Categoricity Results and Large Model Constructions for Second-Order ZF in Dependent Type Theory

Dominik Kirst and Gert Smolka

Received: 26 February 2018 / Accepted: 16 August 2018

Abstract We formalise second-order ZF set theory in the dependent type theory of Coq. Assuming excluded middle, we prove Zermelo's embedding theorem for models, categoricity in all cardinalities, and the categoricity of extended axiomatisations fixing the number of Grothendieck universes. These results are based on an inductive definition of the cumulative hierarchy eliminating the need for ordinals and set-theoretic transfinite recursion.

Following Aczel's sets-as-trees interpretation, we give a concise construction of an intensional model of second-order ZF with a weakened replacement axiom. Whereas this construction depends on no additional logical axioms, we obtain intensional and extensional models with full replacement assuming a description operator for trees and a weak form of proof irrelevance. In fact, these assumptions yield large models with n Grothendieck universes for every number n.

Keywords dependent type theory, second-order set theory, categoricity, model constructions, sets-as-trees interpretation, Coq

1 Introduction

Some operations in ZF set theory have a higher-order character: starting from some set x, separation yields subsets $\{\, y \in x \mid P\, y \,\}$ based on predicates P, and replacement yields image sets $\{\, z \mid \exists y \in x.\, R\, y\, z \,\}$ based on functional relations R. Second-order ZF differs from first-order ZF in that the separation and replacement axioms quantify over all predicates and relations at the class level, respectively. This is faithful to Zermelo's informal view of axiomatic set theory [30] and in sharp contrast to the standard first-order axiomatisation of ZF relying on axiom schemes (cf. [14,10]). The difference between the two theories shows in the existence of artificial and counterintuitive models of first-order ZF that are excluded by the more determined second-order ZF [25].

D. Kirst and G. Smolka
Saarland University
Saarland Informatics Campus
Saarbrücken, Germany
E-mail: {kirst, smolka}@ps.uni-saarland.de

This is a pre-print of an article published in the Journal of Automated Reasoning. The final authenticated version is available online at: https://doi.org/10.1007/s10817-018-9480-6

Zermelo [30] 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 [28] (i.e. sets closed under all set constructions).

The present paper studies second-order ZF in the dependent type theory of Coq [23] augmented by excluded middle (XM). We sharpen Zermelo's result by showing that our concrete axiomatisation **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 $\mathbf{ZF}_n$, which is **ZF** extended by an axiom asserting exactly n universes, is categorical (i.e. all models are isomorphic).

We subsequently apply Aczel's sets-as-types interpretation [1, 27] to construct models for our concrete axiomatisations. This interpretation employs the inductive type of well-founded trees to model the membership structure of sets. All set operations but the non-constructive component of replacement called description can be implemented using their type-theoretical counterparts. Also, since different trees may share the same structure, the tree model does not satisfy the usual extensionality of ZF. Assuming a strong quotient axiom in the form of a description operator for trees (TD) together with a weak form of proof irrelevance (PI_γ), we close the gap and obtain an actual model of the axiomatisation **ZF**. Moreover, the same assumptions allow for constructing large models of all $\mathbf{ZF}_n$.

For our results we employ the cumulative hierarchy, 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 to establish the cumulative hierarchy is through transfinite recursion on ordinals. We replace this long-winded first-order approach by 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 [20, 19]. Tower constructions go back to Zermelo [29] and Bourbaki [6], and are used by Smullyan and Fitting [20] to obtain the ordinal hierarchy.

This paper is an extended version of a previous conference publication [11] including material from a follow-up paper [12]. The mathematical development 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 in some parts of the development and do not miss further built-in support for classical reasoning. The Coq development accompanying this paper has less than 4500 lines of code (about 1600 for specifications and 2700 for proofs) and can be found at `https://www.ps.uni-saarland.de/extras/jar-sets`. The theorems and definitions of the PDF version of this paper are hyperlinked with the Coq development: by a single click one reaches the corresponding position in the Coq development.

The paper is organised in three technical main sections. In Section 2, we introduce our axiomatisation **ZF** and study its internal theory including Grothendieck universes, different forms of replacement, and the cumulative hierarchy. This is followed by a proof of Zermelo's embedding theorem and derived categoricity results in Section 3. In Section 4, regarding consistency, we first construct an axiom-free intensional model and then obtain extensional and large models assuming proof-irrelevant tree description. We end with remarks comparing our type-theoretic approach to ZF set theory with the standard first-order approach and a discussion of further consistency results.

2 Second-Order ZF

Using a type-theoretic approach, an axiomatisation of set theory can be expressed as a predicate on types providing the necessary structure for set-theoretic language. Types satisfying the axioms are models and assuming a model allows for developing the internal theory of the axiomatisation. Following this paradigm, this section is concerned with our concrete axiomatisation **ZF** and internal constructions such as Grothendieck universes and the cumulative hierarchy.

2.1 Structures and Axiomatisations

We begin by introducing some preliminary notation and jargon. We distinguish the sorts Type and Prop of **types** and **propositions**, respectively. The symbol $=$ denotes the standard inductive charaterisation of Leibniz equality. For any type A we call a unary predicate $P : A \to \mathsf{Prop}$ a **class** over A and write $a \in P$ for $P\,a$. In every context of the symbol $\in$ we employ the canonical meaning of $\subseteq$, so for instance $P' \subseteq P$ denotes that $a \in P$ for all $a \in P'$. Furthermore, for a binary relation $R : A \to B \to \mathsf{Prop}$ on two types A and B we define classes $\mathsf{dom}(R) \coloneqq \lambda a.\, \exists b.\, R\,a\,b$ and $\mathsf{ran}(R) \coloneqq \lambda b.\, \exists a.\, R\,a\,b$ representing **domain** and **range** of R. For any type A and class P over A we write $\langle a : A \mid a \in P \rangle$ for the refinement type $\Sigma a : A.\, a \in P$ and $\exists! a.\, a \in P$ if there is a unique $a : A$ with $a \in P$. Finally, two types A and B are called **equipotent** if there are mutually inverse functions $f : A \to B$ and $f^{-1} : B \to A$.

Definition 1 *A **set structure** is a type $\mathcal{M}$ with a relation $\in\colon \mathcal{M} \to \mathcal{M} \to \mathsf{Prop}$ called **membership**. $\mathcal{M}$ is a **ZF-structure** if it further provides the following constants:*

$$
\begin{array}{rll}
\emptyset : \mathcal{M} & & \text{(empty set)} \\
\{\_\,,\_\} : \mathcal{M} \to \mathcal{M} \to \mathcal{M} & & \text{(unordered pair)} \\
\bigcup : \mathcal{M} \to \mathcal{M} & & \text{(union)} \\
\mathcal{P} : \mathcal{M} \to \mathcal{M} & & \text{(power set)} \\
\_ \cap \_ : (\mathcal{M} \to \mathsf{Prop}) \to \mathcal{M} \to \mathcal{M} & & \text{(separation)} \\
\_ \mathbin{@} \_ : (\mathcal{M} \to \mathcal{M}) \to \mathcal{M} \to \mathcal{M} & & \text{(replacement)} \\
\delta : (\mathcal{M} \to \mathsf{Prop}) \to \mathcal{M} & & \text{(description/unique choice)}
\end{array}
$$

Note that the upper four constants are first-order, whereas the lower three operations take classes or functions as arguments. A class P over a set structure $\mathcal{M}$ is called **small** if there exists $x : \mathcal{M}$ that **agrees** with P, i.e. $y \in x$ iff $y \in P$ for all $y : \mathcal{M}$. Given any ZF-structure, we employ the usual shorthands $\{x\} \coloneqq \{x, x\}$ and $x \cup y \coloneqq \bigcup \{x, y\}$. Moreover, we identify sets x with their corresponding classes $\lambda y.\, y \in x$.

Definition 2 *For a set structure $\mathcal{M}$ we define the class WF of **well-founded sets** by*

$$\frac{\forall y \in x.\, y \in WF}{x \in WF}$$

The corresponding induction principle eliminating into Prop is called $\in$-induction and the recursion principle eliminating into Type is called $\in$-recursion.

In Coq's type theory, $x \in WF$ can indeed be eliminated to arbitrary types since WF is defined using a single constructor taking only parameters and proofs as arguments. So one can define functions $F : \mathcal{M} \to X$ for a type X with the definition of $F\,x$ depending on the values $F\,y$ for all $y \in x$. See Definition 70 for an example.

Definition 3 *A ZF-structure $\mathcal{M}$ is a **model of** **ZF** if the following propositions hold:*

Ext :	$x \subseteq y \to y \subseteq x \to x = y$	
Found :	$x \in WF$	
Inf :	$\exists \omega.\, \forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \mathcal{P}^n\, \emptyset$	
Eset :	$x \notin \emptyset$	
Pair :	$z \in \{x, y\} \leftrightarrow z = x \vee z = y$	
Union :	$z \in \bigcup x \leftrightarrow \exists y \in x.\, z \in y$	
Power :	$y \in \mathcal{P} x \leftrightarrow y \subseteq x$	
Sep :	$y \in P \cap x \leftrightarrow y \in x \wedge y \in P$	$(P : \mathcal{M} \to \mathsf{Prop})$
Frep :	$z \in F@x \leftrightarrow \exists y \in x.\, z = F\,y$	$(F : \mathcal{M} \to \mathcal{M})$
Desc :	$(\exists! x.\, x \in P) \to \delta P \in P$	$(P : \mathcal{M} \to \mathsf{Prop})$

*We write $\mathcal{M} \models$ **ZF** if $\mathcal{M}$ is a model of* **ZF** *and use the same notation for all upcoming axiomatisations. We define* $\overline{\textbf{ZF}}$ *to be* **ZF** *without* Inf.

Note that the first three axioms determine structural aspects of the available models whereas the other axioms clarify the membership laws of the first- respectively second-order set operations. Our axiomatisation is similar to a formulation of intensional second-order ZF given by Barras [4]. In comparison, **ZF** imposes extensionality via Ext, however, we will also encounter intensional versions in Section 4. We further use a version of replacement for functions together with a description operator and reconstruct the equivalent relational formulation from Barras [4] in Section 2.3. Thereby we separate relational replacement into a constructive and a non-constructive component, where the former is definable for the axiom-free tree model in Section 4.2 and the latter is not. Description expresses unique choice on ZF-structures.

Also note that Inf is a non-standard (but equivalent) formulation of the infinity axiom in using power sets instead of the von Neumann successor $\sigma x \coloneqq x \cup \{x\}$ and in referring to the external notion of natural numbers. The power set operation naturally matches to the structure of the cumulative hierarchy studied in Section 2.4 and using external numbers is anyway unavoidable for the forthcoming Definition 6.

2.2 Grothendieck universes

We now turn to the question what it means for a set or model to be large. A natural criterion is to ask whether a set is closed under the set operations, meaning that it may serve as a full **universe** for set-theoretic constructions and in fact constitutes a submodel (Lemma 78). Then a nested hierarchy of universes is an indicator for increasing size. An alternative approach would be to explicitly examine the set cardinalities, where so-called **strongly inaccessible cardinals** witness largeness. In fact, in the presence of choice, both approaches coincide [28] and in this work we develop the more elementary approach via universes. We fix a ZF-structure $\mathcal{M}$.

Definition 4 *We call a class P over $\mathcal{M}$ **transitive** if $y \in x \in P$ implies $y \in P$. Similarly, we say that P is **swelled** if $y \subseteq x \in P$ implies $y \in P$.*

Consider the von Neumann ordinal $\overline{3} := \sigma^3\,\emptyset = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. It is easy to verify that $\overline{3}$ is transitive – a general property of von Neumann ordinals $\overline{n} := \sigma^n\,\emptyset$. However, $\overline{3}$ is not swelled given that $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\} \in \overline{3}$ but $\{\{\emptyset\}\} \notin \overline{3}$.

Definition 5 *A transitive class U over $\mathcal{M}$ is **ZF-closed** if it is closed under all set operations. That is, for all $x, y \in U$, classes $P : \mathcal{M} \to \mathsf{Prop}$ and functions $F : \mathcal{M} \to \mathcal{M}$*

(1) $\emptyset \in U$
(2) $\{x, y\} \in U$
(3) $\bigcup x \in U$
(4) $\mathcal{P}x \in U$
(5) $P \cap x \in U$
(6) $F@x \in U$ if $F@x \subseteq U$

*If U is ZF-closed and small, we call it (and the corresponding set) a **universe**.*

Note that a ZF-closed class U yields a submodel $\mathcal{M}_U$ that satisfies $\overline{\mathbf{ZF}}$ (Lemma 78). As ZF-closed classes are not demanded to contain ω in general, the submodel $\mathcal{M}_U$ does not necessarily satisfy Inf.

Definition 6 *We define the **strength** of sets by saying that every set has strength 0 and that x has strength $n+1$ if there is a universe $U \in x$ of strength n. Then we define:*
(1) $\mathbf{ZF}_{\geq n}$ is $\overline{\mathbf{ZF}}$ plus asserting a set of strength n,
(2) $\mathbf{ZF}_n$ is $\mathbf{ZF}_{\geq n}$ plus excluding sets of strength $n+1$,
(3) $\mathbf{ZF}_{\geq \omega}$ is $\mathbf{ZF}$ plus asserting sets of all strengths n.
If $\mathcal{M} \models \mathbf{ZF}_{\geq n}$ for some n we say that $\mathcal{M}$ has strength n.

Note that the notion of set and model strength is only a lower bound and hence not unique, given that every set respectively model of strength n also has strength m for all $m < n$. Further, see [11], [12], and the Coq development for a proof that models of $\mathbf{ZF}$ are uncountable and that $\mathbf{ZF}$ is equivalent to $\mathbf{ZF}_{\geq 1}$. Due to this equivalence and hence to avoid $\mathbf{ZF}_0$ being contradictory, the definition of $\mathbf{ZF}_{\geq n}$ must be based on $\overline{\mathbf{ZF}}$ from Definition 3 rather than $\mathbf{ZF}$.

2.3 Relational Replacement

We assume a model $\mathcal{M}$ of $\mathbf{ZF}$. As mentioned before, functional replacement, separation and description can be combined into relational replacement:

Definition 7 $R@x := (\lambda y.\, \delta(R\,y))@(\mathsf{dom}(R) \cap x)$

Relational replacement (Rep) then holds for the class $\mathcal{F}(\mathcal{M})$ of functional relations $R : \mathcal{M} \to \mathcal{M} \to \mathsf{Prop}$, i.e. relations R with $y = y'$ whenever $R\,x\,y$ and $R\,x\,y'$.

Fact 8 $R \in \mathcal{F}(\mathcal{M}) \to (z \in R@x \leftrightarrow \exists y.\, y \in x \wedge R\,y\,z)$

Proof Let R be functional and let $z \in R@x$. Then by the above definition and the functional replacement axiom we know there is $y \in \mathsf{dom}(R) \cap x$ with $z = \delta(R\,y)$. By $y \in \mathsf{dom}(R)$ and the functionality of R we know that the description axiom applies, so $R\,y\,(\delta(R\,y))$ and thus $R\,y\,z$.

Conversely, suppose that there is $y \in x$ with $R\,y\,z$. By this assumption we can again deduce $R\,y\,(\delta(R\,y))$ and hence $z = \delta(R\,y)$. Since we also know $y \in \mathsf{dom}(R)$ the functional replacement axiom implies $z \in R@x$. □

Relational replacement in turn is strong enough to easily express the operations of pairing, separation, functional replacement and description (cf. [22], [16], [11]).

Fact 9 *The following equations hold:*

(1) $\{x, y\} = (\lambda ab.\, (a = \emptyset \land b = x) \lor (a = \mathcal{P}\emptyset \land b = y))@\mathcal{P}(\mathcal{P}\emptyset)$

(2) $P \cap x = (\lambda ab.\, a \in P \land a = b)@x$

(3) $F@x = (\lambda ab.\, b = F\, a)@x$

(4) $\delta P = \bigcup((\lambda ab.\, b \in P)@\mathcal{P}\emptyset)$ if there is a unique $x \in P$

Proof Since all relations employed are functional, the equations are straight-forward by Rep and the other membership axioms. □

This means that the axiomatisation **ZF** is actually redundant, as pairing can be defined, and that we can give a simplified criterion for ZF-closed classes:

Fact 10 *A class U over $\mathcal{M}$ is ZF-closed iff it is transitive, contains $\emptyset$ and is closed under union, power and relational replacement.*

Proof Suppose U is ZF-closed, we just have to show that it is closed under relational replacement. That is, we assume $x \in U$ and $R@x \subseteq U$ for a functional relation R and have to show that $R@x \in U$. Since U is closed under separation we know that $\mathsf{dom}(R) \cap x \in U$. Thus we can apply the closure under functional replacement to obtain $R@x \in U$ where the necessary condition is exactly $R@x \subseteq U$.

Now let U be closed under union, power and relational replacement, then we have to show closure under pairing, separation and functional replacement. This follows since we can express these operations by relational replacement. □

Henceforth, by just saying replacement we always refer to the functional form.

2.4 Cumulative Hierarchy

It is a main feature of ZF-like set theories that the domain of sets can be stratified by a class of $\subseteq$-well-ordered cumulative 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. However, since establishing the linearity and least elements of the well-ordering relies on classical reasoning, we have to assume **excluded middle** (XM) as an axiom.

Axiom (XM) $\forall A : \mathsf{Prop}.\, A \lor \neg A$

Excluded middle implies **proof irrelevance** (PI), a statement first established by Coquand [7] and formalised in the Coq standard library based on [3].

Fact 11 $\forall (A : \mathsf{Prop})\, (H, H' : A).\, H = H'$

We further assume a model $\mathcal{M} \models \mathbf{ZF}$.

Definition 12 *We define the inductive class $\mathcal{V}$ of **stages** by the following rules:*

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

Fact 13 *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 $\emptyset \subseteq \mathcal{V}$.
(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 14 *Let x be a stage, P a class and $a, b \in x$ then:*

(1) $\bigcup a \in x$ (3) $\{a, b\} \in \mathcal{P}x$
(2) $\mathcal{P}a \in \mathcal{P}x$ (4) $P \cap a \in x$

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 straight-forward using the membership axiom for pairs.
(4) follows since x is swelled and $P \cap a \subseteq a$. □

We now show that the class $\mathcal{V}$ is well-ordered by $\subseteq$. Since $\subseteq$ is a partial order we just have to prove linearity and the existence of least elements, which both rely on XM. An economical proof of linearity employs the following **double-induction principle** [20]:

Fact 15 *For a binary relation R on stages it holds that $R\,x\,y$ for all $x, y \in \mathcal{V}$ if*
(1) $R\,(\mathcal{P}x)\,y$ whenever $R\,x\,y$ and $R\,y\,x$ and
(2) $R\,(\bigcup x)\,y$ whenever $R\,z\,y$ for all $z \in x$.

Proof By nested stage induction. □

Lemma 16 *If $x, y \in \mathcal{V}$, 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 $R\,x\,y$ and $R\,y\,x$ and using that $x \subseteq \mathcal{P}x$ for stages x. (2) 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 $z \not\subseteq y$. So by the assumption $R\,z\,y$ only $\mathcal{P}y \subseteq z$ can be the case which implies $\mathcal{P}y \subseteq \bigcup x$. □

Fact 17 *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 16. Then (3) is by (2). □

Lemma 18 *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 must be 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 19 *We call $a \in \mathcal{V}$ 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 using description.*

Lemma 20 *$\rho x = \bigcup \mathcal{P}@(\rho@x)$ 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 $z \coloneqq \bigcup \mathcal{P}@(\rho@x)$. 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 must be the rank of x. □

It follows that every set occurs in a stage:

Fact 21 *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 studying classes of stages that are closed under some or all set constructors. The two introduction 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 22 *We call $x \in \mathcal{V}$ a **limit** if $x = \bigcup x$ and a **successor** if $x = \mathcal{P}y$ for some $y \in \mathcal{V}$. Note that this means that $\emptyset$ is a limit.*

Fact 23 *If $x \subseteq \mathcal{V}$, 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 24 *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 23. 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 25 *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 13 and 14. 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 14. □

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 26 *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 20. Thus $\rho a \in u$ follows from the closure properties of u. □

Lemma 27 *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. This is done by showing that $u = \bigcup(\mathcal{V} \cap u)$. The inclusion $u \supseteq \bigcup(\mathcal{V} \cap u)$ is by transitivity of u. For the converse suppose $x \in u$. Then $x \subseteq \bigcup(\mathcal{V} \cap u)$ again by knowing $x \in \mathcal{P}(\rho x) \in u$. □

We remark that inhabited limits are models of the set theory $\overline{\mathbf{Z}}$ which is **ZF** without replacement and description. Furthermore, the existence of an infinite set ω asserted by Inf induces the existence of the initial universe $\bigcup \omega$ of hereditarily finite sets, as formalised in [12].

3 Categoricity

Turning to model-theoretic considerations, in this section we prove the embedding theorem given by Zermelo [30]. Phrased for our concrete axiomatisation, it states that of any two models of **ZF** one embeds as a universe into the other. We derive that **ZF** is categorical in every cardinality and that controlling the height of the cumulative hierarchy yields categorical axiomatisations. The embedding theorem and the derived results rely on classical reasoning, so we still assume XM throughout this section.

3.1 Zermelo's Embedding Theorem

Given two models $\mathcal{M}$ and $\mathcal{N}$ of **ZF**, we define a structure-preserving embedding $\approx$, called $\in$-bisimilarity, and prove it either total or surjective. In this case we call $\approx$ **maximal**, and if it is both total and surjective, we call it **full**. If $\approx$ is full, we call $\mathcal{M}$ and $\mathcal{N}$ **isomorphic**. As a convention, we let x, y, z range over the sets in $\mathcal{M}$ and a, b, c range over the sets in $\mathcal{N}$ for the remainder of this section.

Definition 28 *We define an inductive predicate* $\approx\colon \mathcal{M} \to \mathcal{N} \to \mathsf{Prop}$ *by*

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

We call the left defining condition ***(bounded) totality*** *on* x *and* a*, denoted by* $x \triangleright a$*. The right condition is called* ***(bounded) surjectivity*** *on* x *and* a*, denoted by* $x \triangleleft a$*. We call* $\approx$ ***membership-bisimilarity*** *and if* $x \approx a$ *we call* x *and* a ***bisimilar****.*

The following lemma captures the symmetry present in the definition:

Lemma 29 $x \approx a$ *iff* $a \approx x$ *and* $x \triangleright a$ *iff* $a \triangleleft x$*.*

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 $a \triangleright x$. So for $b \in a$ we have to find $y \in x$ with $b \approx y$. By $x \triangleleft a$ we already know there is $y \in x$ with $y \approx b$. Then the inductive hypothesis implies $b \approx y$ as wished. That $x \triangleright a$ 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 30 *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 $x \triangleleft a$ there must be $y \in x$ with $y \approx b$. Moreover, since $x \triangleright a'$ 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 $x' \triangleright a'$ there is $b \in a'$ with $x \approx b$. Hence $a = b$ by functionality of $\approx$ and thus $a \in a'$. □

This justifies calling $\mathcal{M}$ and $\mathcal{N}$ isomorphic if $\approx$ is full. Since all set operations are uniquely determined by their membership laws, they are also respected by $\approx$.

Fact 31 $\emptyset \approx \emptyset$

Proof Both $\emptyset \triangleright \emptyset$ and $\emptyset \triangleleft \emptyset$ hold vacuously. □

Lemma 32 *If* $x \approx a$*, then* $\bigcup x \approx \bigcup a$

Proof By symmetry (Lemma 29) we just have to prove $\bigcup x \triangleright \bigcup a$. So suppose $y \in \bigcup x$, so $y \in z \in x$. By $x \triangleright a$ we have $c \in a$ with $z \approx c$ and applying $z \triangleright c$ we have $b \in c$ with $y \approx b$. So $c \in b \in a$ and thus $b \in \bigcup a$. □

Lemma 33 *If* $x \approx a$*, then* $\mathcal{P}x \approx \mathcal{P}a$

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

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

Definition 34 *For $R : \mathcal{M} \to \mathcal{M} \to \mathsf{Prop}$ we define $\overline{R} : \mathcal{N} \to \mathcal{N} \to \mathsf{Prop}$ by*

$$\overline{R}\,a\,b \coloneqq \exists xy.\, x \approx a \wedge y \approx b \wedge R\,x\,y$$

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

Lemma 35 *If $x \approx a$, $R \in \mathcal{F}(\mathcal{M})$, and $R@x \subseteq \mathsf{dom}(\approx)$, then $R@x \approx \overline{R}@a$.*

Proof We first show that $R@x \triangleright \overline{R}@a$, 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 $\overline{R}\,c\,b$. Now by $y \in R@x$ there is $z \in x$ with $R\,z\,y$. Hence there is $c \in a$ with $z \approx c$ since $x \triangleright a$. This implies $\overline{R}\,c\,b$.

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

Note that these properties immediately imply the following:

Lemma 36 $\mathsf{dom}(\approx)$ *is ZF-closed.*

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 remaining closure properties left by Fact 10 were established in the previous lemmas. □

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

Lemma 37 *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 33 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 33 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 32 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 induction hypothesis for y to establish that c is a stage. □

Lemma 38 *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 32 it follows that $\bigcup b \in a$. The proof for power is completely analogous and for relational replacement one first mechanically verifies that $\overline{R}@y \subseteq x$ for every functional relation $R \in \mathcal{F}(\mathcal{N})$ with $R@b \subseteq a$. □

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

Lemma 39 *Either* $\mathcal{V}_{\mathcal{M}} \subseteq \mathsf{dom}(\approx)$ *or* $\mathcal{V}_{\mathcal{N}} \subseteq \mathsf{ran}(\approx)$.

Proof Suppose there were stages $x \notin \mathsf{dom}(\approx)$ and $a \notin \mathsf{ran}(\approx)$, then we can in particular assume x and a to be the least such stages by Lemma 18. 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 33.

In the case $\bigcup x$ for a set of stages x we may assume that $x \subseteq \bigcup x$ by Fact 23. Now suppose $y \in z \in x$, then we want to find $b \in W$ with $y \approx b$. We distinguish the cases 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 37. 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 40 *Bisimilarity* $\approx$ *is maximal.*

Proof Suppose $\approx$ were neither total nor surjective, so there were $x \notin \mathsf{dom}(\approx)$ and $a \notin \mathsf{ran}(\approx)$. By Fact 21 we know that $x \in \mathcal{P}(\rho x)$ and $a \in \mathcal{P}(\rho a)$. Then by Lemma 39 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 already conclude that embeddability is a linear preorder on models of **ZF**. We can further strengthen the result by proving one side of $\approx$ small if $\mathcal{M}$ and $\mathcal{N}$ are not already isomorphic.

Lemma 41 *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 40. 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 $z \approx b$. Then Lemma 37 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 $\mathcal{N}$ and $\mathsf{ran}(\approx)$, hence we summarise:

Theorem 42 *Exactly one of the following statements holds:*
(1) $\approx$ *is full, so* $\mathcal{M}$ *and* $\mathcal{N}$ *are isomorphic.*
(2) $\approx$ *is surjective and* $\mathsf{dom}(\approx)$ *is a universe of* $\mathcal{M}$.
(3) $\approx$ *is total and* $\mathsf{ran}(\approx)$ *is a universe of* $\mathcal{N}$.

Proof Suppose $\approx$ were not full, then it is still maximal by Theorem 40. 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 41 we know $\mathsf{dom}(\approx) \subseteq x$, so the domain is realised by $\mathsf{dom}(\approx) \cap x$. This set is a universe by Lemma 36. □

Note that description turns the relation $\approx$ into an actual embedding i in the sense of Section 4.1 with direction depending on the outcome of Theorem 42.

3.2 Categoricity Results

Applying Zermelo's embedding theorem, we can now examine to what extent the model theory of **ZF** is determined and study categorical extensions. Formally, an axiomatisation is called **categorical** if $\mathcal{M} \approx \mathcal{N}$ for any two models $\mathcal{M}$ and $\mathcal{N}$. As a first result, we can prove **ZF** categorical in every cardinality:

Fact 43 *Equipotent models of* **ZF** *are isomorphic.*

Proof If models $\mathcal{M}$ and $\mathcal{N}$ are equipotent, we have a function $F : \mathcal{M} \to \mathcal{N}$ with inverse $G : \mathcal{N} \to \mathcal{M}$. Then from either of the cases (2) and (3) of Theorem 42 we can derive a contradiction. So for instance suppose $\approx$ is surjective and $X = \mathsf{dom}(\approx)$ is a universe of $\mathcal{M}$. We use a variant of Cantor's argument where G simulates the surjection of X onto the power set of X. Hence define $Y := \{\, x \in X \mid x \notin G(i\,x) \,\}$ 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 $y \notin G(i\,y) = G(i\,(i^{-1}\,(FY))) = G(F(Y)) = Y$, 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. In particular, it follows that the axiomatisations $\mathbf{ZF}_n$ are categorical. We hence may call the models of $\mathbf{ZF}_n$ unique, provided they exist.

Fact 44 $\mathbf{ZF}_n$ *is categorical for all* $n : \mathbb{N}$.

Proof Let $\mathcal{M}$ and $\mathcal{N}$ be models of $\mathbf{ZF}_n$. Again Theorem 42 admits three cases, whereof (1) yields the claim. Otherwise, if (2) holds, then $\mathsf{ran}(\approx) : \mathcal{N}$ is a universe. Since $\mathcal{M}$ has strength n by assumption, it follows that $\mathsf{ran}(\approx)$ has strength n and thus that $\mathcal{N}$ has strength $n + 1$, contradicting $\mathcal{N} \models \mathbf{ZF}_n$. The case (3) is symmetric. □

As a consequences of categoricity, all properties expressible in set-theoretic language are evaluated equally in any two models of $\mathbf{ZF}_n$. For instance, if one model of $\mathbf{ZF}_n$ satisfies the axiom of choice, any other model does as well. Consider the following natural definition of global choice in dependent type theory:

Definition 45 *We say that a type A is a* ***choice type*** *if there is a function c of type* $\forall(P : A \to \mathsf{Prop}).\,(\exists a : A.\, a \in P) \to \langle a : A \mid a \in P \rangle$.

First of all, categoricity implies that global choice is not independent from $\mathbf{ZF}_n$.

Fact 46 *If $\mathcal{M}$ and $\mathcal{N}$ are models of $\mathbf{ZF}_n$, then $\mathcal{M}$ is a choice type iff $\mathcal{N}$ is.*

Proof By symmetry we just have to show one direction, so suppose there is a choice function $c_{\mathcal{M}}$ for $\mathcal{M}$. In order to construct a choice function for $\mathcal{N}$, we assume a propositionally inhabited class P on $\mathcal{N}$. Since $\mathcal{M}$ and $\mathcal{N}$ are isomorphic by Fact 44, we know that i is a bijection. So $c_{\mathcal{M}}$ applies to the class $P \circ i$ over $\mathcal{M}$, where we know that $P \circ i$ is propositionally inhabited since P is. Hence $c_{\mathcal{M}}$ yields a witness x for $P \circ i$ which is turned into a witness $i\,x$ for P. □

We can further compare this type-theoretic version of choice to an internal set-theoretic version. The following introduces one of the many equivalent formulations of the axiom of choice.

Definition 47 *Let $\mathcal{M}$ be a set structure. A set X is called a* ***partition*** *if the elements of X are non-empty and pairwise disjoint. A set Y is called a* ***trace*** *of a partition X if for every element $x \in X$ there is a unique $y \in Y$ with $y \in x$. We say $\mathcal{M}$ satisfies the axiom of choice (*AC*) if every partition has a trace.*

By the expressive strength of second-order ZF, type-theoretic choice always implies set-theoretic choice and AC is not independent from $\mathbf{ZF}_n$.

Fact 48 *If $\mathcal{M}$ is a model of* $\mathbf{ZF}$ *and a choice type, then $\mathcal{M}$ satisfies* AC.

Proof Let c be the choice function for $\mathcal{M}$ and X be a partition. For simplicity, for $x \in X$ we write $c\,x$ for the application of c to the proof that x is not empty. Now set $Y \coloneqq (\lambda y.\, \exists x \in X.\, y = c\,x) \cap (\bigcup X)$. Then for $x \in X$ we have that $c\,x \in Y$ is unique with $c\,x \in x$, so Y is a trace of X. □

Fact 49 *If $\mathcal{M}$ and $\mathcal{N}$ are models of $\mathbf{ZF}_n$, then $\mathcal{M}$ satisfies* AC *iff $\mathcal{N}$ does.*

Proof Again, by symmetry one direction suffices. So assume $\mathcal{M}$ satisfies AC and let X' be a partition in $\mathcal{N}$. Since $\mathcal{M}$ and $\mathcal{N}$ are isomorphic by Fact 44, we can set $X \coloneqq i^{-1}\,X'$. It follows that X is a partition as well and so there is a trace Y for X by AC for $\mathcal{M}$. Using i again, we obtain the trace $Y' \coloneqq i\,Y$ of X'. □

We remark that the idea of controlling the number of universes underlying $\mathbf{ZF}_n$ can be extended to transfinite ordinalities by asserting that the class of universes is oder-isomorphic to some given well-order.

4 Model Constructions

So far we have developed the theory of second-order ZF simply assuming various models and studying their internal and external properties. In the remainder of this paper, we discuss under which conditions such models exist. Specifically, we show that $\mathbf{ZF}_{\geq n}$ has a model for all numbers n if we assume a proof-irrelevant description operator for the inductive type of well-founded trees, and that $\mathbf{ZF}_n$ has a unique model for all n if we further assume excluded middle. Up to the conclusive remark concerning the models of $\mathbf{ZF}_n$ in Section 4.5, XM will not be used.

4.1 Intensional Axiomatisation and Embeddings

Given that Coq's type theory is intensional and constructive, we cannot expect to freely obtain extensional models of full $\mathbf{ZF}$. Hence we first consider some weakened versions of structures and axiomatisations, which have models without additional assumptions.

Definition 50 ***ZF′-structures*** *are ZF-structures without a constant for description.*

Definition 51 *Let $\mathcal{M}$ be a set structure. We define the relation $x \equiv y \coloneqq x \subseteq y \wedge y \subseteq x$ called* ***set equivalence*** *with equivalence classes $[x] \coloneqq \lambda y.\, y \equiv x$. Further, we say that classes P and functions F over $\mathcal{M}$* ***respect*** *$\equiv$, if*
(1) $\forall x, x'.\, x \equiv x' \to x \in P \to x' \in P$ and
(2) $\forall x, x'.\, x \equiv x' \to F\,x \equiv F\,x'$.
For these properties we write $P : \mathcal{M} \overset{\equiv}{\to} \mathsf{Prop}$ and $F : \mathcal{M} \overset{\equiv}{\to} \mathcal{M}$.

Definition 52 *A ZF-structure $\mathcal{M}$ is an **intensional model** if the following hold:*

Morph :	$x \equiv x' \to x \in y \to x' \in y$	
Found :	$x \in WF$	
Inf :	$\exists \omega.\, \forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x \equiv \mathcal{P}^n\, \emptyset$	
Eset :	$x \notin \emptyset$	
Pair :	$z \in \{x, y\} \leftrightarrow z \equiv x \vee z \equiv y$	
Union :	$z \in \bigcup x \leftrightarrow \exists y \in x.\, z \in y$	
Power :	$y \in \mathcal{P} x \leftrightarrow y \subseteq x$	
Sep :	$y \in P \cap x \leftrightarrow y \in x \wedge y \in P$	$(P : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop})$
Frep :	$z \in F @ x \leftrightarrow \exists y \in x.\, z \equiv F\, y$	$(F : \mathcal{M} \xrightarrow{\equiv} \mathcal{M})$
Desc_1 :	$(\exists x\, \forall y.\, y \in P \leftrightarrow y \in [x]) \to \delta P \in P$	$(P : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop})$
Desc_2 :	$(\forall x.\, x \in P \leftrightarrow x \in P') \to \delta P = \delta P'$	$(P, P' : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop})$

We denote the class of ZF-structures satisfying these axioms by $\mathbf{ZF}_\equiv$. Further, $\mathbf{ZF}'_\equiv$ denotes the class of ZF′-structures satisfying all axioms of $\mathbf{ZF}_\equiv$ but Desc_1 and Desc_2.

Note that $\mathbf{ZF}_\equiv$ essentially expresses **ZF** with equalities replaced by equivalences and with extensionality substituted by asserting membership to be a morphism for equivalence. Furthermore, the higher-order membership laws have additional side conditions requiring the argument classes and functions to respect equivalence. Description is strengthened to providing witnesses for equivalence classes. In total, extending $\mathbf{ZF}_\equiv$ by Ext is exactly equivalent to **ZF**.

One recurring pattern in the remainder of this paper is the situation where we have one model embedded into another, witnessed by a $\in$-preserving injection. For such embeddings, both models agree on the notion of universes and strength of corresponding sets. Let $\mathcal{M}$ and $\mathcal{N}$ be models of $\mathbf{ZF}_\equiv$.

Definition 53 *$h : \mathcal{M} \to \mathcal{N}$ is called an **embedding** if*
(1) $x \in y \leftrightarrow h\, x \in h\, y$ and
(2) for all $x' \in h\, y$ there is $x \in y$ with $h\, x \equiv x'$.
*We define the **image** of a class P by $h[P] \coloneqq \lambda x'.\, \exists x.\, h\, x \equiv x' \wedge x \in P$.*

We now further assume such an embedding h.

Fact 54 *P is ZF-closed iff $h[P]$ is ZF-closed.*

Proof Clearly h respects all set operations since these are uniquely specified by their membership laws. This implies properties like $h\, \emptyset = \emptyset$, $h\, (\bigcup x) = \bigcup (h\, x)$, etc., ultimately transporting all structure from a ZF-closed class P to $h[P]$ and back. Also note the similarity to Lemma 38. □

Corollary 55 *U is a universe iff $h\, U$ is a universe.*

Proof Follows since $h[U]$ agrees with $h\, U$. □

Fact 56 *x has strength n iff $h\, x$ has strength n.*

Proof By induction on n. The case of $n = 0$ is trivial, so suppose x has strength $n+1$. Then there is a universe $U \in x$ of strength n. By the inductive hypothesis we know that $h\,U$ has strength n and by $h\,U \in h\,x$ we conclude that $h\,x$ has strength $n+1$. The converse direction is analogous. □

See the Coq development and [12] for a fully-detailed proof of the above facts.

4.2 Aczel's Intensional Model

The dependent type theory underlying Coq comes with a countably infinite hierarchy of type levels Type_i. From now on, we make the universe levels explicit where necessary and admit definitions that are polymorphic for all type levels, as implemented in Coq [21]. Our main instance of a universe-polymorphic definition is the following:

Definition 57 *We define the universe-polymorphic family of inductive types $\mathcal{T}_i : \mathsf{Type}_i$ of **well-founded trees** with a term constructor $\tau : \forall(A : \mathsf{Type}_j).\,(A \to \mathcal{T}_i) \to \mathcal{T}_i$ for $j < i$. We define projections $p_1(\tau\,A\,f) := A$ and $p_2(\tau\,A\,f) := f$.*

Following Aczel [1], we interpret the trees in $\mathcal{T}_i$ as sets, where the direct subtrees $f\,a$ of trees $\tau\,A\,f$ correspond to the elements of sets. However, since intensionally distinct types and functions can yield bisimilar trees, one first has to impose a notion of tree equivalence and then to define a respectively generalised version of membership.

Definition 58 ***Equivalence*** $\equiv_{\mathcal{T}_i} : \mathcal{T}_i \to \mathcal{T}_i \to \mathsf{Prop}$ *of trees is defined by*

$$\frac{\forall a : A\,\exists b : B.\,f\,a \equiv_{\mathcal{T}_i} g\,b \qquad \forall b : B\,\exists a : A.\,f\,a \equiv_{\mathcal{T}_i} g\,b}{\tau\,A\,f \equiv_{\mathcal{T}_i} \tau\,B\,g}$$

Membership *is defined by $s \in \tau\,A\,f := \exists a.\,s \equiv_{\mathcal{T}_i} f\,a$, making $\mathcal{T}_i$ a set structure.*

Fact 59 *$\equiv_{\mathcal{T}_i}$ is an equivalence and respected by $\in$.*

Proof Reflexivity, symmetry and transitivity of $\equiv_{\mathcal{T}_i}$ all follow by structural induction on $\mathcal{T}_i$. Now let $s \equiv_{\mathcal{T}_i} s'$, $t \equiv_{\mathcal{T}_i} t'$ and $s \in t$. By definition of $s \in t$ we have $a : p_1\,t$ with $s \equiv_{\mathcal{T}_i} p_2\,t\,a$. Now since $t \equiv_{\mathcal{T}_i} t'$ we obtain $a' : p_1\,t'$ with $p_2\,t\,a \equiv_{\mathcal{T}_i} p_2\,t'\,a'$. Then by transitivity $s' \equiv_{\mathcal{T}_i} p_2\,t'\,a'$ and so $s' \in t'$. It follows that inclusion respects $\equiv_{\mathcal{T}_i}$ as well. □

Before we implement the set operations for trees we need to justify the reuse of the notation $\equiv$. In fact, tree equivalence agrees with the abstract notion of set equivalence (Definition 51), so we can use the relations interchangeably.

Fact 60 $s \equiv t \leftrightarrow s \equiv_{\mathcal{T}_i} t$

Proof For the first direction we assume $\tau\,A\,f \equiv \tau\,B\,g$, so $\tau\,A\,f \subseteq \tau\,B\,g$ and $\tau\,B\,g \subseteq \tau\,A\,f$. Then $\tau\,A\,f \equiv_{\mathcal{T}_i} \tau\,B\,g$ follows since, showing one half of the definition, for $a : A$ we know $f\,a \in \tau\,A\,f$ and hence obtain $b : B$ with $f\,a \equiv_{\mathcal{T}_i} g\,b$ from $\tau\,A\,f \subseteq \tau\,B\,g$. The converse direction follows since $s \equiv_{\mathcal{T}_i} t$ implies $s \subseteq t$ using Fact 59. □

All set operations of ZF but description have counterparts in constructive type theory: the empty set in the empty type $\bot$, pairing in booleans $\mathbb{B}$ and conditionals, union in tree concatenation, power sets in predicate types, separation in refinement types, and replacement in function composition. Along those lines, one can define the set operations for trees as follows:

Definition 61 *We turn $\mathcal{T}_i$ into a ZF′-structure by defining*

$$\begin{aligned}
\emptyset &:= \tau \bot \mathrm{elim}_\bot \\
\{s,t\} &:= \tau\, \mathbb{B}\, (\lambda b.\, \text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau\, A\, f) &:= \tau\, (\Sigma a : A.\, p_1(f\, a))\, (\lambda(a,b).\, p_2(f\, a)\, b) \\
\mathcal{P}(\tau\, A\, f) &:= \tau\, (A \to \mathsf{Prop})\, (\lambda P.\, \tau\, \langle a : A \mid a \in P\rangle\, (f \circ \pi_1)) \\
P \cap (\tau\, A\, f) &:= \tau\, \langle a : A \mid (f\, a) \in P\rangle\, (f \circ \pi_1) \\
F@(\tau\, A\, f) &:= \tau\, A\, (\lambda a.\, F\, (f\, a))
\end{aligned}$$

Then $\mathcal{T}_i$ satisfies all intensional ZF axioms but Desc.

Theorem 62 $\mathcal{T}_i \models \mathbf{ZF}'_\equiv$

Proof Morph was already shown in Fact 59. Concerning Found, we show $\tau\, A\, f \in WF$ by structural induction on $\mathcal{T}_i$. By the inductive hypothesis we know $f\, a \in WF$ for all $a : A$ and conclude $s \in WF$ for all $s \in \tau\, A\, f$ by the fact that WF respects $\equiv$.

The membership axioms are fairly routine and we refer to the Coq development for full detail. As instances, we justify Eset and Pair. For the former, we have to show $s \notin \emptyset$ for all $s : \mathcal{T}_i$. This is the case, since the definition of $s \in \emptyset$ carries an inhabitant of $\bot$.

Now for the latter let $s, t : \mathcal{T}_i$ and $u \in \{s,t\}$. Hence there is $b : \mathbb{B}$ with $u \equiv$ (if b then s else t) and by a boolean case analysis we obtain either $u \equiv s$ or $u \equiv t$. Now conversely, suppose we start with either $u \equiv s$ or $u \equiv t$. To show $u \in \{s,t\}$ we have to give a matching $b : \mathbb{B}$ and obviously, depending on the case concerning u, we just pick the respectively correct boolean value.

Finally concerning Inf, we set $\omega_{\mathcal{T}_i} := \tau\, \mathbb{N}\, (\lambda n.\, \mathcal{P}^n\, \emptyset)$. The assertion that $\omega_{\mathcal{T}_i}$ agrees with $\lambda x.\, \exists n : \mathbb{N}.\, x \equiv \mathcal{P}^n\, \emptyset$ is straight-forward. □

4.3 An Extensional Model

In general, the intensional type theory of Coq does not provide quotient types. As a remedy, we assume further logical axioms in order to construct extensional models based on the tree model $\mathcal{T}_i$. In this paper, we only employ a description operator for trees. See the discussion in Section 5, the Coq development, and previous work [12] for other approaches.

Axiom (TD) We assume a function $\delta : (\mathcal{T}_i \to \mathsf{Prop}) \to \mathcal{T}_i$ satisfying Desc_1 and Desc_2.

First note that this assumption makes $\mathcal{T}_i$ a full ZF-structure satisfying $\mathbf{ZF}_\equiv$.

Fact 63 $\mathcal{T}_i \models \mathbf{ZF}_\equiv$

Proof Follows from Theorem 62 and TD. □

Seen as a quotient axiom, TD yields a normaliser for tree equivalence classes.

Definition 64 $\gamma s \coloneqq \delta[s]$

Fact 65 *The following properties of γ hold:*

(1) $\gamma s \equiv s$ (3) $\gamma(\gamma s) = \gamma s$

(2) $s \equiv t \to \gamma s = \gamma t$ (4) $\gamma s = \gamma t \to s \equiv t$

Proof Properties (1) and (2) express Desc_1 and Desc_2, respectively. Idempotency (3) follows from applying (2) to (1) and if $\gamma s = \gamma t$ we have $s \equiv \gamma s = \gamma t \equiv t$. □

The representatives picked by γ then yield an extensional model.

Definition 66 *We define $\mathcal{S}_i$ to be the type $\langle s : \mathcal{T}_i \mid \gamma s = s\rangle$ of **canonical representatives**. We write $\overline{s}$ for the elements in $\mathcal{S}_i$ where $s \in \mathcal{T}_i$ and by idempotency we can judge $\gamma s : \mathcal{S}_i$ for every $s : \mathcal{T}_i$. Membership is inherited from $\mathcal{T}_i$, i.e. $\overline{s} \in \overline{t} \coloneqq s \in t$.*

Definition 67 *We turn $\mathcal{S}_i$ into a ZF-structure by setting*

$$\begin{aligned} \emptyset_{\mathcal{S}_i} &\coloneqq \gamma\emptyset & P \cap \overline{s} &\coloneqq \gamma((P \circ \gamma) \cap s)\\ \{\overline{s}, \overline{t}\} &\coloneqq \gamma(\{s, t\}) & F@\overline{s} &\coloneqq \gamma((F \circ \gamma)@s)\\ \bigcup \overline{s} &\coloneqq \gamma(\bigcup s) & \delta_{\mathcal{S}_i} P &\coloneqq \gamma(\delta(P \circ \gamma))\\ \mathcal{P}\overline{s} &\coloneqq \gamma(\mathcal{P}s) \end{aligned}$$

To make the quotient construction work properly we further have to assume the proofs of identities $\gamma s = s$ to be unique.

Axiom (PI_γ) $\forall(s : \mathcal{T}_i)\,(H, H' : \gamma s = s).\, H = H'$

Then the type $\mathcal{S}_i$ satisfies all axioms of extensional ZF.

Theorem 68 $\mathcal{S}_i \models \mathbf{ZF}$

Proof We first establish Ext, so assume $\overline{s} \subseteq \overline{t}$ and $\overline{t} \subseteq \overline{s}$. Then $s \subseteq t$ and $t \subseteq s$ and thus $s \equiv t$. Since $s = \gamma s$ and $t = \gamma t$ we obtain $s = t$. Hence the first components of $\overline{s}$ and $\overline{t}$ agree. Applying PI_γ yields equality of the second components so we conclude that $\overline{s} = \overline{t}$.

Morph holds trivially and Found as well as Desc follow directly from the corresponding axioms of $\mathcal{T}_i$. Furthermore, Inf is witnessed by $\gamma\omega_{\mathcal{T}_i}$.

Regarding the membership axioms, this time we discuss Sep and Frep. So let $\overline{t} \in P \cap \overline{s}$, we have to show $\overline{t} \in \overline{s}$ and $\overline{t} \in P$. By the definition of membership and separation on $\mathcal{S}_i$ we know that $t \in (P \circ \gamma) \cap s$. Note that $P \circ \gamma$ respects $\equiv$ since if $s \equiv t$ we know that $\gamma s = \gamma t$ and hence that $\gamma s \in P$ trivially implies $\gamma t \in P$. Thus Sep for $\mathcal{T}_i$ yields $t \in s$ and $\gamma t \in P$ which implies $\overline{t} \in \overline{s}$ and $\overline{t} \in P$ as wished. The converse is similar.

Now we assume $\overline{u} \in F@\overline{s}$ and want to find some $\overline{t} \in \overline{s}$ with $\overline{u} = F\,\overline{t}$. By plugging in the definitions, we obtain that $u \in (F \circ \gamma)@s$. Now $F \circ \gamma$ respects $\equiv$ for similar reasons as $P \circ \gamma$ did, so Frep for $\mathcal{T}_i$ applies. This yields $t \in s$ with $u \equiv F\,(\gamma t)$ and we may conclude $\overline{t} \in \overline{s}$ as well as $\overline{u} = F\,\overline{t}$. Again, the converse is similar. □

The following establishes that the intensional model $\mathcal{T}_i$ and the extensional model $\mathcal{S}_i$ agree on universes and strength:

Fact 69 *γ seen as a function $\gamma : \mathcal{T}_i \to \mathcal{S}_i$ is an embedding.*

Proof Both conditions are immediate by the definition of $\mathcal{S}_i$. □

4.4 Large Models

Coq's type theory with countably many type levels admits the construction of large models of **ZF**. Intuitively, the type levels correspond to set universes and indeed, for every number n, the model $\mathcal{S}_i$ at a universe level high enough satisfies $\mathbf{ZF}_{\geq n}$. Thereby the strength of $\mathcal{S}_i$ at a high level is witnessed by recursively embedding $\mathcal{S}_j$ at lower levels $j < i$. In fact, every intensional model embeds into some $\mathcal{S}_i$ by $\in$-recursion. Note that we still assume TD and PI_γ.

Definition 70 *For an intensional model $\mathcal{M} \models \mathbf{ZF}_\equiv$ we define a function $\iota : \mathcal{M} \to \mathcal{T}_i$*

$$\iota\, x \coloneqq \tau\, \langle y : \mathcal{M} \mid y \in x \rangle\, (\iota \circ \pi_1)$$

by $\in$-recursion and set $U_\mathcal{M} \coloneqq \tau\, \mathcal{M}\, \iota$. This assumes $\mathcal{M} : \mathsf{Type}_j$ for $j < i$.

Lemma 71 *ι respects equivalence and membership, that is:*

$$\text{(1) } x \equiv y \leftrightarrow \iota\, x \equiv \iota\, y \qquad \text{(2) } x \in y \leftrightarrow \iota\, x \in \iota\, y$$

Proof (1) Suppose $x \equiv y$. We have to show that for every $z \in x$ there is $z' \in y$ with $\iota\, z \equiv \iota\, z'$ and vice versa. So let $z \in x$, hence by the assumption $x \equiv y$ we know $z \in y$ and by reflexivity of $\equiv$ we know $\iota\, z \equiv \iota\, z$.

The converse is by $\in$-induction on x for all y. We assume $\iota\, x \equiv \iota\, y$ and have to show $x \subseteq y$ and $y \subseteq x$. We just show $x \subseteq y$ since both cases are similar, so let $z \in x$. By $\iota\, x \equiv \iota\, y$ there is $z' \in y$ with $\iota\, z \equiv \iota\, z'$. Then the inductive hypothesis yields $z \equiv z'$ and thus we conclude $z \in y$.

(2) The direction from left to right is immediate by definition. For the converse suppose $\iota\, x \in \iota\, y$, so there is $z \in y$ with $\iota\, x \equiv \iota\, z$. Then by (1) we know $x \equiv z$ and thus $x \in y$. □

Lemma 72 *ι is an embedding.*

Proof The first condition was shown in Lemma 71 and the second condition is straightforward by definition. □

Lemma 73 *If $\mathcal{M} \models \mathbf{ZF}_\equiv$ then $U_\mathcal{M}$ is a universe.*

Proof By definition $U_\mathcal{M}$ agrees with $\iota\, [\lambda\_.\, \top]$ and is ZF-closed by Fact 54. □

Furthermore the strength of $\mathcal{M}$ is reflected by $U_\mathcal{M}$:

Lemma 74 *If $\mathcal{M} \models \mathbf{ZF}_{\geq n}$ then $U_\mathcal{M}$ has strength n.*

Proof If $\mathcal{M} \models \mathbf{ZF}_{\geq n}$ there is $x \in \mathcal{M}$ with strength n. Then $\iota\, x \in U_\mathcal{M}$ has the same strength by Fact 56 and Lemma 72. Hence, being transitive, $U_\mathcal{M}$ has the same strength. □

Fact 75 *If $\mathbf{ZF}_{\geq n}$ has a model, then $\mathbf{ZF}_{\geq n+1}$ has a model.*

Proof Let $\mathcal{M} \models \mathbf{ZF}_{\geq n}$ with $\mathcal{M} : \mathsf{Type}_i$. Then by Lemma 74 we know that $\gamma\, U_\mathcal{M} : \mathcal{S}_{i+1}$ has strength n and hence $\mathcal{P}(\gamma\, U_\mathcal{M})$ has strength $n+1$. Thus $\mathcal{S}_{i+1}$ is a model of $\mathbf{ZF}_{\geq n+1}$ □

Therefore we can conclude the following outside of Coq:

Metatheorem 76 *For every number n, $\mathbf{ZF}_{\geq n}$ has a model.*

Proof We construct the large models by iterating Fact 75. First, by Theorem 68 we know that in particular $\mathcal{S}_i \models \mathbf{ZF}_{\geq 0}$. For the inductive step suppose we have a model $\mathcal{M} \models \mathbf{ZF}_{\geq n}$. Then Fact 75 yields a model of $\mathbf{ZF}_{\geq n+1}$. □

This metatheorem has no formal counterpart in Coq as the type levels of the models of $\mathbf{ZF}_{\geq n}$ depend on n. Coq's syntax only admits instances $\exists \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_{\geq k}$ or a statement like

$$\forall n : \mathbb{N}\, \exists \mathcal{M} : \mathsf{Type}_i.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}$$

for some fixed type level Type_i. However, this statement is not an inductive consequence of Fact 75 as in the inductive step we assume a model $\mathcal{M} : \mathsf{Type}_i$ of $\mathbf{ZF}_{\geq n}$ but only know that $\mathcal{S}_{i+1} \models \mathbf{ZF}_{\geq n+1}$ where $\mathcal{S}_{i+1} : \mathsf{Type}_{i+1}$. In fact, if the statement would be provable, it would induce the existence of a model of $\mathbf{ZF}_{\geq \omega}$ which lies beyond the consistency strength of a type theory with only countably many type levels [2,27]:

Fact 77 $(\forall n : \mathbb{N}\, \exists \mathcal{M} : \mathsf{Type}_i.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}) \to \mathcal{S}_{i+1} \models \mathbf{ZF}_{\geq \omega}$

Proof We have to show that $\mathcal{S}_{i+1}$ contains sets of every finite strength. So let $n : \mathbb{N}$, then given the assumption there is a model $\mathcal{M} : \mathsf{Type}_i$ such that $\mathcal{M} \models \mathbf{ZF}_{\geq n}$. Thus by Fact 75 we know that $\gamma U_{\mathcal{M}} : \mathcal{S}_{i+1}$ has strength n. □

4.5 Model Truncation

We finally study a truncation method for pruning models of $\mathbf{ZF}_{\geq n}$ to models of $\mathbf{ZF}_n$. Together with the previous model construction for $\mathbf{ZF}_{\geq n}$ (Metatheorem 76) and the categoricity of $\mathbf{ZF}_n$ (Fact 44) this implies that $\mathbf{ZF}_n$ has a unique model for all natural numbers n. We now assume XM again.

Lemma 78 *If $\mathcal{M} \models \overline{\mathbf{ZF}}$ and U is ZF-closed, then $\mathcal{M}_U \coloneqq \langle x : \mathcal{M} \mid x \in U \rangle$ with the accordingly restricted set operations is a model of $\overline{\mathbf{ZF}}$ as in Definition 3.*

Proof Since U is ZF-closed, the restrictions of the set operations of $\mathcal{M}$ to $\mathcal{M}_U$ are well-defined. For separation and replacement the argument classes $P : \mathcal{M}_U \to \mathsf{Prop}$ and functions $F : \mathcal{M}_U \to \mathcal{M}_U$ are translated to

$$P' \coloneqq \lambda x.\, x \in U \wedge \overline{x} \in P$$
$$F' \coloneqq \lambda x.\, \delta(\lambda y.\, x \in U \wedge y \in U \wedge \overline{y} = F\, \overline{x})$$

operating on $\mathcal{M}$, where we write $\overline{x}$ for the elements of $\mathcal{M}_U$ with $x : \mathcal{M}$ and $x \in U$. The description operator of $\mathcal{M}_U$ is

$$\delta_U\, P \coloneqq (\lambda \_.\, \exists! x.\, x \in P) \cap \delta P'$$

where the separation ensures that $\delta_U\, P = \emptyset \in U$ in the case where δ is not well-defined.

Concerning the axioms, Ext relies on PI (Fact 11) since the members of $\mathcal{M}_U$ carry proofs as second component. Found follows from $U \subseteq \mathcal{M} \subseteq WF$ and the membership axioms hold in $\mathcal{M}_U$ as they do in $\mathcal{M}$. □

The following ensures that universes and strength are preserved in submodels:

Lemma 79 *If $\mathcal{M} \models \overline{\mathbf{ZF}}$ and U is ZF-closed, then $\pi_1 : \mathcal{M}_U \to \mathcal{M}$ is an embedding.*

Proof π_1 respects membership by definition of $\mathcal{M}_U$. Further, if $x \in \pi_1\, \overline{y} = y$ for $\overline{y} : \mathcal{M}_U$ we have $x \in U$ by transitivity of U and $x \in y$. Then $\overline{x} : \mathcal{M}_U$ satisfies $\overline{x} \in \overline{y}$ and $\pi_1\, \overline{x} = x$. □

Fact 80 *If $\mathbf{ZF}_{\geq n}$ has a model, then $\mathbf{ZF}_n$ has a model.*

Proof Let $\mathcal{M}$ be a model of $\mathbf{ZF}_{\geq n}$, so there is $x : \mathcal{M}$ with strength n. We use XM to analyse whether there is $x' : \mathcal{M}$ with strength $n+1$. If not, then $\mathcal{M}$ is already a model of $\mathbf{ZF}_n$ by definition. So suppose there is such x', then we know there is a universe $U \in x'$ with strength n. Then because of the well-ordering of stages, we can assume U to be the least universe of strength n.

We show that $\mathcal{M}_U \models \mathbf{ZF}_n$. By Lemma 78 we know that $\mathcal{M}_U$ is a model of $\overline{\mathbf{ZF}}$. Further, $\mathcal{M}_U$ has strength n since U does, so $\mathcal{M}_U \models \mathbf{ZF}_{\geq n}$. Finally, suppose there were a set $x' \in \mathcal{M}_U$ with strength $n+1$ and hence a universe $U' \in x'$ with strength n. Then by transitivity of U it follows that $U' \in U$, contradicting the assumption that U is the least universe of strength n. Thus $\mathcal{M}_U \models \mathbf{ZF}_n$. □

Metatheorem 81 *For every number n, $\mathbf{ZF}_n$ has a unique model.*

Proof Fix a number n. By Metatheorem 76 we have a model of $\mathbf{ZF}_{\geq n}$. Applying Fact 80 yields a model of $\mathbf{ZF}_n$ and Fact 44 implies uniqueness (up to isomorphism). □

5 Discussion

In this paper, we have formalised the quasi-categoricity of second-order ZF first established by Zermelo [30] in Coq's type theory assuming excluded middle (XM). As a consequence, we have illustrated that axiomatisations controlling the ordinality of the class of Grothendieck universes such as $\mathbf{ZF}_n$ are categorical. Moreover, we have shown that further assuming a description operator on well-founded trees (TD) and local proof irrelevance (PI_γ) proves the systems $\mathbf{ZF}_n$ consistent. An overview of all main results and their underlying assumptions is given in Table 1.

Table 1 Overview of main results and axioms used.

Statement	Axioms	#
Well-ordering of the class $\mathcal{V}$ of stages	XM	16, 18
Every set appears in a stage	XM	21
Every universe appears as a stage	XM	27
Zermelo's embedding theorem	XM	42
Categoricity of $\mathbf{ZF}$ in every cardinality	XM	43
Categoricity of $\mathbf{ZF}_n$ for every n	XM	44
$\mathcal{T}_i \models \mathbf{ZF}'_{\equiv}$	–	62
$\mathcal{T}_i \models \mathbf{ZF}_{\equiv}$	TD	63
$\mathcal{S}_i \models \mathbf{ZF}$	TD, PI_γ	68
Consistency of $\mathbf{ZF}_{\geq n}$ for every n	TD, PI_γ	76
If $\mathbf{ZF}_{\geq n}$ has a model, then so does $\mathbf{ZF}_n$	XM	80
Consistency of $\mathbf{ZF}_n$ for every n	TD, XM	81

Type-theoretic approach to set theory. The formalisation of ZF in a type theory with inductive predicates as examined in this work differs from common textbook presentations (cf. [20,14,10]) in several ways, most importantly in the use of second-order axioms and the inductive definition of the cumulative hierarchy. We briefly outline some of the consequences.

Concerning the second-order version of the replacement axiom, it has been known since Zermelo [30] 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 the height of their cumulative hierarchy. Thus controlling these parameters induces categorical axiomatisations.

As a consequence of categoricity, all internal properties (including statements undecided in first-order ZF) become semantically determined in that there exist no two models such that a property holds in the first but fails in the second (cf. [13,26]). Concretely, Fact 49 shows that the set-theoretic axiom of choice (AC) either holds or fails in all models of $\mathbf{ZF}_n$. This is strikingly different from the undetermined situation in first-order ZF, where models can be arbitrarily incomparable and linearity of embeddability is only achieved in extremely controlled situations (cf. [9]). This is a consequence of the fact that inner models of second-order ZF are necessarily universes whereas those of first-order ZF can be subsets of strictly less structure. Moreover, since the type-theoretical version of choice as formulated in Definiction 45 is believed to be independent from Coq's type theory and violations of the set-theoretical AC induce violations on type level (Fact 48), we expect that the second-order models discussed in this paper do not invalidate the axiom of choice.

An explanation for those results is that the second-order separation axiom asserts the existence of all subsets of a given set contrarily to only the definable subsets guaranteed by a first-order scheme. This strength fully determines the extent of the power set, which remains underspecified in first-order ZF. Concretely, first-order ZF admits counterexamples to Lemma 33. Furthermore, the notions of external cardinality induced by type bijections and internal cardinality induced by bijections encodable as sets coincide in second-order ZF since every external bijection 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 [18]. 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 are provably uncountable (cf. [11]).

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 $V_\alpha \coloneqq \mathcal{P}^\alpha\,\emptyset$ using transfinite recursion on ordinals α. However, this presupposes at least a basic ordinal theory including the set-theoretic recursion theorem, making the cumulative hierarchy not immediately accessible. That this constitutes an unsatisfactory situation has been addressed by Scott [17] 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 the 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. Similarly, characterising the foundation axiom using an inductive predicate seems superior to a first-order statement in that it gives immediate access to $\in$-induction and $\in$-recursive definitions. Both were of substantial use throughout this paper.

Second-order set theory. Studying axiomatic systems in a formal meta theory with internalised logic such as dependent type theory offers two approaches. First, one can implement a full logical system based on an inductive object syntax and formalise the axioms as concrete formulas within this language. Using such a deep embedding is then complemented by a semantic interpretation of the domains, terms, and formulas of the logic as types, objects, and properties at the meta level. Analogously, if one considers a concrete deduction system for the object logic, proving soundness and, if attainable, completeness with respect to the chosen semantics basically establishes a connection of the object level deductions with the meta level deductions. These parallels suggest the second, more semantic, approach to formalising axiomatic systems: in a shallow embedding, formulas and in particular the axioms are stated directly in the meta logic and the affiliated meta deduction system is employed to explore the axiomatic consequences. This second approach is simpler but arguably not as obviously faithful to the theory under consideration as an explicit formalisation of syntax and deduction would be.

In this article, we present second-order set theory following the second approach. This is in alignment with the work by Aczel [1] and Werner [27], as both consider the second-order version of the axioms at type level. Of course, as the name suggests, second-order ZF is an axiom system normally cast in the considerably weaker second-order logic. In our presentation, however, we took the freedom to transcend the native expressibility of the second-order fragment of Coq's type theory by employing inductive definitions such as the inductive predicates WF and $\mathcal{V}$ or the inductive type $\mathbb{N}$ in order to illustrate some of the benefits of working in a rich type theory. Therefore calling the resulting system "higher-order ZF" or even "ZF in dependent type theory" could be reasonable options but these terms have their own drawbacks. Ultimately, since our main internal results are in principle expressible and provable for second-order logic we deem it appropriate to speak of second-order set theory as used in the literature.

Non-constructive assumptions. The use of excluded middle in the first two technical sections of our development has two main reasons. First, the standard results about the cumulative hierarchy as well as Zermelo's embedding theorem depend on classical reasoning and we see both as key results of an analysis of second-order ZF. One could of course invest more time into finding constructive renderings of these statements but our idea was to present a development of set theory close to the conservative classical formulation. Secondly, the truncation method (Fact 80) for shrinking a model of $\mathbf{ZF}_{\geq n}$ down to a model of $\mathbf{ZF}_n$ is inherently non-constructive as it yields the least universe of a given strength. Since one objective of this paper is to construct the unique models of the axiomatisations $\mathbf{ZF}_n$, we have to include these classical results. However, we emphasize that the consistency of the axiomatisations $\mathbf{ZF}_{\geq n}$ subject to the third technical section does not rely on excluded middle.

Since Coq does not provide built-in quotient types, constructing extensional models relies on additional axioms. Tree description (TD) yields a normaliser (Definition 64) for tree equivalence and therefore provides the necessary means to obtain the quotient models $\mathcal{S}_i$. Moreoever, relational replacement plays a crucial role in the development of ZF, e.g. it is needed to prove that the stages exhaust all sets (Fact 21). Speaking more generally, relational replacement is closer to first-order set theory than the functional version, as the formulas $\phi(a, b)$ in a first-order replacement scheme need not always be definable as type-level functions. So either relational replacement or functional replacement together with description ought to be included in a faithful axiomatisation of second-order ZF, both making tree description necessary for a model construction.

Further consistency results. We finish by discussing some related results from previous work [12]. As it was mentioned in Section 2.2, the system **ZF** is equivalent to $\mathbf{ZF}_{\geq 1}$ where the axiom of infinity is replaced by the assertion of at least one universe. For the more interesting direction from **ZF** to $\mathbf{ZF}_{\geq 1}$ we assume an infinite set ω, establish $\bigcup\omega$ as the set of hereditarily finite sets, and prove it to be the least universe. Note that this direction relies on XM whereas the direction from $\mathbf{ZF}_{\geq 1}$ to **ZF** does not. By the observed equivalence it is justified to see the variously strong assertions of universe existence as a generalised form of the infinity axiom.

In addition to the quotient construction via tree description presented in Section 4.3, in [12] we also explore alternative approaches using weaker assumptions. Solely postulating classes of trees to be extensional, i.e. assuming $P = Q$ whenever $P\,s \leftrightarrow Q\,s$ for all trees s, allows for lifting all set operations but replacement and description to the type $\langle P : \mathcal{T}_i \to \mathsf{Prop} \mid \exists s.\, P = [s]\rangle$ of tree equivalence classes. The so obtained model satisfies all axioms of the set theory **Z** which is **ZF** without replacement and description. Slighty stronger is the explicit assumption of a normaliser γ for trees, where the type $\langle s : \mathcal{T}_i \mid \gamma s = s\rangle$ of canonical representatives is at least a model of $\mathbf{ZF}'$. In general, it should be noted that the axioms needed in order to obtain full models of **ZF** really depend on the concrete type theory one is working in. For instance, in homotopy type theory [24], a system coming with higher inductive types and the strong extensionality principle of univalence, extensional models of (constructive) set theory do not rely on additional quotient axioms [15,5,8].

As elaborated before, an independence proof of AC cannot be given for second-order ZF. However, concerning the foundation axiom one can proceed in the usual manner, as we formalised in [12]. Starting with a non-well-founded model, the class WF of well-founded sets forms a well-founded submodel and, conversely, suitable permutations of well-founded models induce non-well-founded models. The reason is that foundation in contrast to AC does not reflect a property of the ambient meta theory.

Acknowledgements. This research benefited from a quotient construction yielding the extensional model $\mathcal{S}_i$ first formalised by Chad E. Brown in Coq using a full choice axiom. We also thank the anonymous reviewers for their helpful comments and suggestions that improved the final version of this paper.

References

1. P. Aczel. The Type Theoretic Interpretation of Constructive Set Theory. *Studies in Logic and the Foundations of Mathematics*, 96:55–66, Jan. 1978.
2. P. Aczel. On Relating Type Theories and Set Theories. In *Types for Proofs and Programs*, Lecture Notes in Computer Science, pages 1–18. Springer, Berlin, Heidelberg, Mar. 1998.
3. F. Barbanera and S. Berardi. Proof-irrelevance out of excluded-middle and choice in the calculus of constructions. *Journal of Functional Programming*, 6(3):519–525, 1996.
4. B. Barras. Sets in Coq, Coq in Sets. *Journal of Formalized Reasoning*, 3(1):29–48, Oct. 2010.
5. A. Bauer, J. Gross, P. L. Lumsdaine, M. Shulman, M. Sozeau, and B. Spitters. The HoTT Library: A Formalization of Homotopy Type Theory in Coq. In *CPP 2017*, pages 164–172, New York, NY, USA, 2017. ACM.
6. N. Bourbaki. Sur le théorème de Zorn. *Archiv der Mathematik*, 2(6):434–437, 1949.
7. T. Coquand. Metamathematical Investigations of a Calculus of Constructions. 1989. RR-1088, INRIA, <inria-00075471>.
8. H. R. Gylterud. From Multisets to Sets in Hotmotopy Type Theory. Dec. 2016. arXiv: 1612.05468.
9. J. D. Hamkins. Every Countable Model of Set Theory Embeds into its own Constructible Universe. *Journal of Mathematical Logic*, 13(02), Dec. 2013.

10. K. Hrbacek and T. Jech. *Introduction to Set Theory, Third Edition, Revised and Expanded*. CRC Press, June 1999.
11. D. Kirst and G. Smolka. Categoricity results for second-order ZF in dependent type theory. In M. Ayala-Rincón and C. A. Muñoz, editors, *ITP 2017, Brasília, Brazil, September 26-29, 2017*, volume 10499 of *LNCS*, pages 304–318. Springer, 2017.
12. D. Kirst and G. Smolka. Large model constructions for second-order ZF in dependent type theory. In J. Andronick and A. P. Felty, editors, *CPP 2018, Los Angeles, CA, USA, January 8-9, 2018*, pages 228–239. ACM, 2018.
13. G. Kreisel. Two notes on the foundations of set-theory. *Dialectica*, 23(2):93–114, 1969.
14. K. Kunen. *Set Theory: An Introduction to Independence Proofs*. Elsevier, June 2014.
15. J. Ledent. Modeling set theory in homotpy type theory. 2014.
16. L. C. Paulson. Set theory for verification: I. from foundations to functions. *Journal of Automated Reasoning*, 11(3):353–389, Oct 1993.
17. D. Scott. Axiomatizing Set Theory. *Proceedings of Symposia in Pure Mathematics*, 13:207–214, 1974.
18. 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.
19. G. Smolka, S. Schäfer, and C. Doczkal. Transfinite Constructions in Classical Type Theory. In X. Zhang and C. Urban, editors, *ITP 2015, Nanjing, China, August 24-27, 2015*, LNCS 9236. Springer, 2015.
20. R. M. Smullyan and M. Fitting. *Set Theory and the Continuum Problem*. Dover books on mathematics. Dover Publications, 2010.
21. M. Sozeau and N. Tabareau. Universe Polymorphism in Coq. In *Interactive Theorem Proving*, Lecture Notes in Computer Science, pages 499–514. Springer, Cham, July 2014.
22. P. Suppes. *Axiomatic Set Theory*. Dover Books on Mathematics Series. Dover Publications, 1960.
23. The Coq Proof Assistant. `http://coq.inria.fr`, 2018.
24. T. Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. `https://homotopytypetheory.org/book`, Institute for Advanced Study, 2013.
25. G. Uzquiano. Models of Second-Order Zermelo Set Theory. *The Bulletin of Symbolic Logic*, 5(3):289–302, 1999.
26. J. Väänänen. Second-Order Logic or Set Theory? *The Bulletin of Symbolic Logic*, 18(1):91–121, 2012.
27. B. Werner. Sets in Types, Types in Sets. In *Theoretical Aspects of Computer Software*, pages 530–546. Springer, Heidelberg, Sept. 1997.
28. N. H. Williams. On Grothendieck Universes. *Compositio Mathematica*, 21(1):1–3, 1969.
29. E. Zermelo. Neuer Beweis für die Möglichkeit einer Wohlordnung. *Mathematische Annalen*, 65:107–128, 1908.
30. E. Zermelo. Über Grenzzahlen und Mengenbereiche: Neue Untersuchungen über die Grundlagen der Mengenlehre. *Fundamenta Mathematicæ*, 16:29–47, 1930.