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

Dominik Kirst
Saarland University
Saarland Informatics Campus
Saarbrücken, Germany
kirst@ps.uni-saarland.de

Gert Smolka
Saarland University
Saarland Informatics Campus
Saarbrücken, Germany
smolka@ps.uni-saarland.de

Abstract

We study various models of classical second-order set theories in the dependent type theory of Coq. Without logical assumptions, Aczel's sets-as-trees interpretation yields an intensional model of second-order ZF with functional replacement. Building on work of Werner and Barras, we discuss the need for quotient axioms in order to obtain extensional models with relational replacement and to construct large sets. Specifically, we show that the consistency strength of Coq extended by excluded middle and a description operator on well-founded trees allows for constructing models with exactly n Grothendieck universes for every natural number n. By a previous categoricity result based on Zermelo's embedding theorem, it follows that those models are unique up to isomorphism. Moreover, we show that the smallest universe contains exactly the hereditarily finite sets and give a concise independence proof of the foundation axiom based on permutation models.

CCS Concepts • **Theory of computation → Type theory**; *Higher order logic*;

Keywords second-order set theory, dependent type theory, sets-as-trees model constructions, consistency strength, Coq

ACM Reference Format:
Dominik Kirst and Gert Smolka. 2018. Large Model Constructions for Second-Order ZF in Dependent Type Theory. In *Proceedings of 7th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP'18).* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3167095

CPP'18, January 8–9, 2018, Los Angeles, CA, USA

ACM ISBN 978-1-4503-5586-5/18/01…$15.00
https://doi.org/10.1145/3167095

1 Introduction

In his 1978 article, Aczel [1] used well-founded trees to interpret constructive set theory in Martin-Löf type theory. This involved defining a notion of tree equivalence and membership faithful to set theory as well as constructions that implement the usual set operations like empty set, pairing, and union. The obtained tree model is intensional in the sense that it contains distinct but equivalent trees and the set-theoretical axioms only hold in accordingly weakened form. Based on Aczel's interpretation, Werner [17] and Barras [4] formalised models of set theory in the Coq proof assistant [7] in order to determine the consistency strength of Coq's underlying type theory. With the work presented in this paper we address a point observed by both authors: the need for logical assumptions (1) to treat the replacement axiom and (2) to construct models containing Grothendieck universes, i.e. large sets that are closed under all axiomatic set operations.

(1) The replacement axiom of first-order ZF set theory asserts the existence of a set y based on a set x and a formula $\phi(a, b)$ where elements $a \in x$ are replaced by related sets b, provided that $\phi(a, b)$ is functional. In type theory with a type S of sets, the replacement formula $\phi(a, b)$ can be naturally expressed either by a binary relation $S \to S \to \mathrm{Prop}$ or a function $S \to S$. While the functional replacement can be defined directly for Aczel's tree type, the relational version requires a logical assumption turning (partial) functional relations into actual type-level functions. We construct relational replacement assuming a description operator for trees (TD), which is a strong form of unique choice yielding representatives of tree equivalence classes. Since one can reconstruct a description operator from relational replacement [11], we know that this assumption is minimal.

(2) In the sets-as-trees interpretation, Grothendieck universes arise from embedding the tree model at a low type universe into itself at a higher type universe. However, justifying the closure under functional replacement again relies on choice-like axioms. The same assumption of a description operator on trees resolves the problem and thus yields large models containing multiple Grothendieck universes. Moreover, assuming a local form of proof irrelevance (PI), the tree description operator allows for deriving extensional models where equivalent sets are equal.

The relevance of the existence of Grothendieck universes is the induced measure of consistency strength: a large type-theoretical model of set theory proves the consistency of axiomatic systems like ZF with certain large cardinal axioms. Specifically, since the type theory underlying Coq comes with a countably infinite hierarchy of type universes, we can iterate the mentioned self-embedding and thus obtain models with finitely many Grothendieck universes. This correspondence of expressive strength of a Coq-like type theory and ZF set theory with a hierarchy of Grothendieck universes was observed by Werner [17] and Aczel [2]. Our mechanisation of these large model constructions relies on universe-polymorphic definitions of the tree type and the recursive embedding function.

It must be noted that substituting the axiomatic schemes of first-order ZF (referring to formulas such as $\phi(a, b)$ in the case of replacement) by single higher-order statements yields a stronger and semantically more determined theory, especially in the presence of excluded middle (XM). In fact, as a consequence of Zermelo's non-constructive embedding theorem [18], models of second-order ZF only vary in the order type of the class of Grothendieck universes [16]. Thus adding axioms controlling this order type yields categorical axiomatisations describing unique models (up to isomorphism). In a previous paper [8], we study the categorical axiom systems $\mathbf{ZF}_n$, which assert the existence of exactly n Grothendieck universes for natural numbers n.

Contributions. The main result presented in this paper is that the unique models of the axiomatisations $\mathbf{ZF}_n$ can be constructed in Coq assuming tree description and excluded middle. As an intermediate result, the construction of underspecified large models containing at least but not exactly n Grothendieck universes does not rely on excluded middle but only a local form of proof irrelevance. We further verify an explicit construction of the smallest universe containing exactly the hereditarily finite sets, characterised by an inductive predicate. Finally, we formalise a concise proof of the independence of the foundation axiom relying on permutation models. See Table 1 in the final section for the formal statements of the main results and the respective axioms. The definitions and statements of the PDF version of this paper are hyperlinked with the accompanying Coq development available for browsing and downloading on our project web page.[1]

Outline. The paper is split into two parts. First, we give preliminary definitions concerning set structures, axiom systems, and Grothendieck universes and study the recurring notion of membership embeddings. We then discuss Aczel's intensional model and derive extensional models based on two different approaches. The first part ends with Section 6 on large models. In the second part, the theory of ZF is developed concerning the different forms of replacement, the cumulative hierarchy, the initial universe of hereditarily finite sets, Zermelo's embedding theorem, and height-controlled submodels. We conclude with a construction of non-well-founded models and a discussion of our results in the context of related and future work.

[1] https://www.ps.uni-saarland.de/extras/cpp18-sets

2 Preliminaries

For any type A we call a unary predicate $P : A \to \mathrm{Prop}$ 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 $R : A \to B \to \mathrm{Prop}$ on any two types A and B we define classes $\mathrm{dom}(R) := \lambda a.\, \exists b.\, R\,a\,b$ and $\mathrm{ran}(R) := \lambda b.\, \exists a.\, R\,a\,b$ representing the domain and range of R. Finally, for any type A and class P over A we write $\langle a : A \mid a \in P\rangle$ for the refinement type $\Sigma a : A.\, a \in P$.

Definition 2.1. *A **set structure** is a type $\mathcal{M}$ with a binary relation $\in : \mathcal{M} \to \mathcal{M} \to \mathrm{Prop}$ called **membership**. We call $\mathcal{M}$ a **ZF-structure** if it further comes with constants*

$$\begin{aligned} \emptyset &: \mathcal{M} & \_ \cap \_ &: (\mathcal{M} \to \mathrm{Prop}) \to \mathcal{M} \to \mathcal{M} \\ \{\_,\_\} &: \mathcal{M} \to \mathcal{M} \to \mathcal{M} & \_@\_ &: (\mathcal{M} \to \mathcal{M}) \to \mathcal{M} \to \mathcal{M} \\ \bigcup &: \mathcal{M} \to \mathcal{M} & \delta &: (\mathcal{M} \to \mathrm{Prop}) \to \mathcal{M} \\ \mathcal{P} &: \mathcal{M} \to \mathcal{M} \end{aligned}$$

*for empty set, unordered pair, union, power set, separation, replacement and description. If $\mathcal{M}$ lacks a constant δ for description, we call it a **ZF′-structure** and if it also lacks a constant @ for replacement we call it a **Z-structure**.*

A class P over a set structure $\mathcal{M}$ is called **small** if there is $x : \mathcal{M}$ that **agrees** with P, i.e. $y \in x$ iff $y \in P$ for all $y : \mathcal{M}$. Furthermore, set structures carry a notion of set equivalence:

Definition 2.2. *Let $\mathcal{M}$ be a set structure. We define the binary relation $x \equiv y := x \subseteq y \wedge y \subseteq x$ called **set equivalence** with equivalence classes $[x] := \lambda y.\, y \equiv x$. 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) $\forall x, x'.\, x \equiv x' \to F\,x \equiv F\,x'$.
Those are abbreviated by $P : \mathcal{M} \overset{\equiv}{\to} \mathrm{Prop}$ and $F : \mathcal{M} \overset{\equiv}{\to} \mathcal{M}$.

Given any set structure, we employ the usual shorthands such as $\{x\} := \{x, x\}$ and $x \cup y := \bigcup \{x, y\}$. Note that we also identify sets x with their corresponding classes $\lambda y.\, y \in x$.

Definition 2.3. *For a set structure $\mathcal{M}$ we define the inductive class $WF : \mathcal{M} \to \mathrm{Prop}$ of **well-founded sets** by*

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

The corresponding induction principle is called $\in$-induction and the recursion principle in Type *is called $\in$-recursion.*

Note that, in Coq's type theory, proofs of *WF* can be eliminated to arbitrary types since *WF* is defined using a single constructor taking only parameters and proofs as arguments. See Definition 6.1 for an example of an $\in$-recusive definition.

Definition 2.4. *A ZF-structure is an* ***intensional model*** *if all of the following propositions hold:*

$$\begin{aligned}
\mathsf{Morph} &: \forall x, x', y.\, x \equiv x' \to x \in y \to x' \in y\\
\mathsf{Found} &: \forall x.\, x \in \mathit{WF}\\
\mathsf{Eset} &: \forall x.\, x \notin \emptyset\\
\mathsf{Pair} &: \forall x, y.\, z \in \{x, y\} \leftrightarrow z \equiv x \vee z \equiv y\\
\mathsf{Union} &: \forall x, z.\, z \in \bigcup x \leftrightarrow \exists y \in x.\, z \in y\\
\mathsf{Power} &: \forall x, y.\, y \in \mathcal{P}x \leftrightarrow y \subseteq x\\
\mathsf{Sep} &: \forall P : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop}, x, y.\, y \in P \cap x \leftrightarrow y \in x \wedge y \in P\\
\mathsf{Frep} &: \forall F : \mathcal{M} \xrightarrow{\equiv} \mathcal{M}, x, z.\, z \in F@x \leftrightarrow \exists y \in x.\, z \equiv F\, y\\
\mathsf{Desc}_1 &: \forall P.\, (\exists x.\, \forall y.\, y \in P \leftrightarrow y \equiv x) \to \delta P \in P\\
\mathsf{Desc}_2 &: \forall P, P'.\, (\forall x.\, x \in P \leftrightarrow x \in P') \to \delta P = \delta P'
\end{aligned}$$

We denote the class of ZF-structures satisfying these axioms by $\mathbf{ZF}_{\equiv}$ *and write* $\mathcal{M} \models \mathbf{ZF}_{\equiv}$ *instead of* $\mathcal{M} \in \mathbf{ZF}_{\equiv}$*. Further, we write* $\mathcal{M} \models \mathbf{ZF}'_{\equiv}$ *if* $\mathcal{M}$ *is a ZF′-structure satisfying all axioms but* Desc *(meaning both* Desc_1 *and* Desc_2*).*

Our axiomatisation expresses intensional second-order ZF close to the formulation given by Barras [4]. We use a version of replacement for functions together with a description operator and reconstruct the relational formulation from Barras in Section 7. Description implements a weak form of choice by picking canonical representatives for equivalence classes. Further, we do not include an infinity axiom by default but assume it explicitly where needed.

Definition 2.5. *We define the infinity assertion by*

$$\mathsf{Inf} : \exists \omega.\, \forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x \equiv \mathcal{P}^n\, \emptyset$$

We write $\mathbf{ZF}_{\equiv}$ *for* $\mathbf{ZF}_{\equiv} + \mathsf{Inf}$*, similarly for other axiomatisations.*

Note that this is a non-standard formulation in using the external notion of natural numbers and power set instead of the von Neumann successor $\sigma x := x \cup \{x\}$. Using external numbers is anyway unavoidable for the forthcoming Definition 2.9 and the primitive power set operation naturally matches to the structure of the cumulative hierarchy defined in Section 8.

Definition 2.6. *A ZF-Structure is an* ***(extensional) model*** *if it satifies* $\mathbf{ZF}_{\equiv}$ *as well as the proposition*

$$\mathsf{Ext} : \forall x, y.\, x \equiv y \to x = y$$

We write $\mathcal{M} \models \mathbf{ZF}$ *for extensional models and similarly*
(1) $\mathcal{M} \models \overline{\mathbf{Z}}$ *for Z-structures satisfying* **ZF** *but* Frep *and* Desc*,*
(2) $\mathcal{M} \models \mathbf{ZF}'$ *for ZF′-structures satisfying* **ZF** *but* Desc*,*
(3) $\mathcal{M} \models \mathbf{ZF}^*$ *for ZF-structures satisfying* **ZF** *but* Found*.*

Note that in the presence of Ext most of the other axioms can be simplified by replacing $\equiv$ with $=$. In particular, Morph and the conditions in Sep and Frep vanish as all classes and functions respect $=$ and Desc reduces to the more familiar **unique choice** axiom:

$$\forall P : \mathcal{M} \to \mathsf{Prop}.\, (\exists! x.\, x \in P) \to \delta P \in P$$

For the remainder of this section we fix a ZF-structure $\mathcal{M}$.

Definition 2.7. *We call a class* P *over* $\mathcal{M}$ ***transitive*** *whenever* $y \in x \in P$ *implies* $y \in P$*. Similarly, we say that* P *is* ***swelled*** *whenever* $y \subseteq x \in P$ *implies* $y \in P$*.*

Definition 2.8. *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* $P : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop}$ *and functions* $F : \mathcal{M} \xrightarrow{\equiv} \mathcal{M}$*:*

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

If U *satisfies all properties above but (6), we call it* ***Z-closed****. If* U *is ZF-closed and small, we call it a* ***universe****.*

Definition 2.9. *We introduce a notion of* ***strength*** *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* **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* **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/model strength is only a lower bound and hence not unique, given that every set/model of strength n also has strength m for all $m < n$. In Section 9 we show that **ZF** is equivalent to $\mathbf{ZF}_{\geq 1}$.

3 Membership Embeddings

One recurring pattern in this paper is the situation where we have one model embedded into another. For such embeddings, both models agree on the notion of universes and strength of corresponding sets. This section constitutes an abstract proof of this fact which is instantiated for three concrete embeddings in Sections 5, 6 and 11. To this end we assume two models $\mathcal{M}$ and $\mathcal{N}$ of $\mathbf{ZF}_{\equiv}$.

Definition 3.1. $h : \mathcal{M} \to \mathcal{N}$ *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 now further assume such an embedding h.

Lemma 3.2. $x \subseteq y \leftrightarrow h\,x \subseteq h\,y$ *and* $x \equiv y \leftrightarrow h\,x \equiv h\,y$*.*

Proof. The first statement is an easy consequence of the properties of h and directly implies the second statement. □

Fact 3.3. *The following equivalences hold:*

(1) $h\,\emptyset_{\mathcal{M}} \equiv \emptyset_{\mathcal{N}}$ (3) $h\,(\bigcup x) \equiv \bigcup (h\,x)$
(2) $h\,(\{x, y\}) \equiv \{h\,x, h\,y\}$ (4) $h\,(\mathcal{P}x) \equiv \mathcal{P}(h\,x)$

Proof. We verify the statements using the definition of $\equiv$. Concerning (1), supposing $x' \in h\,\emptyset_{\mathcal{N}}$ yields an inhabitant $x \in \emptyset_{\mathcal{M}}$ for $h\,x \equiv x'$, contradicting Eset for $\mathcal{M}$. For the other inclusion we assume $x' \in \emptyset_{\mathcal{N}}$, directly contradicting Eset for $\mathcal{N}$. The other three properties also just use the respective membership axioms of $\mathcal{M}$ and $\mathcal{N}$, we here discuss (2). If $z' \in h\ \{x, y\}$ we know that there is $z \in \{x, y\}$ with $h\,z \equiv z'$. Then by Pair either $z \equiv x$ or $z \equiv y$, so either $z' \equiv h\,x$ or $z' \equiv h\,y$ from which we conclude $z' \in \{h\,x, h\,y\}$. For the converse we start with $z' \in \{h\,x, h\,y\}$ and obtain z with either $z \in x$ or $z \in y$ by the properties of h. The proofs for union and power set follow the same pattern. □

This shows that h is a morphism for most of the set operations. The corresponding statement for replacement needs a bit of preparation.

Definition 3.4. *We define* $h^{-1}x' := \delta(\lambda x.\, h\,x \equiv x')$.

Fact 3.5. $h\,(F@x) \equiv (h \circ F \circ h^{-1})@(h\,x)$ *if* F *respects* $\equiv$.

Proof. Let $z' \in h\,(F@x)$, so there is $z \in F@x$ with $h\,z \equiv z'$. Then Frep yields $y \in x$ with $z \equiv F\,y$. The preimage is well-defined for sets in the range of h, so the equivalences can be summarised by $z' \equiv (h \circ F \circ h^{-1})\,(h\,y)$ which witnesses $z' \in (h \circ F \circ h^{-1})@(h\,x)$. Now suppose $z' \in (h \circ F \circ h^{-1})@(h\,x)$. This yields $y' \in h\,x$ with $z' \equiv (h \circ F \circ h^{-1})\,y'$ which has a preimage y witnessing $z' \in h\,(F@x)$. □

Using these morphism properties, we now prove that h respects ZF-closed classes in both directions.

Definition 3.6. *Let* $P : \mathcal{M} \xrightarrow{\equiv} \mathrm{Prop}$ *be a class that respects* $\equiv$. *Then we define the* ***image*** $h[P] := \lambda x'.\, \exists x.\, h\,x \equiv x' \wedge x \in P$. *We further define the* ***range*** *of* h *by* $\mathrm{ran}(h) := h[\lambda\_.\,\top]$.

Fact 3.7. $h\,x$ *agrees with* $h[x]$.

Proof. Directly by the properties of embeddings. □

Theorem 3.8. P *is ZF-closed iff* $h[P]$ *is ZF-closed.*

Proof. We just discuss the direction from left to right since the other direction is (almost) symmetric. So assume that P is ZF-closed. That $h[P]$ is transitive is easily established using that P is transitive. Moreover, the closure under separation can be justified by the fact that it is equivalent to $h[P]$ being swelled. Similarly as transitivity this follows from P being swelled, which in turn expresses nothing but P being closed under separation.

The remaining closure properties all follow the same pattern, we discuss the case of $\emptyset$ and pairing as examples. Since by assumption $\emptyset_{\mathcal{M}} \in P$, we have $h\,\emptyset_{\mathcal{M}} \in h[P]$. Then we use (1) of Fact 3.3 to conclude $\emptyset_{\mathcal{N}} \in h[P]$. Now suppose we have $x', y' \in h[P]$. By definition of $h[P]$ this yields related preimages $x, y \in P$. Since P is closed under pairing we obtain $\{x, y\} \in P$ and thus $h\ \{x, y\} \in P[x]$. Now (2) of Fact 3.3 yields $\{x', y'\} \in P[x]$ as claimed. The proofs for union and power set are analogous and the proof for replacement uses a similar translation for functions as in Fact 3.5. □

Using Fact 3.7 yields the specific property of universes:

Corollary 3.9. U *is a universe iff* $h\,U$ *is a universe.*

Since the full class $\lambda\_.\top$ is ZF-closed, we further derive:

Corollary 3.10. $\mathrm{ran}(h)$ *is ZF-closed.*

The second property of embeddings concerning the notion of strength is a consequence.

Fact 3.11. x *has strength* n *iff* $h\,x$ *has strength* n.

Proof. We prove the equivalence by natural induction. The statement for 0 is trivial since every set has strength 0 by definition. In the successor case we need to show that there is a universe $U \in x$ of strength n iff there is a universe $U' \in h\,x$ of same strength. Assuming the former yields that $h\,U \in h\,x$ is a universe by Corollary 3.10 and of equal strength by the inductive hypothesis. The other direction is analogous. □

4 Constructing an Intensional Model

We work in the dependent type theory underlying Coq with a countably infinite hierarchy of type universes Type_i. We make the universe levels explicit where necessary and admit definitions that are polymorphic for all type universes, as implemented in Coq [13]. Our main instance of a universe-polymorphic definition is the following:

Definition 4.1. *We define the universe-polymorphic family of inductive types* $\mathcal{T}_i : \mathrm{Type}_i$ *of* ***well-founded trees*** *with a term constructor* $\tau : \forall(A : \mathrm{Type}_j).\, (A \to \mathcal{T}_i) \to \mathcal{T}_i$ *for* $j < i$. *We define projections* $p_1(\tau\,A\,f) := A$ *and* $p_2(\tau\,A\,f) := f$.

Following Aczel [1, 2], we interpret the trees in $\mathcal{T}_i$ as sets, where the trees $f\,a$ correspond to the elements of the tree $\tau\,A\,f$. However, since intensionally distinct types and functions can yield structurally equal trees, we first impose a notion of tree equivalence and then define a respectively generalised version of membership.

Definition 4.2. ***Equivalence*** $\equiv_{\mathcal{T}_i} : \mathcal{T}_i \to \mathcal{T}_i \to \mathrm{Prop}$ *of trees is defined by the inductive predicate*

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

Membership *is defined by* $s \in \tau\,A\,f := \exists a : A.\, s \equiv_{\mathcal{T}_i} f\,a$ *and* ***inclusion*** *accordingly by* $s \subseteq t := \forall u.\, u \in s \to u \in t$.

Fact 4.3. $\equiv_{\mathcal{T}_i}$ *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 2.1), so we can use the relations interchangeably.

Fact 4.4. $s \equiv t \leftrightarrow s \equiv_{\mathcal{T}_i} t$

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 4.3. □

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

Definition 4.5. *We turn $\mathcal{T}_i$ into a ZF′-structure by defining*

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

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

Theorem 4.6. $\mathcal{T}_i \models \mathbf{ZF}'_{\equiv}$

Proof. Morph was already shown in Fact 4.3. 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 $u \equiv (\text{if } b \text{ then } s \text{ else } t)$ 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. □

5 Extensional Models

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 $\mathcal{T}_i$. A first approach is to simply work on the type of all equivalence classes $[s] = \lambda t.\, s \equiv t$ and lift all set operations from trees to classes. The key requirement for this approach to go through is **class extensionality**.

Axiom (CE). $\forall P, P'.\, (\forall s.\, s \in P \leftrightarrow s \in P') \to P = P'$

Note that now in particular $[s] = [t]$ whenever $s \equiv t$.

Definition 5.1. *We define the type $\mathcal{S}'_i$ of equivalence classes by $\mathcal{S}'_i := \langle P : \mathcal{T}_i \to \mathrm{Prop} \mid \exists s.\, P = [s]\rangle$. We write X, Y, Z for the members of $\mathcal{S}'_i$ as well as the underlying classes. Membership is $X \in Y := \forall s, t.\, s \in X \to t \in Y \to s \in t$ and inclusion is defined accordingly.*

In order to obtain strict extensionality concerning the members of the refinement type $\mathcal{S}'_i$, we further assume a local form of **proof irrelevance**, namely that the proofs of propositions $\exists s.\, P = [s]$ are unique. By this assumption also the second components of elements of $\mathcal{S}'_i$ with same first component are equal.

Axiom (PI_1). $\forall P.\, \forall (H, H' : \exists s.\, P = [s]).\, H = H'$

Lemma 5.2. $[s] \in [t] \leftrightarrow s \in t$ *and* $[s] \subseteq [t] \leftrightarrow s \subseteq t$.

Proof. First suppose $[s] \in [t]$ so $s' \in t'$ for all $s' \in [s]$ and $t' \in [t]$. Since in particular $s \in [s]$ and $t \in [t]$ we conclude $s \in t$. Conversely, let $s \in t$. Now we have to show $s' \in t'$ for all $s' \in [s]$ and $t' \in [t]$. This follows since membership respects the equivalences $s \equiv s'$ and $t \equiv t'$. The statement for inclusion follows directly. □

Definition 5.3. *We turn $\mathcal{S}'_i$ into a Z-structure by defining:*

$$\begin{aligned}
\emptyset_{\mathcal{S}'_i} &:= [\emptyset] \\
\{X, Y\} &:= \lambda u.\, \exists s, t.\, s \in X \wedge t \in Y \wedge u \equiv \{s,t\} \\
\bigcup X &:= \lambda t.\, \exists s.\, s \in X \wedge t \equiv \bigcup s \\
\mathcal{P}X &:= \lambda t.\, \exists s.\, s \in X \wedge t \equiv \mathcal{P}s \\
X \cap P &:= \lambda t.\, \exists s.\, s \in X \wedge t \equiv (\lambda z.\, [z] \in P) \cap s
\end{aligned}$$

Justification. Note that we first have to verify that the defined classes are actual equivalence classes and hence constitute members of $\mathcal{S}'_i$. So for instance, we have to find a witness u such that $\{X, Y\} = [u]$. This is not immediate since the representatives corresponding to X and Y are existentially quantified and hence not functionally accessible. However, when constructing the existential proof for $\{X, Y\}$, we obtain some representatives $X = [s]$ and $Y = [t]$ and thus have $\{X, Y\} = [\{s,t\}]$. A similar argument works for the other set operations. □

It seems in fact impossible to define a replacement operation since this requires the representatives of equivalence

classes to be accessible functionally. Hence $\mathcal{S}'_i$ only constitutes an extensional model of $\overline{\mathbf{Z}}$.

Fact 5.4. $\mathcal{S}'_i \models \mathbf{Z}$

Proof. Verifying the axioms for $\mathcal{S}'_i$ becomes simple when making use of Lemma 5.2. First recall that Morph is trivial when considering extensional models. Then for Ext assume $X \subseteq Y$ and $Y \subseteq X$. Since constructing proofs, we can replace the classes by witnesses and obtain $[s] \subseteq [t]$ and $[t] \subseteq [s]$. But then $s \subseteq t$ and $t \subseteq s$, so Ext of $\mathcal{T}_i$ implies $s \equiv t$, from which we in turn conclude $[s] = [t]$.

Similarly, to establish Found we show that $[s] \in \mathit{WF}$ by $\in$-induction on s. So we can assume $[t] \in \mathit{WF}$ for all $t \in s$ and have to show $Y \in \mathit{WF}$ for all $Y \in [s]$. However, we can again replace Y by a class $[t]$ and use that $[t] \in [s]$ implies $t \in s$. Furthermore, Inf is witnessed by $[\omega_{\mathcal{T}_i}]$.

All membership axioms are established by the same idea. This time, Union and Power serve as instances. Concerning Union, we first show that $[\bigcup x] = \bigcup [x]$ which follows from the assumed extensionality of classes. Then the statement of Union reads $[u] \in [\bigcup s] \leftrightarrow \exists t.[u] \in [t] \wedge [t] \in [s]$ which is exactly turned into the corresponding axiom of $\mathcal{T}_i$ by Lemma 5.2. The proof of Power is identical after the fact $[\mathcal{P}x] = \mathcal{P}[x]$ has been established. □

A way to solve the previous problem concerning replacement is to assume **canonical representatives** for the equivalence classes of $\equiv$ in form of a **normaliser**:

Axiom (CR). *We assume a function $\gamma : \mathcal{T}_i \to \mathcal{T}_i$ that yields unique representatives γs for the equivalence classes $[s]$:*

$$(1)\ \gamma s \equiv s \qquad (2)\ s \equiv t \to \gamma s = \gamma t$$

Lemma 5.5. *γ is idempotent and $\gamma s = \gamma t$ implies $s \equiv t$.*

Proof. Idempotency follows from applying (2) to (1) and if $\gamma s = \gamma t$ we have $s \equiv \gamma s = \gamma t \equiv t$. □

Indeed, one could now extend the Z-structure $\mathcal{S}'_i$ to a ZF′-structure by defining a replacement operator employing γ and prove the corresponding membership law. However, since we now have representatives of every equivalence class available, there is a simpler construction. We remark that now the axioms CE and PI_1 from the previous construction are not needed anymore.

Definition 5.6. *We define $\mathcal{S}_i := \langle s : \mathcal{T}_i \mid \gamma s = s \rangle$ to be the subtype 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. $\overline{s} \in \overline{t} := s \in t$ and inclusion is again defined accordingly.*

If we further assume the proofs of propositions $\gamma s = s$ to be unique, then the type $\mathcal{S}_i$ carries a ZF′-structure satisfying all extensional ZF axioms but description.

Axiom (PI_2). $\forall (s : \mathcal{T}_i), (H, H' : \gamma s = s).\ H = H'$

Definition 5.7. *We turn $\mathcal{S}_i$ into a ZF′-structure by setting*

$$\emptyset_{\mathcal{S}_i} := \gamma\emptyset \qquad \mathcal{P}\overline{s} := \gamma(\mathcal{P}s)$$
$$\{\overline{s}, \overline{t}\} := \gamma(\{s, t\}) \qquad P \cap \overline{s} := \gamma((P \circ \gamma) \cap s)$$
$$\bigcup \overline{s} := \gamma(\bigcup s) \qquad F@\overline{s} := \gamma((F \circ \gamma)@s)$$

Fact 5.8. $\mathcal{S}_i \models \mathbf{ZF}'$

Proof. As before, Morph holds trivially and Ext as well as Found 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. □

Since some of the following set-theoretic constructions rely on relational replacement which only can be derived from functional replacement together with description [11], we finally turn $\mathcal{T}_i$ and $\mathcal{S}_i$ into full ZF-structures. To this end we simply assume a description operator for trees:

Axiom (TD). *We assume a function $\delta : (\mathcal{T}_i \to \mathsf{Prop}) \to \mathcal{T}_i$ that satisfies* Desc *for $\mathcal{T}_i$.*

First note that TD implies CR by defining $\gamma s := \delta[s]$. Furthermore, δ extends $\mathcal{T}_i$ to a ZF-structure and by setting $\delta_{\mathcal{S}_i} P := \gamma(\delta(P \circ \gamma))$ we also make $\mathcal{S}_i$ a ZF-structure.

Theorem 5.9. *$\mathcal{T}_i \models \mathbf{ZF}_{\equiv}$ and $\mathcal{S}_i \models \mathbf{ZF}$.*

Proof. $\mathcal{T}_i \models \mathbf{ZF}_{\equiv}$ follows from Theorem 4.6 and TD. Then for $\mathcal{S}_i \models \mathbf{ZF}$ we apply Fact 5.8 using that TD implies CR. So it remains to show that $\delta_{\mathcal{S}_i}$ satisfies Desc. By construction of $\delta_{\mathcal{S}_i}$ this follows from the corresponding property of δ. □

In the next section we will use that the intensional and extensional model agree on universes and strength:

Fact 5.10. *γ is an embedding.*

Proof. Both conditions are by construction of $\mathcal{S}_i$. □

6 Large Models

The type theory with countably many type universes underlying Coq admits the construction of large models of **ZF**. Intuitively, the type universes correspond to set universes and indeed, for every number $n : \mathbb{N}$ 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 self-embedding $\mathcal{S}_j$

at lower levels $j < i$. In fact, any intensional model embeds into some $\mathcal{S}_i$ by $\in$-recursion. Note that in this section we still assume TD and PI_2.

Definition 6.1. *For an intensional model $\mathcal{M} \models \mathbf{ZF}_{\equiv}$ we define a function $\iota : \mathcal{M} \to \mathcal{T}_i$ by $\in$-recursion*

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

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

Lemma 6.2. *ι respects equivalence and membership, that is:*

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

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 6.3. *ι is an embedding.*

Proof. The first condition was shown in Lemma 6.2 and the second condition is straight-forward by definition. □

Lemma 6.4. *If $\mathcal{M} \models \mathbf{ZF}_{\equiv}$ then $U_{\mathcal{M}}$ is a universe.*

Proof. By definition $U_{\mathcal{M}}$ agrees with $\mathsf{ran}(\iota)$. That $\mathsf{ran}(\iota)$ is ZF-closed follows from Corollary 3.10 using Lemma 6.3. □

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

Lemma 6.5. *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 3.11 and Lemma 6.3. Hence, being transitive, $U_{\mathcal{M}}$ has the same strength. □

Fact 6.6. *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 6.5 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 on paper:

Theorem 6.7. *$\mathbf{ZF}_{\geq n}$ has a model for all $n : \mathbb{N}$.*

Proof. We construct the large models by inductively iterating Fact 6.6. First, by Theorem 5.9 we know that $\mathcal{S}_i \models \mathbf{ZF}_{\geq 0}$. For the inductive step suppose we have a model $\mathcal{M} \models \mathbf{ZF}_{\geq n}$. Then Fact 6.6 yields a model of $\mathbf{ZF}_{\geq n+1}$. □

Note that this remains a meta-statement as, when formalised in Coq with explicit universe levels, it reads

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

for a fixed type universe Type_i. This is not an inductive consequence of Fact 6.6 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 universes [2].

Fact 6.8. $(\forall n : \mathbb{N}.\, \exists \mathcal{M} : \mathsf{Type}_i.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}) \to \mathcal{S}_{i+1} \models \mathbf{ZF}_{\geq \omega}$

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 6.6 we know that $\gamma U_{\mathcal{M}} : \mathcal{S}_{i+1}$ has strength n. □

7 Relational Replacement

We now move away from the consistency question to the internal theory of extensional second-order ZF followed by model-theoretic considerations. The main results in this second part of the paper rely on **excluded middle**.

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

The axioms TD and PI_2 are not needed from now on. In fact, excluded middle implies global proof irrelevance (PI), a statement proven based on [3] in the Coq standard library.

Fact 7.1. $\forall (A : \mathsf{Prop}), (H, H' : A).\, H = H'$

For this and the following two sections we assume an extensional model $\mathcal{M}$ of **ZF**. As mentioned before, separation, functional replacement, and description can be combined to relational replacement:

Definition 7.2. $R@x \coloneqq (\lambda y.\, \delta(R\, y))@(\mathsf{dom}(R) \cap x)$

Relational replacement then holds for the class $\mathcal{F}(\mathcal{M})$ of functional relations $R : \mathcal{M} \to \mathcal{M} \to \mathsf{Prop}$:

Fact 7.3. $R \in \mathcal{F}(\mathcal{M}) \to (z \in R@x \leftrightarrow \exists y.\, y \in x \wedge R\, y\, z)$

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 is strong enough to express the operations of pairing, separation, functional replacement and description (cf. [8, 11, 14]). Hence we can give a simplified criterion for ZF-closed classes:

Fact 7.4. *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 $\mathrm{dom}(R) \cap x \in U$. 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. □

8 Cumulative Hierarchy and Universes

In this section, we develop the basic theory of the cumulative hierarchy and universes. The cumulative hierarchy, which stratifies the well-founded sets into a well-ordered class of stages, is a fundamental construction in set theory. Our development of ZF in dependent type theory allows a direct approach to this structure via inductive predicates instead of transfinite recursion on ordinals. This was discussed in a previous paper [8] where we have already established that the stages of the cumulative hierarchy are well-ordered and that all universes are such stages. Here, we briefly sketch these proofs to familiarise the reader with our inductive approach.

Definition 8.1. *We define the inductive class $\mathcal{V}$ of **stages**:*

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

*We call a stage V a **limit** if $V \subseteq \bigcup V$ and a **successor** if there is a stage V' with $V = \mathcal{P}\,V'$.*

Fact 8.2. *$\mathcal{V}$ is well-ordered by inclusion and every set occurs as a subset of a stage. Hence we can define a **rank function** $\rho : \mathcal{M} \to \mathcal{M}$ such that $\rho\,x$ is the least stage V with $x \subseteq V$. Then in particular $x \in \mathcal{P}(\rho x) \in \mathcal{V}$.*

Sketch. Clearly, inclusion is a partial order. Linearity of stages in the form $V \in V' \vee V' \subseteq V$ can be proved by double-induction (cf. [12]), which simplifies the necessary nested stage-induction on $V, V' \in \mathcal{V}$. Next, let P be a non-empty class of stages, so there is some $V \in P$. By $\in$-induction on V we find an $\subseteq$-least element of P because either V is already $\subseteq$-least or there is some $V' \in V$ with $V' \in P$ to which we can apply the inductive hypothesis. Thus inclusion on stages is well-founded.

Finally, by $\in$-induction we show that for every set x there is a stage V with $x \subseteq V$. The inductive hypothesis yields a stage V with $y \subseteq V$ for all $y \in x$. By well-foundedness of stages, for every $y \in x$ there is a unique least such stage which we denote by $\rho\,y$ using δ. Then $\rho\,x := \bigcup(\mathcal{P} \circ \rho)@x$ is a stage and $x \subseteq \rho\,x$. Thus $\rho\,x$ is well-defined for all $x : \mathcal{M}$. □

Fact 8.3. *Inhabited limits are Z-closed and universes are exactly the inhabited limits closed under replacement.*

Sketch. For the former, suppose V is a limit. One first proves that for every $x \in V$ there is a stage V' with $x \in V' \in V$. Then one shows that $\bigcup x \in V'$, $\mathcal{P}x \in \mathcal{P}V'$ and $P \cap x \in V'$ for all P. It follows that all those are contained in V and pairing works similarly with a second set $y \in V$. Further, all stages are transitive, which is a part of being Z-closed, and swelled, which implies that inhabited limits contain $\emptyset$. Thus, if the limit V is closed under replacement, it is a universe.

For the converse, we just have to show that universes U are limits. First note that $U = \bigcup(\mathcal{V} \cap U)$ where the inclusion $\subseteq$ follows since $\rho\,x \in U$ for all $x \in U$. So U is the union of a set of stages and hence a stage. The condition $U \subseteq \bigcup U$ to qualify U as limit is by $x \in \mathcal{P}(\rho\,x) \in U$ for $x \in U$. □

9 Infinity Axioms

In our treatment of ZF without an infinity axiom it is undetermined whether or not an inhabited limit exists. However, we can show that in models with an infinite set, the first inhabited limit is already a universe. To this end, we assume that our model $\mathcal{M}$ satisfies Inf for the remainder of this section and set $\Omega := \bigcup \omega$. Note that we can explicitly refer to the existentially quantified set ω in Inf using description.

Definition 9.1. *We define **adjunction** by $x.\,y := \{x\} \cup y$.*

Fact 9.2. $z \in x.y \leftrightarrow z = x \vee z \in y$

Proof. This is routine by the pairing and union axioms. □

Definition 9.3. *We define the inductive classes FI of **finite sets** and HF of **hereditarily finite sets** by the rules*

$$\frac{}{\emptyset \in FI} \qquad \frac{y \in FI}{x.y \in FI} \qquad \frac{x \in FI \quad \forall y \in x.\, y \in HF}{x \in HF}$$

Just using the set operations one cannot construct infinite sets from hereditarily finite sets. Hence it follows that all set operations remain within HF, making the class ZF-closed. Further, the finite powers included in Ω exhaust HF similarly as the transfinite powers of $\mathcal{V}$ exhaust all sets. Hence Ω agrees with HF and thus forms a universe.

Fact 9.4. *HF is ZF-closed.*

Proof. We apply the criterion from Fact 7.4. Transitivity of HF and $\emptyset \in HF$ are trivial. It remains to prove the closure under relational replacement, power and union.

Concerning replacement, let $x \in FI$ and R be a functional relation. We show that $R@x \in FI$ by induction on $x \in FI$. This is trivial in the first case since $R@\emptyset = \emptyset$. So suppose in the second case that we know $R@y \in FI$ and want to show that $R@(x.y) \in FI$. To this end consider that $R@(x.y) \subseteq (\bigcup R@\{x\}).(R@y)$. The set on the right-hand side is finite since $R@y$ is finite. Hence $R@(x.y)$ is finite as it is a subset of a finite set. This immediately implies the closure of HF under replacement.

Turning to power, we again first assume $x \in \mathit{FI}$ and want to show $\mathcal{P}x \in \mathit{FI}$. The first inductive case of $x \in \mathit{FI}$ is again easy since $\mathcal{P}\emptyset = \emptyset.\emptyset \in \mathit{FI}$. So now suppose we know $y \in \mathit{FI}$ as well as $\mathcal{P}y \in \mathit{FI}$ and want that $\mathcal{P}(x.y) \in \mathit{FI}$. To this end we show that $\mathcal{P}(x.y) = \mathcal{P}y \cup ((\lambda z.\, x.z)@\mathcal{P}y)$. This is finite since $\mathcal{P}y$ is so and FI is closed under replacement. Again, the corresponding closure of HF follows directly.

Finally, we assume $x \in \mathit{HF}$ and show $\bigcup x \in \mathit{HF}$. The first condition $\bigcup x \subseteq \mathit{HF}$ is trivial since $x \subseteq \mathit{HF}$. We verify the second condition $\bigcup x \in \mathit{FI}$ by induction on $x \in \mathit{FI}$. As before, the empty case is trivial given that $\bigcup \emptyset = \emptyset$. In the second case, we know that $x.y \subseteq \mathit{HF}$ and $\bigcup y \in \mathit{FI}$ and want to show that $\bigcup x.y \in \mathit{FI}$. Since $\bigcup x.y = x \cup (\bigcup y)$ we just have to show that x and $\bigcup y$ are finite, which follow from the assumptions. □

Lemma 9.5. *If $x \in \mathit{FI}$ is inhabited and a **chain**, i.e. for all $y, z \in x$ either $y \subseteq z$ or $z \subseteq y$, then $\bigcup x \in x$.*

Proof. This is by induction on $x \in \mathit{FI}$. The empty case is impossible since we assumed x to be inhabited. Hence we are in the situation where we know that $x.y$ is a chain for $y \in \mathit{FI}$. Now if y is inhabited the inductive hypothesis yields that $\bigcup y \in y$ and comparing $\bigcup y$ with x using the chain property of $x.y$ yields that $\bigcup x.y$ equals either $\bigcup y$ or x and is hence in any case element of $x.y$. If y is itself empty, however, we know that $\bigcup x.y = \bigcup \{x\} = x \in x.y$. □

Lemma 9.6. *Ω is a limit and agrees with HF.*

Proof. Note that Ω is a stage since $\mathcal{P}^n\,\emptyset$ is a stage for all $n : \mathbb{N}$, given that $\emptyset = \bigcup \emptyset$ is a stage. Now suppose that $x \in \Omega$, so $x \in \mathcal{P}^n\,\emptyset$ for some $n : \mathbb{N}$. Then $\mathcal{P}^n\,\emptyset \in \Omega$ since $\mathcal{P}^n\,\emptyset \in \mathcal{P}^{n+1}\,\emptyset$. Thus $\Omega \subseteq \bigcup \Omega$ and hence Ω is a limit.

We now show that Ω agrees with HF. If $x \in \Omega$, we know that $x \in \mathcal{P}^n\,\emptyset$ for some n and conclude $x \in \mathit{HF}$ given that $\mathcal{P}^n\,\emptyset \in \mathit{HF}$ by Fact 9.4. Conversely, let $x \in \mathit{HF}$. It suffices to show that $\rho\, x \in \Omega$ since Ω is a stage and hence swelled and we know $x \subseteq \rho x$. We show $\rho\, x \in \Omega$ by HF-induction on x, so we know $\rho\, y \in \Omega$ for all $y \in x$. We can further assume some $y \in x$ since, if x is empty, we have $\rho\, x = \emptyset \in \Omega$. Given these conditions, the set $X := (\mathcal{P} \circ \rho)@x$ is a finite inhabited chain and hence Lemma 9.5 yields the fact that $\bigcup X \in X$. Then by definition of X there is some $y \in x$ such that $\bigcup X = \mathcal{P}(\rho\, y)$. By the equation $\rho x = \bigcup(\mathcal{P} \circ \rho)@x = \bigcup X$ from the proof of Fact 8.2 we hence know that $\rho x = \mathcal{P}(\rho\, y)$. Since $y \in x$ we can apply the inductive hypothesis to get $\rho\, y \in \Omega$ but then finally $\rho\, x = \mathcal{P}(\rho\, y) \in \Omega$ since Ω is a limit and hence closed under taking power sets. □

Fact 9.7. *Ω is the least universe.*

Proof. We first show that Ω is a universe by applying Fact 8.3. We have already argued that Ω is a limit stage (Lemma 9.6) and since for instance $\emptyset \in \Omega$, it is clearly inhabited. The closure under relational replacement follows from Fact 9.4 given that Ω agrees with HF.

Concerning leastness, we show the slightly stronger result that Ω is the least inhabited limit. So let V be another inhabited limit. By linearity of stages, we know that either $V \in \Omega$ or $\Omega \subseteq V$. We show that the first case is contradictory. By Lemma 9.6 we know that $V \in \Omega$ implies that V is finite. However, as V contains $\emptyset$ and is closed under power, we have $\omega \subseteq V$ and so ω must be finite, too. But then Lemma 9.5 would imply $\bigcup \omega \in \omega$, so there is $n : \mathbb{N}$ with $\mathcal{P}^n\,\emptyset = \bigcup \omega = \Omega$ which in turn implies $\mathcal{P}^n\,\emptyset \in \mathcal{P}^n\,\emptyset$, contradicting Found. □

We can summarise the results of this section as follows:

Theorem 9.8. **ZF** *is equivalent to* $\mathbf{ZF}_{\geq 1}$.

Proof. The first direction follows from Fact 9.7 since then $\mathcal{P}\Omega$ has strength 1. For the converse, assume that $\mathcal{M} \models \mathbf{ZF}_{\geq 1}$, so there is a set $x : \mathcal{M}$ of strength 1 and hence a universe $U : \mathcal{M}$. Then $\omega := (\lambda x.\, \exists n : \mathbb{N}.\, x = \mathcal{P}^n\,\emptyset) \cap U$ witnesses Inf since U contains $\emptyset$ and is closed under taking power sets. □

10 Zermelo's Embedding Theorem

In this section, we switch to an external perspective and compare the structure of models. The main observation is the embedding theorem [18], stating that any two models are either isomorphic or one embeds as a universe into the other. A consequence is the categoricity of $\mathbf{ZF}_n$, meaning that all models of $\mathbf{ZF}_n$ are isomorphic. Both results were already proved in [8] and as we did in Section 8, we just sketch the adaption to our now slightly modified axiomatisation.

Definition 10.1. *For models $\mathcal{M}$ and $\mathcal{N}$ we define a binary inductive predicate $\approx : \mathcal{M} \to \mathcal{N} \to \mathrm{Prop}$ called **bisimilarity**:*

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

It follows by well-founded induction that $\approx$ is functional, injective and respects membership. Hence the embedding theorem follows if $\approx$ can be proved either total or bijective. In the case where $\approx$ is both total and bijective, we call $\mathcal{M}$ and $\mathcal{N}$ **isomorphic**.

Fact 10.2. *If a set $U : \mathcal{M}$ agrees with $\mathrm{dom}(\approx)$, then U is a universe. Similarly, if a set $U' : \mathcal{N}$ agrees with $\mathrm{ran}(\approx)$, then U' is a universe.*

Sketch. We just prove the first statement since the second follows by symmetry. So suppose that $U : \mathcal{M}$ agrees with $\mathrm{dom}(\approx)$. Since $\approx$ respects membership, it respects all set operations given that they are uniquely determined by their membership laws. Hence we know $\emptyset \approx \emptyset$ and properties such that, if $x \approx x'$, then $\bigcup x \approx \bigcup x'$, $\mathcal{P}x \approx \mathcal{P}x'$ and so on. Thus $\mathrm{dom}(\approx)$ is closed under all set operations and hence U is a universe. □

The embedding theorem is deduced using the structure of the cumulative hierarchy studied in Section 8:

Theorem 10.3. *Any two models of* **ZF** *are either isomorphic or* $\approx$ *embeds one as a universe into the other. That is, for models* $\mathcal{M}$ *and* $\mathcal{N}$ *one of the following holds:*
(1) $\mathcal{M}$ *and* $\mathcal{N}$ *are isomorphic*
(2) $\approx$ *is total and* $\mathsf{ran}(\approx)$ *is a universe in* $\mathcal{N}$
(3) $\approx$ *is surjective and* $\mathsf{dom}(\approx)$ *is a universe in* $\mathcal{M}$

Sketch. First suppose there were stages $V \notin \mathsf{dom}(\approx)$ and $V' \notin \mathsf{ran}(\approx)$. By the well-orderedness of stages (Fact 8.2) we can assume them to be the least such stages. However, then it follows that $V \approx V'$ and hence $\approx$ must exhaust the stages at least of one of both models.

If $\approx$ in fact exhausts the stages of both models, we can conclude (1) since the stages exhaust all sets. Otherwise, suppose that $\approx$ just exhausts the stages of $\mathcal{M}$. Then certainly $\approx$ is total but there is a stage $V' \notin \mathsf{ran}(\approx)$. It follows that $\mathsf{ran}(\approx) \subseteq V'$ and hence $\mathsf{ran}(\approx)$ is small. Thus we conclude (2) using Fact 10.2. The case (3) follows similarly if it were that $\approx$ just exhausts the stages of $\mathcal{N}$ □

It follows that the axiomatisations $\mathbf{ZF}_n$ are **categorical**, i.e. if models $\mathcal{M}$ and $\mathcal{N}$ both satisfy $\mathbf{ZF}_n$ then they are isomorphic. We hence may call the models of $\mathbf{ZF}_n$ unique, provided they exist.

Fact 10.4. $\mathbf{ZF}_n$ *is categorical for all* $n : \mathbb{N}$.

Sketch. Let $\mathcal{M}$ and $\mathcal{N}$ be models of $\mathbf{ZF}_n$. The embedding theorem (Theorem 10.3) admits three cases, whereof (1) yields the claim. Otherwise, if (2) holds, we have that $\mathsf{ran}(\approx) : \mathcal{N}$ 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. □

11 Model Truncation

We now study a truncation method for shrinking models of $\mathbf{ZF}_{\geq n}$ to submodels of $\mathbf{ZF}_n$. Together with the consistency of $\mathbf{ZF}_{\geq n}$ and the categoricity of $\mathbf{ZF}_n$ this implies that $\mathbf{ZF}_n$ has a unique model for all natural numbers $n : \mathbb{N}$.

Lemma 11.1. *If* $\mathcal{M} \models \mathbf{ZF}^*$ *and* $U \subseteq WF$ *is a ZF-closed class, then* $\mathcal{M}_U := \langle x : \mathcal{M} \mid x \in U \rangle$ *with the accordingly restricted set operations is a model of* **ZF**.

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

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

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

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

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 7.1) since the members of $\mathcal{M}_U$ carry proofs. Found follows from $U \subseteq WF$ and the membership axioms hold in $\mathcal{M}_U$ as they do in $\mathcal{M}$. Desc_1 is by construction of δ_U and Desc_2 by case analysis on whether or not the two assumed classes are singletons. □

The following ensures that the notion of universes and strength is preserved by submodels:

Lemma 11.2. *If* $\mathcal{M} \models \mathbf{ZF}$ *and* U *is a ZF-closed class over* $\mathcal{M}$, *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 11.3. *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 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 11.1 we know that $\mathcal{M}_U$ is a model of **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 $\mathcal{M}_U \models \mathbf{ZF}_n$. □

Turning back to the large model constructions in Section 6 (and assuming TD again), we conclude the meta-result that $\mathbf{ZF}_n$ is consistent:

Theorem 11.4. $\mathbf{ZF}_n$ *has a unique model for all* $n : \mathbb{N}$.

Proof. For $n : \mathbb{N}$, by the (informal) Theorem 6.7 we have a model of $\mathbf{ZF}_{\geq n}$. Then Fact 11.3 induces a submodel of $\mathbf{ZF}_n$ and uniqueness follows from Fact 10.4. □

12 Non-Well-Founded Models

By the nature of their inductive definitions, the tree models $\mathcal{T}_i$ and the derived set models $\mathcal{S}_i$ are well-founded. If they were not, the class *WF* would yield well-founded models following a standard argument.

Fact 12.1. *If* $\mathcal{M} \models \mathbf{ZF}^*$ *then* $\mathcal{M}_{WF} \models \mathbf{ZF}$.

Proof. We apply Lemma 11.1 and hence just have to prove that *WF* is ZF-closed. All defining properties are routine. □

The remainder of this section addresses the converse question, namely whether dependent type theory admits non-well-founded models at all and hence whether the axiom Found is independent from the other axioms. Indeed, the standard independence proof based on permutation models (cf. [6]) can be carried out concisely in type theory.

Definition 12.2. *Let $\mathcal{M} \models \mathbf{ZF}$ be a model and π be a permutation of $\mathcal{M}$, i.e. a function $\pi : \mathcal{M} \to \mathcal{M}$ with inverse π^{-1}. With the membership relation $x \in_\pi y := x \in (\pi\, y)$ we define the **permutation structure** $\mathcal{M}_\pi$ given by operations*

$$\begin{aligned} \emptyset_\pi &:= \pi^{-1}\,\emptyset & P \cap_\pi x &:= \pi^{-1}(P \cap (\pi\, x)) \\ \{x,y\}_\pi &:= \pi^{-1}(\{x,y\}) & F@_\pi x &:= \pi^{-1}(F@(\pi\, x)) \\ \bigcup_\pi x &:= \pi^{-1}(\bigcup(\pi@(\pi\, x))) & \delta_\pi P &:= \delta P \\ \mathcal{P}_\pi x &:= \pi^{-1}(\pi^{-1}@(\mathcal{P}(\pi\, x))) \end{aligned}$$

Fact 12.3. *$\mathcal{M}_\pi \models \mathbf{ZF}^*$ for every permutation $\pi : \mathcal{M} \to \mathcal{M}$.*

Proof. The extensionality of $\mathcal{M}_\pi$ follows trivially from the extensionality of $\mathcal{M}$. Moreover, Desc as well as most of the membership axioms are immediate consequences of the corresponding axioms of $\mathcal{M}$. Only Union and Power are slightly more complex as they are defined using replacement. □

Definition 12.4. *$(0\,1)$ is the permutation of $\emptyset$ and $\{\emptyset\}$.*

Note that the formal definition of $(0\,1)$ is carried out by defining a corresponding binary relation on $\mathcal{M}$, proving it functional and finally turning it into an actual function using the description operator δ. It then follows that $(0\,1)$ is a permutation violating Found.

Fact 12.5. $x \in_{(0\,1)} \emptyset \leftrightarrow x = \emptyset$

Proof. Let $x \in_{(0\,1)} \emptyset$, then by definition of $\in_{(0\,1)}$ we have $x \in (0\,1)\,\emptyset = \{\emptyset\}$. Hence we know $x = \emptyset$. The converse $\emptyset \in_{(0\,1)} \emptyset$ is immediate by $\emptyset \in \{\emptyset\}$. □

Sets with the property $x = \{x\}$ such as the one in Fact 12.5 are usually called **Quine sets** and constitute the simplest violation of foundation. With more involved permutations one could introduce much heavier violations such as cycles of arbitrary depth or a proper class of Quine sets. However, at this point we just draw the general conclusion that the axiom of foundation is independent:

Theorem 12.6. *$\mathbf{ZF}^*$ has a non-well-founded model.*

Proof. By Fact 12.3 the permutation structure $\mathcal{M}_{(0\,1)}$ is a model of $\mathbf{ZF}^*$ and by Fact 12.5 it contains a Quine set. □

13 Discussion

In this paper we have shown that Coq augmented by a (proof-irrelevant) description operator on well-founded trees proves strong versions of second-order ZF consistent. Further assuming excluded middle, we can control the height of the obtained models and prove the axiomatisations $\mathbf{ZF}_n$ [8] consistent. In comparison to prior work by Werner [17] and Barras [4] based on Aczel's interpretation of constructive set theory in type theory [1], we clarify that tree description rather than a full choice axiom is sufficient for the large model constructions. Moreover, we use the universe polymorphism implemented in Coq [13] in order to give a concise formalisation of the model hierarchy and the respective embeddings. An overview of all main results and their underlying assumptions is given in Table 1. The employed extensions of Coq and some general observations concerning formalisations of second-order ZF in constructive type theories are discussed in this final section.

Table 1. Overview of main results and axioms used.

Formal Statement	Axioms	#
$\mathcal{T}_i \models \mathbf{ZF}'_\equiv$	none	4.6
$\mathcal{S}'_i \models \mathbf{Z}$	CE, PI_1	5.4
$\mathcal{S}_i \models \mathbf{ZF}'$	CR, PI_2	5.8
$\mathcal{T}_i \models \mathbf{ZF}_\equiv$ and $\mathcal{S}_i \models \mathbf{ZF}$	TD, PI_2	5.9
$\forall n : \mathbb{N}.\, \exists \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}$	TD, PI_2	6.7
$\mathcal{M} \models \mathbf{ZF} \to (\forall x.\, x \in \Omega \leftrightarrow x \in HF)$	XM	9.6
$\mathcal{M} \models \mathbf{ZF} \to \mathcal{M} \models \mathbf{ZF}_{\geq 1}$	XM	9.8
$\mathcal{M} \models \mathbf{ZF}_{\geq 1} \to \mathcal{M} \models \mathbf{ZF}$	none	9.8
$(\exists \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}) \to (\exists \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_n)$	XM	11.3
$\forall n : \mathbb{N}.\, \exists! \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_n$	TD, XM	11.4
$\mathcal{M} \models \mathbf{ZF}^* \to \mathcal{M}_{WF} \models \mathbf{ZF}$	XM	12.1
$\mathcal{M} \models \mathbf{ZF} \to \mathcal{M}_{(0\,1)} \models \mathbf{ZF}^* + \neg\mathsf{Found}$	XM	12.6

Since Coq does not provide built-in quotient types, our construction of extensional models $\mathcal{S}$ relies on quotient axioms. As we have shown, just assuming classes to be extensional (CE) allows for lifting all set operations but replacement from $\mathcal{T}$ to the equivalence classes of tree equivalence $\equiv$. However, even assuming a full quotient type $\mathcal{T}/_\equiv$ with a mapping $[\_] : \mathcal{T} \to \mathcal{T}/_\equiv$ and the property that all functions $F : \mathcal{T} \to A$ that respect $\equiv$ can be decomposed into $\overline{F} \circ [\_]$ where $\overline{F} : \mathcal{T}/_\equiv \to A$ seems not to suffice to treat replacement. Only the strong assumption of canonical representatives (CR) allows for turning replacement functions on the quotient type $\mathcal{S}$ back into functions that are subject to the replacement operator of $\mathcal{T}$. In contrast, in alternative type theories such as homotopy type theory [15], a system coming with higher inductive types and the strong extensionality principle of univalence, extensional model constructions do not rely on additional quotient axioms [5, 10].

Relational replacement plays a crucial role in the development of ZF, e.g. in Section 8 it is necessary to prove that the stages exhaust all sets. More generally, relational replacement is closer to first-order set theory than the functional version, as the formulas $\phi(a,b)$ 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 our model construction.

The use of excluded middle in 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. Secondly, the truncation method (Fact 11.3) for cutting 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 those classical results. However, we emphasize that the consistency of the axiomatisations $\mathbf{ZF}_{\geq n}$ does not rely on excluded middle.

Universe polymorphism is a rather recent feature of Coq which has not been available for Werner's and Barras' work. Both were tied to defining several copies of the tree type with separate notions of equivalence and membership in order to study the resulting Grothendieck universes. Hence an iterated construction of arbitrary strength was not feasible. The universe-polymorphic definition of the tree types $\mathcal{T}_i$ makes the result accessible since the recursive embedding of smaller into larger copies can be defined simultaneously for all type levels. We remark that our presentation using concrete type levels differs from but is faithful to the treatment in Coq employing systems of constrained universe variables. If we were to define the notion of model strength on paper with the same external notion of natural numbers underlying the type levels, we could phrase the one-to-one correspondence of type and set universes as $\mathcal{S}_i \models \mathbf{ZF}_{\geq i}$.

As a consequence of Zermelo's quasi-categoricity result, all models of second-order ZF only differ in the ordinality of their universes. Intuitively, all set-theoretic propositions not referring to the height of the cumulative hierarchy evaluate equally in all models. Hence, contrarily to first-order ZF where the classical independence results apply, we cannot construct models of second-order ZF that evaluate properties such as the axiom of choice or the continuum hypothesis differently. Moreover, since the type-theoretical versions of these properties are believed to be independent from the theory underlying Coq and violations of the set-theoretical properties induce violations on type level, we expect that the second-order models discussed in this paper neither negate the axiom of choice nor the continuum hypothesis. This refines a statement given by Kreisel [9] that the continuum hypothesis is not independent from second-order ZF.

From this perspective it is worth emphasizing that, as we have shown in Section 12, the axiom of foundation can still be proved independent from the other axioms in the usual way. Starting with a non-well-founded model, the class *WF* forms a well-founded submodel and suitable permutations of well-founded models induce non-well-founded models. In contrast, due to the reasons mentioned above, all attempts to formalise the independence results of the axiom of choice and the continuum hypothesis, which are standard in first-order ZF, must fail for second-order ZF.

A natural idea for future work is to formalise first-order set theory relying on the notion of first-order definability of classes and relations and to study the then applicable classical independence proofs. Another direction we plan to investigate is to find type-theoretical versions of set-theoretical cardinality theorems such as the existence of arbitrarily large well-orders (due to Hartogs) or the deduction of choice from the generalised continuum hypothesis (due to Sierpinski). Both would involve developing suitable type-theoretical notions of ordinals and cardinals.

Acknowledgments

This research benefited from a quotient construction yielding the extensional models $\mathcal{S}_i$ 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] Peter Aczel. 1978. The Type Theoretic Interpretation of Constructive Set Theory. *Studies in Logic and the Foundations of Mathematics* 96 (Jan. 1978), 55–66.

[2] Peter Aczel. 1998. On Relating Type Theories and Set Theories. In *Types for Proofs and Programs (Lecture Notes in Computer Science)*. Springer, Berlin, Heidelberg, 1–18.

[3] Franco Barbanera and Stefano Berardi. 1996. Proof-irrelevance out of Excluded-middle and Choice in the Calculus of Constructions. *Journal of Functional Programming* 6, 3 (1996), 519–525.

[4] Bruno Barras. 2010. Sets in Coq, Coq in Sets. *Journal of Formalized Reasoning* 3, 1 (Oct. 2010), 29–48.

[5] Andrej Bauer, Jason Gross, Peter LeFanu Lumsdaine, Michael Shulman, Matthieu Sozeau, and Bas Spitters. 2017. The HoTT Library: A Formalization of Homotopy Type Theory in Coq. In *CPP 2017*. ACM, New York, NY, USA, 164–172.

[6] Paul Bernays. 1954. A System of Axiomatic Set Theory–Part VII. *The Journal of Symbolic Logic* 19, 2 (1954), 81–96.

[7] The Coq development team. 2009. *The Coq proof assistant reference manual*. LogiCal Project. http://coq.inria.fr/doc/

[8] Dominik Kirst and Gert Smolka. 2017. Categoricity Results for Second-Order ZF in Dependent Type Theory. In *ITP 2017, Brasília, Brazil, September 26-29, 2017 (LNCS)*, Mauricio Ayala-Rincón and César A. Muñoz (Eds.), Vol. 10499. Springer, 304–318. https://doi.org/10.1007/978-3-319-66107-0_20

[9] Georg Kreisel. 1969. Two notes on the foundations of set-theory. *Dialectica* 23, 2 (1969), 93–114.

[10] Jeremy Ledent. 2014. Modeling set theory in homotpy type theory. (2014). http://perso.ens-lyon.fr/jeremy.ledent/internship_report.pdf

[11] Lawrence C. Paulson. 1993. Set theory for verification: I. From foundations to functions. *Journal of Automated Reasoning* 11, 3 (01 Oct 1993), 353–389.

[12] Raymond M. Smullyan and Melvin Fitting. 2010. *Set Theory and the Continuum Problem*. Dover Publications.

[13] Matthieu Sozeau and Nicolas Tabareau. 2014. Universe Polymorphism in Coq. In *Interactive Theorem Proving (Lecture Notes in Computer Science)*. Springer, Cham, 499–514.

[14] P. Suppes. 1960. *Axiomatic Set Theory*. Dover Publications.

[15] The Univalent Foundations Program. 2013. *Homotopy Type Theory: Univalent Foundations of Mathematics*. https://homotopytypetheory.org/book, Institute for Advanced Study.

[16] Gabriel Uzquiano. 1999. Models of Second-Order Zermelo Set Theory. *The Bulletin of Symbolic Logic* 5, 3 (1999), 289–302.

[17] Benjamin Werner. 1997. Sets in Types, Types in Sets. In *Theoretical Aspects of Computer Software*. Springer, Heidelberg, 530–546.

[18] Ernst Zermelo. 1930. Über Grenzzahlen und Mengenbereiche: Neue Untersuchungen über die Grundlagen der Mengenlehre. *Fundamenta Mathematicæ* 16 (1930), 29–47.