constructive type theory of Coq [16] assuming excluded middle. We sharpen Zermelo's result by showing that second-order ZF is categorical in every cardinality, which means that equipotent models are always isomorphic. Using the fact that the height of a model is determined by its universes, we show that second-order ZF extended with an axiom fixing the number of universes to a finite n is categorical (i.e., all models are isomorphic).

For our results we employ the cumulative hierarchy, which is a well-ordered hierarchy of sets called stages such that every set appears in a stage and every universe appears as a stage. The usual way the cumulative hierarchy is established is through the ordinal hierarchy and transfinite recursion. We replace this long-winded first-order approach with a direct definition of the cumulative hierarchy as an inductive predicate, which leads to an elegant and compact development. While an inductive definition of the cumulative hierarchy has not been proposed before, inductive definitions of this form are known as tower constructions [14,12]. Tower constructions go back to Zermelo [21] and Bourbaki [4], and are used by Smullyan and Fitting [14] to obtain the ordinal hierarchy.

The development of this paper is formalised and verified with the Coq proof assistant. Coq proves as an ideal tool for our research since types and thus models are first-class, inductive predicates and inductive proofs are well supported, and unnecessary assumptions (e.g. choice functions) are not built in. We assume excluded middle throughout the development and do not miss further built-in support for classical reasoning. The Coq development accompanying this paper has less than 1500 lines of code (about 500 for specifications and 1000 for proofs) and can be found at `https://www.ps.uni-saarland.de/extras/itp17-sets`. The theorems and definitions of the PDF version of this paper are hyperlinked with the Coq development.

The paper is organised as follows. We first discuss our formalisation of ZF and pay attention to the notion of inner models. Then, we study the cumulative hierarchy and prove that Grothendieck universes appear as stages. Next we prove the embedding theorem and show that ZF is categorical in every cardinality. Then we discuss categorical extensions of ZF. We end with remarks comparing our type-theoretic approach to ZF with the standard first-order approach.

2 Axiom System and Inner Models

We work in the type theory of Coq augmented by excluded middle for classical reasoning. Our model-theoretical approach is to study types that provide interpretations for the relations and constructors of set theory as follows:

Definition 1. *A* ***set structure*** *is a type M together with constants*

$$\_ \in \_ : M \to M \to \mathsf{Prop} \qquad \bigcup : M \to M$$
$$\emptyset : M \qquad \mathcal{P} : M \to M$$
$$\_ @ \_ : (M \to M \to \mathsf{Prop}) \to M \to M$$

for membership, empty set, union, power, and replacement.

Most of the following definitions rely on some fixed set structure M. We call the members $x, y, z, a, b, c : M$ **sets** and the members $p, q : M \to \mathsf{Prop}$ **classes**. Further, we use set-theoretical notation where convenient, for instance we write $x \in p$ if px and $x \subseteq p$ if $y \in p$ for all $y \in x$. We say that p and x **agree** if $p \subseteq x$ and $x \subseteq p$ and we call p **small** if there is some agreeing x. We take the freedom to identify a set x with the agreeing class $(\lambda y.\, y \in x)$.

ZF-like set theories assert every set to be free of infinitely descending $\in$-chains, in particular to be free of any $\in$-loops. This can be guaranteed by demanding all sets to contain a $\in$-least element, the so-called regularity axiom. From this assertion one can deduce the absence of infinitely descending $\in$-chains and hence an induction principle that implies $x \in p$ for all x if one can show that $y \in p$ whenever $y \subseteq p$. Given a type theory that provides inductive predicates, $\in$-induction can be obtained with an inductive predicate defining well-ordered sets.

Definition 2. *We define the class of* ***well-founded sets*** *inductively by:*

$$\frac{x \subseteq WF}{x \in WF}$$

Then the induction principle of WF is exactly $\in$-induction and the wished axiom can be formulated as $x \in WF$ for all x. This and the other usual axioms of ZF yield the notion of a model:

Definition 3. *A set structure M is a* ***model (of ZF)*** *if*

$$\begin{aligned}
\mathsf{Ext} &: \forall x, y.\, x \subseteq y \to y \subseteq x \to x = y \\
\mathsf{Eset} &: \forall x.\, x \notin \emptyset \\
\mathsf{Union} &: \forall x, z.\, z \in \bigcup x \leftrightarrow \exists y.\, z \in y \wedge y \in x \\
\mathsf{Power} &: \forall x, y.\, y \in \mathcal{P}x \leftrightarrow y \subseteq x \\
\mathsf{Rep} &: \forall R \in \mathcal{F}(M).\, \forall x, z.\, z \in R@x \leftrightarrow \exists y \in x.\, Ryz \\
\mathsf{WF} &: \forall x.\, x \in WF
\end{aligned}$$

where $R \in \mathcal{F}(M)$ denotes that $R : M \to M \to \mathsf{Prop}$ is a functional relation. We denote the predicate on structures expressing this collection of axioms by **ZF** *and write $M \models \mathbf{ZF}$ for* **ZF** *M.*

Apart from the inductive formulation of the foundation axiom, there are further ways in which our axiomatisation **ZF** differs from standard textbook presentations. Most importantly, we employ the second-order version of relational replacement which is strictly more expressive than any first-order scheme and results in a more determined model theory. Moreover, we do not assume the axiom of infinity because guaranteeing infinite sets is an unnecessary restriction for our investigation of models. Finally, we reconstruct the redundant notions of pairing, separation, and description instead of assuming them axiomaticly in order to study some introductory example constructions. The following definition of unordered pairs can be found in [15]:

Definition 4. *We define the* ***unordered pair*** *of x and y by:*

$$\{x, y\} := (\lambda ab.\, (a = \emptyset \wedge b = x) \vee (a = \mathcal{P}\emptyset \wedge b = y))@\mathcal{P}(\mathcal{P}\emptyset)$$

As usual we abbreviate $\{x, x\}$ by $\{x\}$ and call such sets ***singletons****.*

Lemma 5. *$z \in \{x, y\}$ if and only if $z = x$ or $z = y$.*

Proof. The given defining relation is obviously functional. So by applying Rep we know that $z \in \{x, y\}$ if and only if there is $z' \in \mathcal{P}(\mathcal{P}\emptyset)$ such that $z' = \emptyset$ and $z = x$ or $z' = \mathcal{P}\emptyset$ and $z = y$. This is equivalent to the statement $z = x$ or $z = y$ since we can simply pick z' to be the respective element of $\mathcal{P}(\mathcal{P}\emptyset)$. $\square$

The next notion we recover is separation, allowing for defining subsets of the form $x \cap p = \{\, y \in x \mid y \in p \,\}$ for a set x and a class p. By the strong replacement axiom we can show the separation axiom again in higher-order formulation.

Definition 6. *We define* ***separation*** *by* $x \cap p := (\lambda ab.\, a \in p \land a = b)@x$.

Lemma 7. *$y \in x \cap p$ if and only if $y \in x$ and $y \in p$.*

Proof. The defining relation is again functional by construction. So Rep states that $y \in x \cap p$ if and only if there is $z \in x$ such that $z \in p$ and $z = y$. This is equivalent to $y \in x$ and $y \in p$. □

Finally, relational replacement implies the description principle in the form that we can construct a function that yields the witness of uniquely inhabited classes. The construction we employ can be found in [9]:

Definition 8. *We define a* ***description operator*** *by* $\delta p := \bigcup\,((\lambda ab.\, b \in p)@\{\emptyset\})$.

Lemma 9. *If p is uniquely inhabited, then $\delta p \in p$.*

Proof. Let x be the unique inhabitant of p. By uniqueness we know that the relation $(\lambda ab.\, b \in p)$ is functional, so Rep implies that $(\lambda ab.\, b \in p)@\{\emptyset\} = \{x\}$ and Union implies that $\delta p = \bigcup\{x\} = x \in p$. □

We note that functional replacement, i.e. the existence of a set $f@x$ for a function $f : M \to M$ and a set x is logically weaker than the relational replacement we work with. First, it is clear that such functions can be turned into functional relations by $(\lambda xy.\, fx = y)$. So relational replacement implies functional replacement and we will in fact use the latter where possible. Conversely, functional relations can only be turned into actual functions in the presence of a description operator. Hence description, which can be seen as a weak form of choice, must be assumed separately when opting for functional replacement.

At this point we can start discussing the model-theory of **ZF**. A first result is in direct contrast to the existence of countable models of first-order ZF guaranteed by the Löwenheim-Skolem Theorem. To this end, we employ the inductive data type $\mathbb{N}$ of natural numbers n for a compact formulation of the infinity axiom: we assume an injection $\overline{n}$ that maps numbers to sets together with a set ω that exactly contains the sets $\overline{n}$.

Lemma 10. *If M is a model of* **ZF** *with infinity, then M is uncountable.*

Proof. Suppose $f : \mathbb{N} \to M$ were a surjection from the inductive data type of natural numbers onto M. Then consider the set $X := \{\, \overline{n} \in \omega \mid \overline{n} \notin fn \,\}$. Since f is assumed surjective, there is $m : \mathbb{N}$ with $fm = X$. But this implies the contradiction $\overline{m} \in X \leftrightarrow \overline{m} \notin fm = X$. □

When studying the cumulative hierarchy in the next section we will frequently encounter classes or, more specifically, sets that are closed under the set constructors. Such classes resemble actual models of **ZF** and we use the remainder of this section to make this correspondence formal.

Definition 11. *A class $p : M \to \mathsf{Prop}$ is called* ***inner model*** *if the substructure of M consisting of the subtype induced by p and the correspondingly restricted set constructors is a model in the sense of Definition 3. We then write $p \models$* **ZF**.

Definition 12. *A class p is **transitive** whenever $x \in y \in p$ implies $x \in p$ and **swelled** (following the wording in [14]) whenever $x \subseteq y \in p$ implies $x \in p$. Transitive and swelled sets are defined analogously.*

Definition 13. *A transitive class p with $\emptyset \in p$ is **ZF-closed** if for all $x \in p$:*
*(1) $\bigcup x \in p$ (**closure under union**),*
*(2) $\mathcal{P}x \in p$ (**closure under power**),*
*(3) $R@x \in p$ if $R \in \mathcal{F}(M)$ and $R@x \subseteq p$ (**closure under replacement**).*
*If p is small, then we call the agreeing set a **(Grothendieck) universe**.*

Lemma 14. *If p is ZF-closed, then $p \models$ **ZF**.*

Proof. Most axioms follow mechanically from the closure properties and transitivity. To establish WF we show that the well-foundedness of sets $x \in p$ passes on to the corresponding sets in the subtype by $\in$-induction. ☐

3 Cumulative Hierarchy

It is a main concern of ZF-like set theories that the domain of sets can be stratified by a class of $\subseteq$-well-ordered stages. The resulting hierarchy yields a complexity measure for every set via the first stage including it, the so-called rank. One objective of our work is to illustrate that studying the cumulative hierarchy becomes very accessible in a dependent type theory with inductive predicates.

Definition 15. *We define the inductive class $\mathcal{S}$ of **stages** by the following rules:*

$$\frac{x \in \mathcal{S}}{\mathcal{P}x \in \mathcal{S}} \qquad\qquad \frac{x \subseteq \mathcal{S}}{\bigcup x \in \mathcal{S}}$$

Fact 16. *The following hold:*
(1) $\emptyset$ is a stage.
(2) All stages are transitive.
(3) All stages are swelled.

Proof. We prove the respective statements in order.
(1) is by the second definitional rule as $\emptyset \subseteq \mathcal{S}$.
(2) is by stage induction using that power and union preserve transitivity.
(3) is again by stage induction. ☐

The next fact expresses that union and separation maintain the complexity of a set while power and pairing constitute an actual rise.

Fact 17. *Let x be a stage, p a class and $a, b \in x$ then:*
(1) $\bigcup a \in x$
(2) $\mathcal{P}a \in \mathcal{P}x$
(3) $\{a, b\} \in \mathcal{P}x$
(4) $a \cap p \in x$

Proof. Again we show all statements independently.
(1) is by stage induction with transitivity used in the first case.
(2) is also by stage induction.
(3) is direct from Lemma 5.
(4) follows since x is swelled and $a \cap p \subseteq a$. □

We now show that the class $\mathcal{S}$ is well-ordered by $\subseteq$. Since $\subseteq$ is a partial order we just have to prove linearity and the existence of least elements, which bot An economical proof of linearity employs the following **double-induction principle** [14]:

Fact 18. *For a binary relation R on stages it holds that Rxy for all $x, y \in \mathcal{S}$ if*
(1) $R(\mathcal{P}x)y$ whenever Rxy and Ryx and
(2) $R(\bigcup x)y$ whenever Rzy for all $z \in x$.

Proof. By nested stage induction. □

Lemma 19. *If $x, y \in \mathcal{S}$, then either $x \subseteq y$ or $\mathcal{P}y \subseteq x$.*

Proof. By double-induction we just have to establish (1) and (2) for R instantiated by the statement that either $x \subseteq y$ or $\mathcal{P}y \subseteq x$. Then 1 is directly by case analysis on the assumptions Rxy and Ryx and using that $x \subseteq \mathcal{P}x$ for stages x. The second follows from a case distinction whether or not y is an upper bound for x in the sense that $z \subseteq y$ for all $z \in x$. If so, we know $(\bigcup x) \subseteq y$. If not, there is some $z \in x$ with $z \nsubseteq y$. So by the assumption Rzy only $\mathcal{P}y \subseteq z$ can be the case which implies $\mathcal{P}y \subseteq \bigcup x$. □

Fact 20. *The following alternative formulations of the linearity of stages hold:*
(1) $\subseteq$-linearity: $x \subseteq y$ or $y \subseteq x$
(2) $\in$-linearity: $x \subseteq y$ or $y \in x$
(3) trichotomy: $x \in y$ or $x = y$ or $y \in x$

Proof. (1) and (2) are by case distinction on Lemma 19. Then (3) is by (2). □

Lemma 21. *If p is an inhabited class of stages, then there exists a least stage in p. This means that there is $x \in p$ such that $x \subseteq y$ for all $y \in p$.*

Proof. Let $x \in p$. By $\in$-induction we can assume that every $y \in x$ with $y \in p$ admits a least stage in p. So if there is such a y there is nothing left to show. Conversely, suppose there is no $y \in x$ with $y \in p$. In this case we can show that x is already the least stage in p by $\in$-linearity. □

The second standard result about the cumulative hierarchy is that it exhausts the whole domain of sets and hence admits a total rank function.

Definition 22. *We call $a \in \mathcal{S}$ the **rank** of a set x if $x \subseteq a$ but $x \notin a$. Since the rank is unique by trichotomy we can refer to it via a function ρ.*

Lemma 23. *$\rho x = \bigcup \mathcal{P}@(\rho@x)$ for every x. Thus every set has a rank.*

Proof. For a set x we can assume that every $y \in x$ has rank ρy by $\in$-induction. Then consider the stage $z := \bigcup \mathcal{P}@(\rho@x)$. Since for every $y \in x$ we know $y \in \mathcal{P}(\rho y)$, we deduce $x \subseteq z$. Moreover, suppose it were $x \in z$, so $x \in \mathcal{P}(\rho y)$ for some $y \in x$. Then this would imply the contradiction $y \in \rho(y)$, so we know $x \notin z$. Thus z is the rank of x. As a consequence, for every set x we know that $x \in \mathcal{P}(\rho x)$. Hence every set occurs in a stage. ☐

Fact 24. *The hierarchy of stages exhausts all sets.*

Proof. Holds since every set x is an element of the stage $\mathcal{P}(\rho x)$. ☐

We now turn to study classes of stages that are closed under some or all set constructors. The two introductory rules for stages already hint at the usual distinction of successor and limit stages. However, since we do not require x to contain an infinitely increasing chain in the second rule this distinction will not exactly mirror the non-exclusive rule pattern.

Definition 25. *We call $x \in \mathcal{S}$ a* ***limit*** *if $x = \bigcup x$ and a* ***successor*** *if $x = \mathcal{P}y$ for some $y \in \mathcal{S}$. Note that this means $\emptyset$ is a limit.*

Fact 26. *If $x \subseteq \mathcal{S}$, then either $\bigcup x \in x$ or $x \subseteq \bigcup x$.*

Proof. Suppose it were $x \not\subseteq \bigcup x$ so there were $y \in x$ with $y \notin \bigcup x$. Then to establish $\bigcup x \in x$ it suffices to show that $y = \bigcup x$. Since $\bigcup x$ is the unique $\subseteq$-greatest element of x, it is enough to show that y is a $\subseteq$-greatest element, i.e. that $z \subseteq y$ for all $z \in x$. So let $z \in x$, then by linearity of stages it must be either $z \subseteq y$ or $y \in z$. The latter case implies $y \in \bigcup x$ contradicting the assumption. ☐

Lemma 27. *Every stage is either a limit or a successor.*

Proof. Let x be a stage and apply stage induction. In the first case we know that x is a successor. In the second case we know that x is a set of stages that are either successors or limits and want to derive a decision for $\bigcup x$. Now we distinguish the two cases of Fact 26. If $\bigcup x \in x$, the inductive hypothesis yields the decision. If $x \subseteq \bigcup x$, it follows that $\bigcup x$ is a limit. ☐

Lemma 28. *If x is an inhabited limit, then x is transitive, contains $\emptyset$, and is closed under union, power, pairing, and separation.*

Proof. Transitivity and closure under union and separation hold for arbitrary stages by Facts 16 and 17. Further, x must contain $\emptyset$ since it can be constructed from the set witnessing inhabitance by separation. The closure under power follows from the fact that every set $y \in x$ occurs in a stage $a \in x$. Then finally, the closure under pairing follows from Fact 17. ☐

Hence, inhabited limits almost satisfy all conditions that constitute universes, only the closure under replacement is not necessarily given. So in order to study actual inner models one can examine the subclass of inhabited limits closed under replacement. In fact, this subclass turns out to be exactly the universes.

Lemma 29. *If $a \in u$ for a universe u, then $\rho a \in u$.*

Proof. By ϵ-induction we may assume that $\rho b \in u$ for all $b \in a$, so we know $\rho@a \in u$ by the closure of u under replacement. Also, we know $\rho a = \bigcup \mathcal{P}@(\rho@a)$ by Lemma 23. Thus $\rho a \in u$ follows from the closure properties of u. □

Lemma 30. *Universes are exactly inhabited limits closed under replacement.*

Proof. The direction from right to left is simple given that limits are already closed under all set constructors but replacement. Conversely, a universe is closed under replacement by definition and it is also easy to verify $u = \bigcup u$ given that for $x \in u$ we know $x \in \mathcal{P}(\rho x) \in u$ by the last lemma. So we just need to justify that u is a stage. We do this by showing that $u = \bigcup(u \cap S)$. The inclusion $u \supseteq \bigcup(u \cap S)$ is by transitivity. For the converse suppose $x \in u$. Then $x \subseteq \bigcup(u \cap S)$ again by knowing $x \in \mathcal{P}(\rho x) \in u$. □

We remark that inhabited limits are models of the set theory Z which is usually defined to be ZF with pairing and separation instead of replacement. Also note that in our concrete axiomatisation **ZF** without infinity it is undecided whether there exists a universe, whereas assuming the existence of an infinite set allows for constructing the universe of all hereditarily finite sets.

4 Embedding Theorem

In this section we prove Zermelo's embedding theorem for models of second-order ZF given in [22]. Given two models M and N of **ZF**, we define a structure-preserving embedding $\approx$, called $\in$-bisimilarity, and prove it either total, surjective or both. We call this property of $\approx$ **maximality**. By convention, we let x, y, z range over the sets in M and a, b, c range over the sets in N in the remainder of this document.

Definition 31. *We define an inductive predicate $\approx\colon M \to N \to \mathsf{Prop}$ by*

$$\frac{\forall y \in x.\, \exists b \in a.\, y \approx b \quad \forall b \in a.\, \exists y \in x.\, y \approx b}{x \approx a}$$

We call the first condition ***(bounded) totality*** *on x and a and write $x \rhd a$. The second condition is called* ***(bounded) surjectivity*** *on x and a, written $x \lhd a$. We call $\approx$* ***$\in$-bisimilarity*** *and if $x \approx a$ we call x and a* ***bisimilar****.*

The following lemma captures the symmetry present in the definition.

Lemma 32. *$x \approx a$ iff $a \approx x$ and $x \rhd a$ iff $a \lhd x$.*

Proof. We first show that $a \approx x$ whenever $x \approx a$, the converse is symmetric. By $\in$-induction on x we may assume that $b \approx y$ whenever $y \approx b$ for some $y \in x$. Now assuming $x \approx a$ we show $a \rhd x$. So for $b \in a$ we have to find $y \in x$ with $b \approx y$. By $x \lhd a$ we already know there is $y \in x$ with $y \approx b$. Then the inductive hypothesis implies $b \approx y$ as wished. That $x \rhd a$ follows analogously and the second statement is a consequence of the first. □

It turns out that $\approx$ is a partial $\in$-isomorphism between the models:

Lemma 33. *The relation $\approx$ is functional, injective, and respects membership.*

Proof. We show that $\approx$ is functional. By induction on $x \in WF$ we establish $a = a'$ whenever $x \approx a$ and $x \approx a'$. We show the inclusion $a \subseteq a'$, so first suppose $b \in a$. Since $x \lhd a$ there must be $y \in x$ with $y \approx b$. Moreover, since $x \rhd a'$ there must be $b' \in a'$ with $y \approx b'$. By induction we know that $b = b'$ and hence $b \in a'$. The other inclusion is analogous and injectivity is by symmetry.

It remains to show that $\approx$ respects membership. Hence let $x \approx a$ and $x' \approx a'$ and suppose $x \in x'$. Then by $x' \rhd a'$ there is $b \in a'$ with $x \approx b$. Hence $a = b$ by functionality of $\approx$ and thus $a \in a'$. $\square$

Since the other set constructors are uniquely determined by their members, it follows that they are also respected by the $\in$-bisimilarity:

Fact 34. $\emptyset \approx \emptyset$

Proof. Both $\emptyset \rhd \emptyset$ and $\emptyset \lhd \emptyset$ hold vacuously. $\square$

Lemma 35. *If $x \approx a$, then $\bigcup x \approx \bigcup a$*

Proof. By symmetry (Lemma 32) we just have to prove $\bigcup x \rhd \bigcup a$. So suppose $y \in \bigcup x$, so $y \in z \in x$. By $x \rhd a$ we have $c \in a$ with $z \approx c$ and applying $z \rhd c$ we have $b \in c$ with $y \approx b$. So $c \in b \in a$ and thus $b \in \bigcup a$. $\square$

Lemma 36. *If $x \approx a$, then $\mathcal{P}x \approx \mathcal{P}a$*

Proof. Again, we just show $\mathcal{P}x \rhd \mathcal{P}a$. Hence let $y \in \mathcal{P}x$, so $y \subseteq x$. Then we can construct the image of y under $\approx$ by $b := \{\, c \in a \mid \exists z \in y. z \approx c \,\}$. Clearly $b \subseteq a$ so $b \in \mathcal{P}a$ and by $x \approx a$ it is easy to establish $y \approx b$. $\square$

Before we can state the corresponding lemma for replacement we first have to make precise how binary relations in one model are expressed in the other.

Definition 37. *For $R : M \to M \to \mathsf{Prop}$ we define $\overline{R} : N \to N \to \mathsf{Prop}$ by*

$$\overline{R}ab := \exists xy.\, x \approx a \land y \approx b \land Rxy$$

In particular, if $R \in \mathcal{F}(M)$ is functional then it follows that $\overline{R} \in \mathcal{F}(N)$.

Lemma 38. *If $x \approx a$, $R \in \mathcal{F}(M)$, and $R@x \subseteq \mathsf{dom}(\approx)$, then $R@x \approx \overline{R}@a$.*

Proof. We first show that $R@x \rhd \overline{R}@a$, so let $y \in R@x$. Then by $R@x \subseteq \mathsf{dom}(\approx)$ there is b with $y \approx b$. It suffices to show $b \in \overline{R}@a$ which amounts to finding $c \in a$ with $\overline{R}cb$. Now by $y \in R@x$ there is $z \in x$ with Rzy. Hence there is $c \in a$ with $z \approx c$ since $x \rhd a$. This implies $\overline{R}cb$.

We now show $R@x \lhd \overline{R}@a$, so let $b \in \overline{R}@a$. Then there is $c \in a$ with $\overline{R}cb$. By definition this already yields z and y with $z \approx c$, $y \approx b$, and Rzy. Since $\approx$ respects membership we know $z \in x$ and hence $y \in R@x$. $\square$

Note that these properties immediately imply the following:

Lemma 39. *If* $\mathsf{dom}(\approx)$ *is small, then it agrees with a universe.*

Proof. First, $\emptyset \in \mathsf{dom}(\approx)$ since $\emptyset \approx \emptyset$. Further, $\mathsf{dom}(\approx)$ is transitive by the totality part of $x \approx a$ for every $x \in \mathsf{dom}(\approx)$. The necessary closure properties of universes were established in the last lemmas. $\square$

The dual statement for $\mathsf{ran}(\approx)$ holds as well by symmetry. Now given that $\approx$ preserves all structure of the models, every internally specified property holds simultaneously for similar sets. In particular, $\approx$ preserves the notion of stages and universes:

Lemma 40. *If* $x \approx a$ *and* x *is a stage, then* a *is a stage.*

Proof. We show that all a with $x \approx a$ must be stages by stage induction on x. So suppose x is a stage and we have $\mathcal{P}x \approx b$. Since $x \in \mathcal{P}x$, by $\mathcal{P}x \triangleright b$ there is $a \in b$ with $x \approx a$. Then by induction a is a stage. Moreover, Lemma 36 implies that $\mathcal{P}x \approx \mathcal{P}a$. Then by functionality we know that b equals the stage $\mathcal{P}a$.

Now suppose x is a set of stages and we have $\bigcup x \approx b$. Since $\mathcal{P}(\mathcal{P}(\bigcup x)) \approx \mathcal{P}(\mathcal{P}b)$ by Lemma 36 and $x \in \mathcal{P}(\mathcal{P}(\bigcup x))$ there is some $a \in \mathcal{P}(\mathcal{P}b)$ with $x \approx a$. But then we know that $\bigcup x \approx \bigcup a$ by Lemma 35 and $b = \bigcup a$ by functionality, so it remains to show that a is a set of stages. Indeed, if we let $c \in a$ then $x \triangleleft a$ yields $y \in x$ with $y \approx c$ and since x is a set of stages we can apply the inductive hypothesis for y to establish that c is a stage. $\square$

Lemma 41. *If* $x \approx a$ *and* x *is a universe, then* a *is a universe.*

Proof. We first show that a is transitive, so let $c \in b \in a$. By bounded surjectivity there are $z \in y \in x$ with $z \approx c$ and $y \approx b$. Then $z \in x$ since x is transitive, which implies $c \in a$ since $\approx$ preserves membership.

The proofs that a is closed under the set constructors are all similar. Consider some $b \in a$, then for instance we show $\bigcup b$ in a. The assumption $x \approx a$ yields $y \in x$ with $y \approx b$. Since x is closed under union it follows $\bigcup y \in x$ and since $\bigcup y \approx \bigcup b$ by Lemma 35 it follows that $\bigcup b \in a$. The proof for power is completely analogous and for replacement one first mechanically verifies that $\overline{R}@y \subseteq x$ for every functional relation $R \in \mathcal{F}(N)$ with $R@b \subseteq a$. $\square$

In order to establish the maximality of $\approx$ we first prove it maximal on stages:

Lemma 42. *Either* $\mathcal{S}_M \subseteq \mathsf{dom}(\approx)$ *or* $\mathcal{S}_N \subseteq \mathsf{ran}(\approx)$*.*

Proof. Suppose there were $x \notin \mathsf{dom}(\approx)$ and $a \notin \mathsf{ran}(\approx)$, then we can in particular assume x and a to be the least such stages by Lemma 21. We will derive the contradiction $x \approx a$. By symmetry, we just have to show $x \triangleright a$ which we do by stage induction for x. The case $\mathcal{P}(x)$ for some stage x is impossible given that, by leastness of $\mathcal{P}x \notin \mathsf{dom}(\approx)$, necessarily $x \in \mathsf{dom}(\approx)$ holds which would, however, imply $\mathcal{P}x \in \mathsf{dom}(\approx)$ by Lemma 36.

In the case $\bigcup x$ for a set of stages x we may assume that $x \subseteq \bigcup x$ by Fact 26. Now suppose $y \in z \in x$, then we want to find $b \in W$ with $y \approx b$. We do case analysis whether or not $z \in \mathsf{dom}(\approx)$. If so, then there is c with $z \approx c$. Since $z \in x$ we know that z is a stage and so must be c by Lemma 40. Then by linearity it must be $c \in W$ and $z \triangleright c$ yields the wished $b \in W$ with $y \approx b$. If z were not in $\mathsf{dom}(\approx)$, we have $\bigcup x \subseteq z$ since $\bigcup x$ is the least stage not in the domain. But since $z \in x$ and $x \subseteq \bigcup x$ this yields $z \in z$ contradicting well-foundedness. □

Theorem 43. *The relation $\approx$ is maximal, that is $M \subseteq \mathsf{dom}(\approx)$ or $N \subseteq \mathsf{ran}(\approx)$.*

Proof. Suppose $\approx$ were neither total nor surjective, so there were $x \notin \mathsf{dom}(\approx)$ and $a \notin \mathsf{ran}(\approx)$. By Fact 24 we know that $x \in \mathcal{P}(\rho x)$ and $a \in \mathcal{P}(\rho a)$. Then by Lemma 42 it is either $\mathcal{P}(\rho x) \in \mathsf{dom}(\approx)$ or $\mathcal{P}(\rho a) \in \mathsf{ran}(\approx)$. But then it follows either $x \in \mathsf{dom}(\approx)$ or $a \in \mathsf{ran}(\approx)$ contradicting the assumption. □

From this theorem we can conclude that embeddebility is a linear pre-order on models of ZF. We can further strengthen the result by proving one side of $\approx$ small if $\approx$ is not already **full**, meaning both total and surjective.

Lemma 44. *If x is a stage with $x \notin \mathsf{dom}(\approx)$, then $\mathsf{dom}(\approx) \subseteq x$.*

Proof. Since $x \notin \mathsf{dom}(\approx)$ we know that $\approx$ is surjective by Theorem 43. So let $y \approx a$, then we want to show that $y \in a$. By exhaustiveness a occurs in some stage b and since $\approx$ is surjective there is z with $z \approx b$. Lemma 40 justifies that z is a stage. By linearity we have either $z \subseteq x$ or $x \in z$. In the former case we are done since $y \in z$ given that $\approx$ respects the membership $a \in b$. The other case is a contradiction since it implies $x \in \mathsf{dom}(\approx)$. □

The dual holds for the stages of N and $\mathsf{ran}(\approx)$, hence we summarise:

Theorem 45. *Exactly one of the following statements holds:*
(1) $\approx$ is full, so $M \subseteq \mathsf{dom}(\approx)$ and $N \subseteq \mathsf{ran}(\approx)$.
(2) $\approx$ is surjective and $\mathsf{dom}(\approx)$ is small and a universe of M.
(3) $\approx$ is total and $\mathsf{ran}(\approx)$ is small and a universe of N.

Proof. Suppose $\approx$ were not full, then it is still maximal by Theorem 43. So for instance let $\approx$ be surjective but not total, then we show (2). Being not total, $\approx$ admits a stage x with $x \notin \mathsf{dom}(\approx)$. Then by Lemma 44 we know $\mathsf{dom}(\approx) \subseteq x$, so the domain is realised by $x \cap \mathsf{dom}(\approx)$. This set is a universe by Lemma 39. □

5 Categoricity Results

In the remainder of this work, we examine to what extent the model theory of **ZF** is determined and study categorical extensions. If $\approx$ is full for models M and N, we call M and N **isomorphic**. An axiomatisation is called **categorical** if all of its models are isomorphic. Without assuming any further axioms, we can prove **ZF** categorical in every cardinality:

Theorem 46. *Equipotent models of* **ZF** *are isomorphic.*

Proof. If models M and N are equipotent, we have a function $F : M \to N$ with inverse $G : N \to M$. Then from either of the cases (2) and (3) of Theorem 45 we can derive a contradiction. So for instance suppose $\approx$ is surjective and $X = \mathsf{dom}(\approx)$ is a universe of M. We use a variant of Cantor's argument where G simulates the surjection of X onto the power set of X. Hence define $Y := \{\, x \in X \mid x \notin G(ix) \,\}$ where i is the function obtained from $\approx$ by description. Then Y has preimage $y := i^{-1}(FY)$ and we know that $y \in X$ by surjectivity. Hence, by definition of Y we have $y \in Y$ iff $y \notin G(iy) = G(i(i^{-1}(FY))) = G(F(Y)) = Y$, contradiction. Thus case (1) holds and so $\approx$ is indeed full. □

An internal way to determine the cardinality of models and hence to obtain full categoricity is to control the number of universes guaranteed by the axioms. For instance, one can add an axiom excluding the existence of any universe.

Definition 47. $\mathbf{ZF}_0$ *is* **ZF** *plus the assertion that there exists no universe.*

Note that $\mathbf{ZF}_0$ axiomatises exactly the structure of hereditarily finite sets [1,13] and this is of course incompatible with an infinity axiom. That $\mathbf{ZF}_0$ is consistent relative to **ZF** is guaranteed:

Lemma 48. *Every model of* **ZF** *has an inner model without universes.*

Proof. Let M be a model of **ZF**. If M contains no universe, then the full class $(\lambda x.\top)$ is an inner model of $\mathbf{ZF}_0$. Otherwise, if M contains a universe u, then we can assume u to be the least such universe since universes are stages by Lemma 30 and stages are well-ordered by Lemma 21. Then it follows that u constitutes an inner model of $\mathbf{ZF}_0$. First, u is an inner model of **ZF** by Lemma 14. Secondly, if there were a universe u' in the sub-structure induced by u, then u' would be a universe that is smaller than u, contradiction. □

Lemma 49. $\mathbf{ZF}_0$ *is categorical.*

Proof. Again from either of the cases (2) and (3) of Theorem 45 we can derive a contradiction. So for instance suppose $\approx$ is surjective and $X = \mathsf{dom}(\approx)$ is a universe of M. This directly contradicts the minimality assumption of M. □

The categoricity result for $\mathbf{ZF}_0$ can be generalised to axiomatisations that guarantee exactly n universes. Note that stating axioms of such a form presupposes an external notion of natural numbers, for instance given by the inductive type $\mathbb{N}$. We avoid employing further external structure such as lists to express finite cardinalities and instead make use of the linearity of universes as follows:

Definition 50. *We define* $\mathbf{ZF}_{n+1}$ *to be* **ZF** *plus the following assertions:*
(1) there exists a universe that contains at least n universes and
(2) there exists no universe that contains at least $n+1$ universes.
The notion that a universe u contains at least n universes is defined recursively with trivial base case and where u is said to contain $n+1$ universes if there is a universe $u' \in u$ that contains at least n universes.

Since it is undecided whether or not a given model contains a universe, we cannot construct inner models that satisfy $\mathbf{ZF}_{n+1}$ for any n. Due to the connection of universes and inaccessible cardinals (cf. [20]), $\mathbf{ZF}_{n+1}$ constitutes a rise in proof-theoretic strength over $\mathbf{ZF}_n$. Independent of the consistency question, we can still prove all models of $\mathbf{ZF}_n$ isomorphic for every n:

Lemma 51. $\mathbf{ZF}_n$ *is categorical for all* n.

Proof. We have already proven $\mathbf{ZF}_0$ categorical in Lemma 49 so we just have to consider $\mathbf{ZF}_{n+1}$. As in the two proofs above we suppose that $\approx$ is surjective as well as that $X = \mathsf{dom}(\approx)$ is a universe of M and derive a contradiction. In fact, we show that X contains at least $n+1$ universes and hence violates (2) of the above definition for M. By (1) for N we know there is a universe $u \in N$ that contains at least n universes. Hence by surjectivity we know that $i^{-1}u \in X$, where i is again the function obtained from $\approx$. Then Lemma 41 implies that $i^{-1}u$ is a universe of M. Moreover, since $\approx$ preserves all structure, it follows that $i^{-1}u$ contains at least n universes as u did. But then X contains a universe that contains at least n universes, so it must contain at least $n+1$ universes. $\square$

We remark that this process can be extended to transfinite ordinalities. For instance, one could consider axiomatisations $\mathbf{ZF}_W$ relative to a well-ordered type W with the axiom that W and the class of universes are order-isomorphic. Then it follows that $\mathbf{ZF}_W$ is categorical, subsuming our discussed examples.

6 Discussion

The formalisation of ZF in a type theory with inductive predicates as examined in this work differs from common textbook presentations (cf. [14,8,6]) in several ways, most importantly in the use of second-order replacement and the inductive definition of the cumulative hierarchy. Now we briefly outline some of the consequences.

Concerning the second-order version of the replacement axiom, it has been known since Zermelo [22] that second-order ZF admits the embedding theorem for models. It implies that models only vary in their external cardinality, i.e. the notion of cardinality defined by bijections on type level or, equivalently, in height of their cumulative hierarchy. Thus controlling these parameters induces categorical axiomatisations.

As a consequence of categoricity, all internal properties (including first-order undecided statements such as the axiom of choice or the continuum hypothesis) become semantically determined in that there exist no two models such that a property holds in the first but fails in the second (cf. [7,18]). This is strikingly different from the extremely undetermined situation in first-order ZF, where models can be arbitrarily incomparable and linearity of embeddability is only achieved in extremely controlled situations (cf. [5]). This is related to the fact that the inner models admitted by second-order ZF are necessarily universes whereas those of first-order ZF can be subsets of strictly less structure.

The main insight is that the second-order replacement axiom asserts the existence of all subsets of a given set contrarily to only the definable ones guaranteed by a first-order scheme. This fully determines the extent of the power set operation whereas it remains underspecified in first-order ZF. Concretely, first-order ZF admits counterexamples to Lemma 36. Furthermore, the notions of external cardinality induced by type bijections and internal cardinality induced by type bijections that can be encoded as sets coincide in second-order ZF since every bijection witnessing external equipotence of sets can be represented by a replacement set. That the two notions of cardinality differ for first-order set theory has been pointed out by Skolem [11]. The Löwenheim-Skolem Theorem implies the existence of a countable model of first-order ZF (that still contains internally uncountable sets) whereas models of second-order ZF with infinity are provably uncountable.

Inductive predicates make a set-theoretic notion of ordinals in their role as a carrier for transfinitely recursive definitions superfluous. Consider that commonly the cumulative stages are defined by $V_\alpha := \mathcal{P}^\alpha\emptyset$ using transfinite recursion on ordinals α. However, this presupposes at least a basic ordinal theory including the recursion theorem, making the cumulative hierarchy not immediately accessible. That this constitutes an unsatisfying situation has been addressed by Scott [10] where an axiomatisation of ZF is developed from the notion of rank as starting point.

In the textbook approach, the well-ordering of the stages V_α is inherited directly from the ordinals by showing $V_\alpha \subseteq V_\beta$ iff $\alpha \subseteq \beta$. Without presupposing ordinals, we have to prove linearity of $\subseteq$ and the existence of least $\subseteq$-elements directly. As it was illustrated in this work these direct proofs are not substantially harder than establishing the corresponding properties for ordinals.

We end with a remark on our future directions. We plan to first make the axiomatisations $\mathbf{ZF}_W$ precise and formalise the categoricity proof. Subsequently, we will turn to the consistency question and construct actual models following Aczel [2], Werner [19], and Barras [3]. Note that all these implement a flavour of (constructive) second-order ZF whereas Paulson [9] develops classical first-order ZF using the proof assistant Isabelle. We conjecture that the type theory of Coq with excluded middle and a weak form of choice allows for constructing models of $\mathbf{ZF}_n$ for every n. Moreover, it would be interesting to formalise first-order ZF in type theory by making the additional syntax for predicates and relations explicit. Then the classical relative consistency results concerning choice and the continuum hypothesis can be examined.

References

1. W. Ackermann. Die Widerspruchsfreiheit der allgemeinen Mengenlehre. *Mathematische Annalen*, 114:305–315, 1937.
2. P. Aczel, A. Macintyre, L. Pacholski, and J. Paris. The type theoretic interpretation of constructive set theory. *Journal of Symbolic Logic*, 49(1):313–314, 1984.
3. B. Barras. Sets in Coq, Coq in Sets. *Journal of Formalized Reasoning*, 3(1):29–48, Oct. 2010.
4. N. Bourbaki. Sur le théorème de Zorn. *Archiv der Mathematik*, 2(6):434–437, 1949.
5. J. D. Hamkins. Every Countable Model of Set Theory Embeds into its own Constructible Universe. *Journal of Mathematical Logic*, 13(02), Dec. 2013.
6. K. Hrbacek and T. Jech. *Introduction to Set Theory, Third Edition, Revised and Expanded*. CRC Press, June 1999.
7. G. Kreisel. Two Notes on the Foundations of Set-Theory. *Dialectica*, 23(2):93–114, 1969.
8. K. Kunen. *Set Theory: An Introduction to Independence Proofs*. Elsevier, June 2014.
9. L. C. Paulson. Set theory for verification: I. from foundations to functions. *Journal of Automated Reasoning*, 11(3):353–389, Oct 1993.
10. D. Scott. Axiomatizing Set Theory. *Proceedings of Symposia in Pure Mathematics*, 13:207–214, 1974.
11. T. Skolem. Some Remarks on Axiomatized Set Theory. In J. van Heijenoort, editor, *From Frege to Gödel: A Sourcebook in Mathematical Logic*, pages 290–301. toExcel, Lincoln, NE, USA, 1922.
12. G. Smolka, S. Schäfer, and C. Doczkal. Transfinite Constructions in Classical Type Theory. In X. Zhang and C. Urban, editors, *Interactive Theorem Proving - 6th International Conference, ITP 2015, Nanjing, China, August 24-27, 2015*, LNCS 9236. Springer-Verlag, 2015.
13. G. Smolka and K. Stark. Hereditarily Finite Sets in Constructive Type Theory. In *Interactive Theorem Proving*, pages 374–390. Springer, Aug. 2016.
14. R. Smullyan and M. Fitting. *Set Theory and the Continuum Problem*. Dover books on mathematics. Dover Publications, 2010.
15. P. Suppes. *Axiomatic Set Theory*. Dover Books on Mathematics Series. Dover Publications, 1960.
16. The Coq Proof Assistant. `http://coq.inria.fr`.
17. G. Uzquiano. Models of Second-Order Zermelo Set Theory. *The Bulletin of Symbolic Logic*, 5(3):289–302, 1999.
18. J. Väänänen. Second-Order Logic or Set Theory? *The Bulletin of Symbolic Logic*, 18(1):91–121, 2012.
19. B. Werner. Sets in Types, Types in Sets. In *Theoretical Aspects of Computer Software*, pages 530–546. Springer, Heidelberg, Sept. 1997.
20. N. H. Williams. On Grothendieck Universes. *Compositio Mathematica*, 21(1):1–3, 1969.
21. E. Zermelo. Neuer Beweis für die Möglichkeit einer Wohlordnung. *Mathematische Annalen*, 65:107–128, 1908.
22. E. Zermelo. Über Grenzzahlen und Mengenbereiche: Neue Untersuchungen über die Grundlagen der Mengenlehre. *Fundamenta Mathematicæ*, 16:29–47, 1930.