The Generalised Continuum Hypothesis Implies the Axiom of Choice in Coq

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

Felix Rech
Saarland University
Saarland Informatics Campus, Saarbrücken, Germany
s9ferech@gmail.com

Abstract

We discuss and compare two Coq mechanisations of Sierpiński's result that the generalised continuum hypothesis (GCH) implies the axiom of choice (AC). The first version shows the result, originally stated in first-order ZF set-theory, for a higher-order set theory convenient to work with in Coq. The second version presents a corresponding theorem for Coq's type theory itself, concerning type-theoretic formulations of GCH and AC. Both versions rely on the classical law of excluded middle and extensionality assumptions but we localise the use of axioms where possible.

CCS Concepts: • **Theory of computation → Type theory**; *Constructive mathematics*; Higher order logic.

Keywords: dependent type theory, higher-order set theory, generalised continuum hypothesis, axiom of choice, Coq

ACM Reference Format:
Dominik Kirst and Felix Rech. 2021. The Generalised Continuum Hypothesis Implies the Axiom of Choice in Coq. In *Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP '21), January 18–19, 2021, Virtual, Denmark.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3437992.3439932

1 Introduction

An early but somewhat surprising result in axiomatic set theory states that the generalised continuum hypothesis (GCH) implies the axiom of choice (AC), already announced by Tarski in 1926 [27] and proven by Sierpiński in 1947 [35]. GCH, generalising Cantor's continuum hypothesis stating that there are no cardinalities between the set $\mathbb{N}$ of natural numbers and its power set $\mathcal{P}(\mathbb{N})$, rules out cardinalities between X and $\mathcal{P}(X)$ for every infinite X. Therefore, GCH narrows the range of the power set operation otherwise left rather underspecified by the usual Zermelo-Fraenkel (ZF) axioms. AC, in one typical set-theoretic formulation, states that every set X of non-empty sets admits a choice function f such that $f(x) \in x$ for all $x \in X$.

That GCH as a statement about power sets and cardinality implies AC, a statement providing a means to uniformly pick elements from non-empty sets, may seem surprising indeed [14]. However, since AC is equivalent to the well-ordering theorem (WO), asserting that every (infinite) set can be well-ordered, and since well-orders transport along injections, there is a well-established strategy how Sierpiński's result can be deduced. Intuitively, given an infinite set X, the intermediate step is to construct a well-ordered set $H(X)$, for instance the *Hartogs number* of X [18], which is not embeddable into X but bounded by a finite iteration of the power set on X, i.e. with $|H(X)| \not\leq |X|$ but $|H(X)| \leq |\mathcal{P}^k(X)|$ for some number k. Deducing $|X| \leq |H(X)|$ would now suffice in order to transport the well-order of $H(X)$ onto X and to conclude WO and thus AC. However, since cardinalities need not be comparable in the absence of AC, just $|H(X)| \not\leq |X|$ is not enough to deduce $|X| \leq |H(X)|$. Yet applying GCH on a suitable instance yields that either $|X| \leq |H(X)|$ as desired or $|H(X)| \leq |\mathcal{P}^{k-1}(X)|$, the latter allowing for iterating the argument ultimately terminating since $|H(X)| \not\leq |X|$.[1]

Sierpiński's theorem as a result in *first-order set theory* has been canonised in standard textbooks (e.g. [38], we follow their wording of "Sierpiński's theorem" for simplicity and are conscious of other results referred to by the same name) and in fact mechanised in Metamath by Carneiro [9].[2] In this paper, in contrast, we study Sierpiński's theorem as a statement in *higher-order set theory*, disposing of the need for first-order encodings, as well as in dependent type theory, disposing of the axiomatic framework altoghether, and provide respective mechanisations in Coq [42].[3]

As argued in a previous paper [24], higher-order set theory is a natural framework for mechanising set-theoretic results in proof assistants implementing a higher-order logic. Specifically, the ZF axiom scheme used to express replacement for

CPP '21, January 18–19, 2021, Virtual, Denmark

ACM ISBN 978-1-4503-8299-1/21/01…$15.00
https://doi.org/10.1145/3437992.3439932

[1] Sierpiński's original proof works with $k = 3$ and hence applies GCH three times. A proof applying GCH only twice was later given by Specker [40].
[2] See Section 8.3 for a more detailed comparison to Carneiro's work.
[3] Available at https://www.ps.uni-saarland.de/extras/sierpinski/.

every first-order formula $\phi(x, y)$ describing a functional relation can be condensed into a single axiom simply quantifying over all relations, not just the first-order definable ones. So in consequence there is no need to represent the syntax of first-order logic and the full expressivity of the meta-logic can be used. In particular regarding Sierpiński's theorem, every function on the meta-level can be encoded as a set-theoretic representation, which makes the central notion of cardinality coincide on both levels. This is a fundamental difference from first-order set theory, where, for instance, externally countable models with internally uncountable sets exist as noted early on by Skolem [36].

This simplification of axiom schemes, together with further streamlining of the foundation and infinity axioms, yields a higher-order version of ZF very convenient to work with in Coq. Therefore complementing [9], we give a compact Coq mechanisation using features like inductive predicates and recursive function definitions although still presenting the argument in its typical set-theoretic outline. Especially, this framework admits a notion of inductively characterised ordinals similar to the inductive treatment of the cumulative hierarchy in [24]. Going one step further, in the second part of the paper, we will contrast this set-theoretic development with a type-theoretic version of Sierpiński's result that does without any intermediate axiomatisation.

The fact that, if one interprets sets as types in a type universe $\mathbb{T}$, statements usually rendered in set theory have natural counterparts in dependent type theory (possibly extended with axioms regarding extensionality and classical logic) has been illustrated in many places, for instance in [19], [43], and [37] with type-theoretic versions of Zermelo's result that AC implies WO. In particular, type theories as implemented in Coq with its impredicative universe $\mathbb{P}$ of propositions, providing the necessary notions of anonymous propositional existence and power sets, are well-suited for such a *synthetic reformulation* of set-theoretic results.

In our case, we can formulate GCH in Coq by

$$\begin{aligned}\mathrm{GCH}_{\mathbb{T}} : \mathbb{P} \;:= \forall XY : \mathbb{T}.\, |\mathbb{N}| \leq |X| \leq |Y| \leq |X \to \mathbb{P}| \\ \to |Y| \leq |X| \vee |X \to \mathbb{P}| \leq |Y|\end{aligned}$$

where $|X| \leq |Y|$ now formally denotes the propositional existence of an injective function $f : X \to Y$, and AC by

$$\begin{aligned}\mathrm{AC}_{\mathbb{T}} : \mathbb{P} \;:= \forall XY : \mathbb{T}.\, \forall R : X \to Y \to \mathbb{P}.\, (\forall x.\, \exists y.\, Rxy) \\ \to \exists f : X \to Y.\, \forall x.\, Rx(fx)\end{aligned}$$

which is notably a proposition weaker than a type-level choice operator such as the one assumed in the Lean proof assistant. In contrast to the axiom of choice, the continuum hypothesis seems not to be a typical axiom in dependent type theory but is considered as a target for type-theoretic forcing in [20]. The consistency of both $\mathrm{AC}_{\mathbb{T}}$ and $\mathrm{GCH}_{\mathbb{T}}$ is justified by the standard set-theoretical interpretation of Coq's type theory [45], provided one works in a strong enough set theory satisfying AC and GCH itself.

Regarding the role of additional axioms, it is obvious that a result from classical set theory does not necessarily transport to Coq's constructive type theory directly. In fact, we will assume functional extensionality (FE), propositional extensionality (PE), and the law of excluded middle $\mathrm{LEM} := \forall P : \mathbb{P}.\, P \vee \neg P$ throughout this paper. Note that FE and PE together imply that predicates $p : X \to \mathbb{P}$ are determined by their elements and that both PE and LEM separately imply proof irrelevance (PI) and hence the existence of well-behaved subtypes $\Sigma x : X.\, px$. While FE and PE are only needed for the mentioned shortcuts and could possibly be circumvented, the necessity of LEM shall be subject of further investigation. Furthermore, we first give a proof variant relying on a unique choice operator (UC) to identify total functional relations with functions for a simplified presentation in alignment with the usual set-theoretic practice. That this requirement can be eliminated is shown afterwards.

The remaining text is organised as follows. We begin by introducing the general notions of cardinality and orderings in Section 2. Then, in the first part of the paper, the set-theoretic version of Sierpiński's theorem will be presented, with a focus on the representation of ordinals (Section 3) and the Hartogs numbers (Section 4). The second part then outlines the type-theoretic version, comprising the encoding of the Hartogs numbers as types (Section 5) and the remaining argument with (Section 6) and without (Section 7) employing UC. Both parts can be read independently, only the analogous conclusion of Sierpiński's theorem after constructing the Hartogs numbers is left out in the first part to avoid redundancy. We conclude with some remarks on the comparison of both versions, on their respective Coq mechanisations, as well as on related and future work in Section 8. All statements in this PDF version are hyperlinked with HTML documentation of the Coq development.

2 Cardinality and Well-Orderings

We use common notation for dependent product $\forall x.\, Fx$, dependent sum $\Sigma x.\, Fx$, (binary) product $X \times Y$, (binary) sum $X + Y$, and function types $X \to Y$ in the type universe (hierarchy) $\mathbb{T}$. In the universe $\mathbb{P}$ of propositions, we employ the usual logical notation for the corresponding notions. Moreover, we call $\mathcal{P}(X) := X \to \mathbb{P}$ the *power type* of X and define inclusion $p \subseteq q$ for predicates $p, q : \mathcal{P}(X)$ by $\forall x.\, px \to qx$.

We extend Coq's type theory with the propositional axioms for (simply typed) functional extensionality, propositional extensionality, and excluded middle:

$$\begin{aligned}\mathrm{FE} &:= \forall XY.\, \forall f, g : X \to Y.\, (\forall x.\, fx = gx) \to f = g \\ \mathrm{PE} &:= \forall PQ : \mathbb{P}.\, (P \leftrightarrow Q) \to P = Q \\ \mathrm{LEM} &:= \forall P : \mathbb{P}.\, P \vee \neg P\end{aligned}$$

We use FE and PE tacitly but indicate if LEM is needed in the label of each statement. FE and PE together induce predicate extensionality, proof irrelevance, and subtypes:

Fact 2.1. *The following statements hold.*

1. $\forall X.\, \forall pq : \mathcal{P}(X).\, (\forall x.\, px \leftrightarrow qx) \to p = q$
2. *Proof irrelevance* $\mathrm{PI} := \forall P : \mathbb{P}.\, \forall h, h' : P.\, h = h'$
3. *Elements* (x, h) *and* (x', h') *of* $\Sigma x.\, px$ *are equal if* $x = x'$.

Proof. We prove the three claims one by one.

1. From $\forall x.\, px \leftrightarrow qx$ we obtain $\forall x.\, px = qx$ by PE and thus $p = q$ by FE.
2. If $P : \mathbb{P}$ is inhabited, then $P = \top$ by PE. Thus P is a singleton since $\top$ is.
3. After eliminating $x = x'$ the proofs h and h' of px are equal by PI. □

Note that the latter justifies that we can identify elements (x, h) of a subtype $\Sigma x.\, px$ with x where convenient.

Having fixed the logical basis, we now first introduce injections, inducing cardinality comparisons $|X| \le |Y|$.

Definition 2.2. *A function* $f : X \to Y$ *is called* injective *if* $fx = fy$ *implies* $x = y$ *for all* $x, y : X$. *We write* $|X| \le |Y|$ *if there exists an injection from* X *to* Y.

Fact 2.3. $|X| \le |Y|$ *is a preorder respected by sums, products, and powers.*

Proof. All but the last are witnessed by the obvious constructions. If $f : X \to Y$ is injective, then $Fp := \lambda y.\, \exists x.\, px \wedge y = fx$ defines an injection from $\mathcal{P}(X)$ to $\mathcal{P}(Y)$. Indeed, assuming $Fp = Fq$ and w.l.o.g. px, we obtain $Fp(fx)$ and hence $Fq(fx)$. But then $fx = fx'$ for some x' with qx' and by injectivity of f we conclude qx. □

Fact 2.4. *For all* X *and* $p : X \to \mathbb{P}$ *we have* $|\Sigma x.\, px| \le |X|$ *and* $|X| \le |\mathcal{P}(X)|$.

Proof. The former is by injectivity of the first projection $\pi_1 : (\Sigma x.\, px) \to X$ given in (3) of Fact 2.1 and the latter is witnessed by $\lambda xy.\, x = y$. □

Employing the inductive type $\mathbb{N}$ of natural numbers, cardinality comparisons yield a natural definition of infinity:

Definition 2.5. *We call* X infinite *if* $|\mathbb{N}| \le |X|$.

Fact 2.6. *If* X *is infinite, then so is* $\mathcal{P}(X)$.

Proof. This holds by Fact 2.4 and transitivity. □

We next define bijections, inducing equipotency $|X| = |Y|$.

Definition 2.7. *A function* $f : X \to Y$ *is a* bijection *if it has an inverse* $g : Y \to X$. *We write* $|X| = |Y|$ *if there exists a bijection between* X *and* Y.

Note that $|X| = |Y|$ is indeed stronger than only requiring both $|X| \le |Y|$ and $|Y| \le |X|$ since the Cantor-Bernstein theorem for this setting relies on LEM [33] and likely even on unique choice since we are employing type-theoretic functions and not just total functional relations.

Fact 2.8. $|X| = |Y|$ *is an equivalence congruent for sums, products, and powers.*

Proof. The injections in Fact 2.3 have obvious inverses. □

Fact 2.9. $|X| = |Y|$ *implies* $|X| \le |Y|$.

Proof. Trivial since invertible functions are injective. □

Having established the relevant notion of cardinality, we now approach the second key notion involved in Sierpinski's theorem, namely (well-)orderings. We first consider inclusion as a canonical partial order on power types.

Fact 2.10. *Inclusion* $p \subseteq q$ *for* $p, q : \mathcal{P}(X)$ *is a partial order.*

Proof. Reflexivity and transitivity are trivial and antisymmetry holds by (1) of Fact 2.1. □

The missing property defining a well-order can be expressed abstractly via least elements for arbitrary (and possibly undecidable) inhabited predicates.

Definition 2.11. *Let* $R : X \to X \to \mathbb{P}$ *be a partial order. We say that* $x : X$ *is a* least element *of* $p : \mathcal{P}(X)$ *if* px *and if* Rxy *for all* $y : X$ *with* py. *We call* R *a* well-order *if it is* well-founded, *i.e. if for every inhabited* $p : \mathcal{P}(X)$ *there exists a least element.*

We also employ the related notion of strict well-orderings:

Definition 2.12. *Given a relation* $R : X \to X \to \mathbb{P}$, *we characterise its* accessible points $T_R : \mathcal{P}(X)$ *inductively by inferring* $T_R x$ *whenever* $T_R y$ *for all* y *with* Ryx:

$$\frac{\forall y.\, Ryx \to T_R y}{T_R x}$$

We call R *a* strict well-order *if it is transitive, trichotomous* $(\forall xy.\, Rxy \vee x = y \vee Ryx)$, *and terminating* $(\forall x.\, T_R x)$.

Given a strict well-order R, we refer to the propositional elimination principle of T_R as *well-founded induction* and to the computational elimination principle as *well-founded recursion.*

Employing LEM, one can easily verify the usual translations of well-orders R to strict well-orders $R'xy := Rxy \wedge x \neq y$ and, conversely, of strict well-orders S to well-orders $S'xy := Sxy \vee x = y$. Already without LEM, given that they yield least and not just minimal elements as frequently required, we can show that well-orders are linear:

Fact 2.13. *Well-orders* R *are linear, i.e.* $Rxy \vee Ryx$ *for all* x, y.

Proof. Given R and $x, y : X$, consider $pz := z = x \vee z = y$. Since p is obviously inhabited, we obtain a least element z. Since either $z = x$ or $z = y$, we obtain the expected comparisons Rxy or Ryx, respectively. □

Next, we show that well-orders transport along injections.

Fact 2.14. *If* X *has a (strict) well-order and* $|Y| \le |X|$, *then* Y *has a (strict) well-order.*

Proof. If R_X is a (strict) well-order on X and $f : Y \to X$ an injection, then it is easy to verify that $R_Y yy' := R_X(fy)(fy')$ is a (strict) well-order on Y. □

Finally, we introduce order embeddings and isomorphisms.

Definition 2.15. *Given two relations $R : X \to X \to \mathbb{P}$ and $S : Y \to Y \to \mathbb{P}$, a function $f : X \to Y$ is an* order embedding *if it is a morphism from R to S, i.e. if $Rxx' \leftrightarrow S(fx)(fx')$ for all $x, x' : X$. We write $X \preceq Y$ if there is an order embedding from X to Y for relations clear from the context.*

Fact 2.16. *$X \preceq Y$ is a preorder.*

Definition 2.17. *An order embedding $f : X \to Y$ is an* order isomorphism *if it has an inverse $g : Y \to X$. We call X and Y (strongly) isomorphic, written $X \approx Y$, if there is an order isomorphism for X and Y for relations clear from the context.*

Fact 2.18. *$X \approx Y$ is an equivalence relation.*

3 Ordinals in Higher-Order ZF

In this section, we axiomatise a higher-order set theory and develop the basic theory of ordinals. Concretely, we work in a fixed model of higher-order ZF (cf. [24]), i.e. we assume a type $\mathcal{S}$ with constants

$$
\begin{array}{rl}
\_ \in \_ : \mathcal{S} \to \mathcal{S} \to \mathbb{P} & \text{(membership)} \\
\emptyset : \mathcal{S} & \text{(empty set)} \\
\{\_,\_\} : \mathcal{S} \to \mathcal{S} \to \mathcal{S} & \text{(unordered pair)} \\
\bigcup : \mathcal{S} \to \mathcal{S} & \text{(union)} \\
\mathcal{P} : \mathcal{S} \to \mathcal{S} & \text{(power set)} \\
\_ \mathbin{@} \_ : \mathcal{F}(\mathcal{S}) \to \mathcal{S} \to \mathcal{S} & \text{(replacement)} \\
\omega : \mathcal{S} & \text{(natural numbers)}
\end{array}
$$

where $\mathcal{F}(\mathcal{S})$ denotes the type of functional relations of type $R : \mathcal{S} \to \mathcal{S} \to \mathbb{P}$. We call the elements $A, x : \mathcal{S}$ *sets* and predicates $p, q : \mathcal{S} \to \mathbb{P}$ *classes*, the latter borrowing the notation $A \in p$ for pA where convenient. Moreover, we frequently identify sets A with their corresponding classes $\lambda x.\, x \in A$ and classes p with their subtypes $\Sigma A.\, pA$. Similarly, we simply say that a class p is a set, if there is a set A with $p = \lambda x.\, x \in A$ or, with the above identification $p = A$.

In order to equip the introduced constants with their intended meaning, we assume that they are characterised by the following axioms:

$$
\begin{array}{rl}
\forall AB.\, A = B \leftrightarrow \forall x.\, x \in A \leftrightarrow x \in B & \text{(Extensionality)} \\
\forall A.\, A \notin \emptyset & \text{(Empty Set)} \\
\forall ABx.\, x \in \{A, B\} \leftrightarrow x = A \vee x = B & \text{(Pairing)} \\
\forall Ax.\, x \in \bigcup A \leftrightarrow \exists y \in A.\, x \in y & \text{(Union)} \\
\forall Ax.\, x \in \mathcal{P}(A) \leftrightarrow x \subseteq A & \text{(Power Set)} \\
\forall RAy.\, y \in R \mathbin{@} A \leftrightarrow \exists x \in A.\, Rxy & \text{(Replacement)} \\
\forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \sigma^n(\emptyset) & \text{(Infinity)} \\
\forall A.\, T_\in A & \text{(Foundation)}
\end{array}
$$

Here, $x \subseteq A$ is the usual notation for $\forall y.\, y \in x \to y \in A$ and the von Neumann successor $\sigma : \mathcal{S} \to \mathcal{S}$ is defined by $\sigma(A) := A \cup \{A\}$ where $A \cup B := \bigcup\{A, B\}$ and $\{A\} := \{A, A\}$.

Specifically the last three axioms are stronger than their first-order versions, in that first-order replacement only applies to functional relations R coinciding with a first-order formula $\phi(x, y)$, in that first-order infinity just asserts the existence of a set closed under $\emptyset$ and σ with no reference to the external type $\mathbb{N}$, and in that foundation is usually assumed in form of the weaker first-order regularity axiom. So every model of higher-order ZF satisfies the axioms of first-order ZF while the converse does not hold in general.

Note that the conditions under which such a higher-order model $\mathcal{S}$ exists in Coq's type theory are analysed in [45] and [26]. Also note that this axiomatisation is not minimal since the replacement axiom is strong enough to define $\emptyset$ from ω and unordered pairs from $\emptyset$ and power sets, the latter actually done in the Coq development. Given its expressiveness, replacement for arbitrary functional relations also yields separation, replacement for functions, and a description operator:

Lemma 3.1. *There are operations as follows.*

$$
\begin{array}{l}
\_ \cap \_ : (\mathcal{S} \to \mathbb{P}) \to \mathcal{S} \to \mathcal{S} \text{ s.t. } x \in p \cap A \leftrightarrow x \in A \wedge px \\
\_ \mathbin{@} \_ : (\mathcal{S} \to \mathcal{S}) \to \mathcal{S} \to \mathcal{S} \text{ s.t. } y \in f \mathbin{@} A \leftrightarrow \exists x \in A.\, y = fx \\
\delta : \forall p : \mathcal{S} \to \mathbb{P}.\, (\exists! A.\, pA) \to \Sigma A.\, pA
\end{array}
$$

Proof. The respective constructions can be given as follows:

- separation: $p \cap A := (\lambda xy.\, x = y \wedge px) \mathbin{@} A$
- function replacement: $f \mathbin{@} A := (\lambda xy.\, y = fx \wedge px) \mathbin{@} A$
- description: $\delta p := \bigcup(\lambda xy.\, py) \mathbin{@} \mathcal{P}(\emptyset)$ □

Note that functional replacement together with description is in fact equivalent to relational replacement, we choose the latter as axiom due to its proximity to the corresponding first-order axiom scheme. With functional replacement, we can define the common notation $\bigcup_{x \in A} fx := \bigcup(f \mathbin{@} A)$ for indexed union and for separation we will also use the more customary notation $\{x \in A \mid px\} := p \cap A$.

Before we continue, there is need to justify the reuse of the power type notation $\mathcal{P}(A)$ for power sets, leading to the core why higher-order ZF is more convenient to mechanise than first-order ZF.

Definition 3.2. *We call a type $X : \mathbb{T}$* set-like *if it can be encoded as a set, i.e. if there is a set $\overline{X} : \mathcal{S}$ with an encoding function $e_X : X \to \overline{X}$ that is injective and surjective.*[4]

Lemma 3.3 (LEM). *$\mathbb{N}$, every proposition $P : \mathbb{P}$, and $\mathbb{P}$ itself are set-like and if types X and Y are set-like, then so are $X \times Y$, $X + Y$, $X \to Y$, and $\mathcal{P}(X)$.*

Proof. The infinity axiom exactly states that ω is an encoding of $\mathbb{N}$ witnessed by the numeral function $e_{\mathbb{N}} := \lambda n.\, \sigma^n(\emptyset)$.

[4] Note that the stronger property $|X| = |\overline{X}|$ would require assuming a stronger elimination principle for $\mathcal{S}$ in most cases.

Similarly, the power set axiom ensures that the power set $\mathcal{P}(\overline{X})$ encodes the power type $\mathcal{P}(X)$, since predicates on X and subsets of $\overline{X}$ are in one-to-one correspondence due to the strong replacement axiom. Further overloading the type-level notations, the remaining encodings are standard using the Kuratowski ordered pairs $(x, y) := \{\{x\}, \{x, y\}\}$ for $\overline{X}\times\overline{Y}$, the disjoint union $\overline{X}+\overline{Y} := (\{\emptyset\}\times\overline{X})\cup(\{\{\emptyset\}\}\times\overline{Y})$, and the set-theoretic function space $\overline{X} \to \overline{Y} \subseteq \overline{X} \times \overline{Y}$ of total functional graphs. Finally, given $P : \mathbb{P}$, we define $\overline{P} := (\lambda x.\, P) \cap \{\emptyset\}$ with $e_P := \lambda h.\, \emptyset$ and $\overline{\mathbb{P}} := \{\emptyset, \{\emptyset\}\}$ with $e_{\mathbb{P}} := \lambda P.\, \overline{P}$. □

This means that the type-theoretic fragment relevant to state GCH and AC has a faithful representation within the assumed model $\mathcal{S}$ of higher-order ZF and all notions from Section 2 regarding cardinality and orderings carry over without need for reformulation. If $\mathcal{S}$ were just a model of first-order ZF, neither power types, function spaces, nor propositions could be shown set-like and the stricter first-order versions of these constructs and the related notions of cardinality and orderings were necessary to define. Sidestepping this problem, we freely reuse all type-theoretic notation and hide the particular encodings. The only statement concretely depending on a chosen encoding is the following:

Lemma 3.4. *$A \times A \subseteq \mathcal{P}^2(A)$ and hence $|A \times A| \leq |\mathcal{P}^2(A)|$.*

Proof. The elements $(x, y) \in A\times A$ are Kuratowski pairs of the form $\{\{x\}, \{x, y\}\}$ that are obviously subsets of $\mathcal{P}(A)$. □

Although formulated for sets here, the bound $|X \times X| \leq |\mathcal{P}^2(X)|$ can be analogously shown for arbitrary types X.

After having established the framework of higher-order set theory, we now introduce *ordinals*. As common in a set-theoretic foundation, ordinals are sets that serve two purposes. First, ordinals are well-ordered by the element relation and represent equivalence classes of well-ordered sets: for every well-ordered set, there is exactly one isomorphic ordinal. Secondly, we can regard ordinals as a generalisation of natural numbers that allows us to count beyond infinities: there is a zero element, a successor function, and, additionally, every set of ordinals has a least upper bound.

There are many possible definitions of ordinals but it seems difficult to find one that expresses both properties at once. We consider a definition that can only be formulated in a higher-order logic but is most convenient for our purposes. To this end, we use the notion of transitive sets.

Definition 3.5. *We call a set A* transitive *if for all sets x and y, whenever $x \in A$ and $y \in x$ then $y \in A$. In other words, a set is transitive if every element is also a subset.*

Definition 3.6. *We define the class O of* ordinals *inductively: an ordinal is a transitive set of ordinals, i.e. $\alpha \in O$ if α is transitive and $\alpha \subseteq O$.*

Note that this inductive definition of ordinals is not expressible in first-order ZF but remains an equivalent characterisation once one of the first-order encodings of ordinals is chosen as definition. Analogously, we prove our definition equivalent to a first-order characterisation (Fact 3.11) once we have established the expected ordering properties, where we only give the proofs that differ from the standard setting.

The transitivity condition is exactly what makes the element relation on the class of ordinals transitive. Moreoever, even if we didn't have the axiom of foundation, the inductive definition would imply that the element relation on ordinals is well-founded. So only trichotomy is needed to conclude:

Lemma 3.7 (LEM)**.** *The class O is strictly well-ordered by $\in$.*

Proof. Transitivity follows from transitivity of ordinals as sets and well-foundedness of the element relation on the class of ordinals follows by induction from the axiom of foundation.

To show trichotomy, we fix two ordinals α and β and need to deduce $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$. We apply well-founded induction on both, α and β. By LEM, we have that $\alpha = \beta$ or $\alpha \neq \beta$. The first case is trivial and in the second case we know that $\alpha \not\subseteq \beta$ or $\beta \not\subseteq \alpha$, yielding an ordinal $\gamma \in \alpha$ with $\gamma \notin \beta$ (or vice versa) suitable to apply the inductive hypothesis for. □

Thus as announced before, ordinals represent well-orders:

Lemma 3.8 (LEM)**.** *Every $\alpha \in O$ is strictly well-ordered by $\in$.*

Proof. Trivial since every ordinal is a subclass of O. □

Lemma 3.9. *Isomorphic ordinals are equal: $\alpha \approx \beta \to \alpha = \beta$.*

Proof. Fix $\alpha, \beta \in O$ with an isomorphism $f : \alpha \to \beta$. We apply well-founded induction on both. We need to show that $\alpha \subseteq \beta$ and $\beta \subseteq \alpha$. W.l.o.g., we focus on the former. So fix some $\xi \in \alpha$. It suffices to show that $\xi \approx f(\xi)$ since, by the inductive hypothesis on ξ, this implies $\xi = f(\xi) \in \beta$.

So consider the restriction $f|_\xi : \xi \to \beta$. This is actually a function $\xi \to f(\xi)$ since for all $x \in \xi$, we have $f(x) \in f(\xi)$ by the morphism property of f. As the inverse, we have $f^{-1}|_{f(\xi)}$. The function $f|_\xi$ is still a morphism since it is the restriction of a morphism. □

A characteristic property of ordinals is that membership and strict inclusion coincide, so the previous results hold for the latter as well.

Lemma 3.10 (LEM)**.** *For $\alpha, \beta \in O$ we have $\alpha \in \beta$ iff $\alpha \subsetneq \beta$.*

It is now easy to show the agreement of our inductive definition to a common first-order characterisation of ordinals as the transitive sets well-ordered by membership:

Fact 3.11 (LEM)**.** *The class O contains exactly the transitive sets α that are strictly well-ordered by $\in$ in the first-order sense, i.e. with $\in$-least elements for every non-emtpy subset of α.*

Proof. The first direction is straightforward with Lemma 3.8. For the converse direction, we can directly show that every $\beta \in \alpha$ is an ordinal employing the foundation axiom. □

One could proceed and also show that every well-ordered set has an isomorphic ordinal, its order type. But we do not need that fact and will not prove it here.

Instead, turning to the second announced property of ordinals, we briefly discuss how they generalise the natural numbers by deriving constructors as well as the respective elimination principle. These results are not needed to derive Sierpiński's theorem either but illustrate one alternative inductive characterisation of ordinals in higher-order ZF.

Lemma 3.12. 1. *The empty set is an ordinal.*
2. *The successor $\sigma(\alpha)$ of an ordinal α is an ordinal.*
3. *If A is a set of ordinals then $\bigcup A$ is an ordinal.*

Proof. 1. Both conditions are trivial since $\emptyset$ is empty.
2. Assume that α is an ordinal. We need to show that every element of α is a subset of $\sigma(\alpha)$ and an ordinal. Fix such an element x. By definition of the successor, $x = \alpha$ or $x \in \alpha$. The first case is trivial. In the second case, $x \subseteq \alpha \subseteq \sigma(\alpha)$ by transitivity of α and definition of the successor. Moreover, as an element of an ordinal, x is also an ordinal.
3. Fix a set of ordinals A. We need to show that every element of $\bigcup A$ is a subset of $\bigcup A$ and an ordinal. Fix such an element x. By the union axiom, there is an ordinal $\alpha \in A$, such that $x \in \alpha$. Then $x \subseteq \alpha \subseteq \bigcup A$ by transitivity of α. Moreover, as an element of an ordinal, x is also an ordinal. □

Since O contains $\emptyset$ and is closed under the successors, we can see by induction that it contains the encodings $\sigma^n(\emptyset)$ of all natural numbers $n : \mathbb{N}$. Note that these constructors could equally be taken as the inductive definition of ordinals, with Definition 3.6 then becoming a provable property.

The constructors that we provided are not disjoint since $\alpha = \bigcup \sigma(\alpha)$ for all α. To formulate useful elimination principles, we distinguish the ordinals that can only be constructed by the third constructor.

Definition 3.13. *A* limit ordinal *is an ordinal that is neither the empty set nor the successor of another ordinal. We use λ as an identifier that implicitly ranges over limit ordinals.*

It is easy to show that λ is a limit ordinal exactly iff it is non-empty and satisfies $\lambda = \bigcup_{\alpha \in \lambda} \alpha = \bigcup \lambda$. There are versions of this definition that include the empty set as a limit ordinal but it is standard to treat the empty set separately in the following transfinite induction principle.

Lemma 3.14 (LEM). *Fix a predicate $P : O \to \mathbb{P}$ as follows:*

- *The empty set satisfies P.*
- *If α satisfies P then the successor $\sigma(\alpha)$ satisfies P.*
- *If all elements of a limit λ satisfy P then λ satisfies P.*

Then every ordinal satisfies P.

Proof. By well-founded induction on $\in$ using the fact that every ordinal is either empty, a successor, or a limit. □

4 Sierpiński's Result in Higher-Order ZF

We now outline the set-theoretic proof of Sierpiński's theorem with a focus on the steps utilising ordinals. The remaining steps that agree with the type-theoretic proof are deferred to Section 6. We begin with the formal statements of the generalised continuum hypothesis and the axiom of choice in higher-order set theory.

$$\begin{aligned}\mathrm{GCH}_{\mathcal{S}} &:= \forall AB : \mathcal{S}.\, |\omega| \le |A| \le |B| \le |\mathcal{P}(A)| \\ &\quad \to |B| \le |A| \vee |\mathcal{P}(A)| \le |B|\end{aligned}$$

$$\begin{aligned}\mathrm{AC}_{\mathcal{S}} &:= \forall AB : \mathcal{S}.\, \forall R : A \to B \to \mathbb{P}.\, (\forall x.\, \exists y.\, Rxy) \\ &\quad \to \exists f : A \to B.\, \forall x : A.\, Rx(fx)\end{aligned}$$

Recall that we can use the type-level function space to state $\mathrm{GCH}_{\mathcal{S}}$ and $\mathrm{AC}_{\mathcal{S}}$ since, in higher-order set theory, it agrees with the set-level function space (Lemma 3.3). So in particular $\mathrm{GCH}_{\mathbb{T}}$ implies $\mathrm{GCH}_{\mathcal{S}}$ and $\mathrm{AC}_{\mathbb{T}}$ implies $\mathrm{AC}_{\mathcal{S}}$.

Fact 4.1. $\mathrm{AC}_{\mathcal{S}}$ *is equivalent to the statement that every set A of non-empty sets admits a choice function $f : A \to \bigcup A$ with $fx \in x$ for all x.*

Proof. For such a set A the relation $R : A \to \bigcup A \to \mathbb{P}$ given by $Rxy := y \in x$ is turned into a choice function $f : A \to \bigcup A$ by $\mathrm{AC}_{\mathcal{S}}$. Conversely, given a total relation $R : A \to B \to \mathbb{P}$, a choice function f for the range defined as $D := \{C \in \mathcal{P}(B) \mid \exists x \in A.\, C = Rx\}$ yields $g : A \to B$ with $Rx(gx)$ by setting $gx := f(Rx)$. □

A standard argument shows that the assumption that every set can be well-ordered ($\mathrm{WO}_{\mathcal{S}}$) implies $\mathrm{AC}_{\mathcal{S}}$.

Fact 4.2. $\mathrm{WO}_{\mathcal{S}}$ *implies* $\mathrm{AC}_{\mathcal{S}}$.

Proof. Given a total relation $R : A \to B \to \mathbb{P}$, a well-order on B, and an element $a \in A$, there exists a unique least element of Ra. The corresponding function $f : A \to B$ can be defined with the description operator δ. □

With this fact we are left to show that $\mathrm{GCH}_{\mathcal{S}}$ implies $\mathrm{WO}_{\mathcal{S}}$. To this end, we introduce the Hartogs numbers as a means to obtain arbitrarily large ordinals.

Definition 4.3. *The* Hartogs number *of a set A is the class*

$$\aleph(A) := \lambda\alpha \in O.\, |\alpha| \le |A|.$$

Once we have shown that the Hartogs number is an ordinal, then the crucial property $|\aleph(A)| \not\le |A|$ follows immediately from this definition because otherwise, the Hartogs number would contain itself. We proceed in three steps:

1. We show that $|\aleph(A)| \le |\mathcal{P}^6(A)|$.
2. We show that the Hartogs number is an ordinal.
3. We conclude that $\aleph(A) \not\le A$.

Fact 4.4 (LEM). $\aleph(A)$ *satisfies* $|\aleph(A)| \le |\mathcal{P}^6(A)|$.

Proof. Employing the bound for the cartesian product established in Lemma 3.4 twice, we deduce

$$\begin{aligned}|\mathcal{P}\,(\mathcal{P}(A)\times\mathcal{P}(A\times A))\,| &\le |\mathcal{P}\,\big(\mathcal{P}(A)\times\mathcal{P}^3(A)\big)\,|\\ &\le |\mathcal{P}\,\big(\mathcal{P}^3(A)\times\mathcal{P}^3(A)\big)\,|\\ &\le |\mathcal{P}^6(A)|.\end{aligned}$$

By transitivity, it suffices to define the injection

$$\begin{aligned}f &: \aleph(A)\to\mathcal{P}(\mathcal{P}(A)\times\mathcal{P}(A\times A))\\ f(\alpha) &:= \{x\in\mathcal{P}(A)\times\mathcal{P}(A\times A)\mid x\approx\alpha\},\end{aligned}$$

where we treat every $x\in\mathcal{P}(A)\times\mathcal{P}(A\times A)$ as a subset of A with a relation on it that might satisfy $x\approx\alpha$. To see that f is injective, fix two ordinals $\alpha,\beta\in\aleph(A)$ with $f(\alpha)=f(\beta)$. By definition of the Hartogs number, there is an injection $\alpha\to A$. We embed the order on α along this injection to obtain an $x\in\mathcal{P}(A)\times\mathcal{P}(A\times A)$. Note that $x\approx\alpha$. Therefore $x\in f(\alpha)=f(\beta)$ and hence $x\approx\beta$ by definition of f. Together, we have $\alpha\approx x\approx\beta$ which implies $\alpha=\beta$ since isomorphic ordinals are equal (Lemma 3.9). □

We could use a different encoding of ordered subsets to get the bound down to $\mathcal{P}^3(A)$ as illustrated in the type-theoretic variant of Sierpiński's theorem (cf. Section 5). In the presence of set-theoretic ordinals, however the above proof is charmingly compact and leaves the set-theoretic notion of orderings on A as subsets of $A\times A$ explicit.

We next show that the Hartogs number is an ordinal.

Lemma 4.5. *Classes p with $|p|\le|A|$ for some set A are sets.*

Proof. Fix an arbitrary class p and a set A with $|p|\le|A|$. By definition, we have an injection $f:p\to A$. Then the class p coincides with the set $(\lambda yx.\,y=fx)\,@\,A$. □

Corollary 4.6 (LEM)**.** *The Hartogs number $\aleph(A)$ of A is a set.*

Proof. This follows from the previous two lemmas. □

Fact 4.7 (LEM)**.** *The Hartogs number $\aleph(A)$ of A is an ordinal.*

Proof. We know that the Hartogs number $\aleph(A)$ contains only ordinals by definition and that it is a set by the previous corollary. It hence remains to show that the Hartogs number is transitive. Fix two ordinals α and β with $\beta\in\alpha\in\aleph(A)$. Our goal is to prove that $\beta\in\aleph(A)$. By definition of the Hartogs number, we have $|\alpha|\le|A|$ and need to show $|\beta|\le|A|$. From $\beta\in\alpha$ we obtain $\beta\subseteq\alpha$ and thus already $|\beta|\le|\alpha|$. □

Theorem 4.8 (LEM)**.** *For all sets A, we have $\aleph(A)\not\le A$.*

Proof. Assume that $\aleph(A)\le A$. By definition of $\aleph(A)$, we get the contradiction $\aleph(A)\in\aleph(A)$. □

Theorem 4.9 (LEM)**.** $\mathrm{GCH}_{\mathcal{S}}$ *implies* $\mathrm{WO}_{\mathcal{S}}$.

Corollary 4.10 (LEM)**.** $\mathrm{GCH}_{\mathcal{S}}$ *implies* $\mathrm{AC}_{\mathcal{S}}$.

We leave Theorem 4.9 without proof here since the remaining argument is completely analogous to the type-theoretic version presented in Section 6, Theorem 6.7. In order to prepare this result, we first discuss in the next section a way to represent the Hartogs numbers in type theory.

5 Hartogs Numbers in Coq's Type Theory

Turning to the second part concerned with a type-theoretic version of Sierpiński's theorem, we begin with a construction of arbitrarily large well-ordered types. More precisely, we fix a type X and construct a type $H(X)$ such that $H(X)$ is well-ordered and $|H(X)|\not\le|X|$ but $|H(X)|\le|\mathcal{P}^3(X)|$. In contrast to set-theory, Coq's type theory lacks a canonical notion of ordinals natural to work with and so we directly work on a representation of the well-orders of subsets of X. This time we opt for the tighter representation with $|H(X)|\le|\mathcal{P}^3(X)|$ compared to the previous bound $|\aleph(A)|\le|\mathcal{P}^6(A)|$ since in a type-theoretic setting both are equally indirect. The idea is to consider inclusion $p\subseteq q$ for predicates $p,q:\mathcal{P}(X)$ to isolate the well-founded orders $P,Q:\mathcal{P}^2(X)$ and their corresponding equivalence classes $\alpha,\beta:\mathcal{P}^3(X)$.

As done with sets and classes before, we continue on identifying predicates $p:\mathcal{P}(Y)$ on a type Y with their subtypes $\Sigma y.\,py$. So in particular we are able to apply the abstract notions of well-orders, embeddings, and isomorphisms introduced in Section 2 to $P,Q:\mathcal{P}^2(X)$ ordered by inclusion. In this particular setting, we moreover establish the following properties regarding embeddability.

Fact 5.1. *If $P\preceq Q$ and Q is well-founded, then so is P.*

Proof. Suppose that f embeds P into Q and that Q is well-founded. Then for some inhabited $P'\subseteq P$ we obtain that $Q':=\lambda q.\,\exists p.\,P'p\wedge q=fp$ is included in Q and inhabited as well. Hence it contains a least element q which is fp for some p with $P'p$ and since f respects inclusion it is straightforward to show that p is indeed least in P'. □

Fact 5.2. *If $P\subseteq Q$ then $P\preceq Q$.*

Complementing the notion of strong isomorphism $P\approx Q$, we consider a weaker notion easier to show constructively.

Definition 5.3. *We say that P and Q are* weakly isomorphic, *written $P\sim Q$, if both $P\preceq Q$ and $Q\preceq P$.*

Fact 5.4. *$P\approx Q$ implies $P\sim Q$ and both $P\approx Q$ and $P\sim Q$ respect well-foundedness.*

Proof. If f is an isomorphism between P and Q, then it is an embedding witnessing $P\preceq Q$ and its inverse is an embedding witnessing $Q\preceq P$. Moreover, f respects well-foundedness by Fact 5.1. □

We will later see that also $P\sim Q$ implies $P\approx Q$ (employing LEM). Furthermore (and without referring to additional axioms), it suffices to come up with relational embeddings and isomorphisms to establish $P\preceq Q$ and $P\approx Q$, respectively:

Lemma 5.5. *Assume $R : P \to Q \to \mathbb{P}$ such that $p \subseteq p' \leftrightarrow q \subseteq q'$ whenever Rpq and $Rp'q'$. If R is total, then $P \preceq Q$ and if, additionally, R is surjective, then $P \approx Q$.*

Proof. Let R be total. If we were to assume some form of unique choice, we could directly reify R into a function. However, even without unique choice we can simulate this reification since the codomain is a power type. We define $f' : P \to \mathcal{P}(X)$ by $f'p := \lambda x. \forall q. Qq \to Rpq \to qx$. First, we show that $Q(f'p)$ for all p. Indeed, since R is total, we have Rpq for some q with Qq and can show $f'p = q$ relying on the fact that R respects inclusion and is hence functional. Then f' can be lifted to a function $f : P \to Q$ respecting inclusion since R does. Moreover, if R is also surjective, we symmetrically obtain an embedding $g : Q \to P$ that is easily verified to invert f. □

This is an instance of the more general fact that total functional relations with a power type as codomain can be turned into functions constructively.

We next introduce the notion of initial segments and establish the characteristic property that well-orders do not embed into their initial segments.

Definition 5.6. *Given $P : \mathcal{P}^2(X)$, we define* initial segments *$P{\downarrow} : \mathcal{P}(X) \to \mathcal{P}^2(X)$ by $P{\downarrow}p := \lambda q. Pq \wedge q \subseteq p \wedge p \nsubseteq q$.*

Lemma 5.7. *If $P : \mathcal{P}^2(X)$ is well-founded, then so is $P{\downarrow}p$.*

Proof. Straightforward since $P{\downarrow}p \subseteq P$. □

Fact 5.8. *We always have $P{\downarrow}p \preceq P$. Contrarily, $P \not\preceq P{\downarrow}p$ if P is well-founded and Pp.*

Proof. $P{\downarrow}p \preceq P$ follows from Fact 5.2. Now suppose P is well-founded with $P \preceq P{\downarrow}p'$ for some p' with Pp'. By well-foundedness, there is a least element p with this property. However, if f witnesses the embedding of P into $P{\downarrow}p$, then iterating f twice witnesses $P \preceq P{\downarrow}(fp)$ and hence $p \subseteq fp$, contradicting $P{\downarrow}p(fp)$. □

Moreover, embeddability of segments is reflected by $\subseteq$.

Lemma 5.9 (LEM)**.** *If $P : \mathcal{P}^2(X)$ is well-founded with Pp and Pq, then $p \subseteq q \leftrightarrow P{\downarrow}p \preceq P{\downarrow}q$.*

Proof. From $p \subseteq q$ we obtain $P{\downarrow}p \subseteq P{\downarrow}q$ and hence $P{\downarrow}p \preceq P{\downarrow}q$. Conversely, let $P{\downarrow}p \preceq P{\downarrow}q$ and, employing LEM, suppose $p \nsubseteq q$. Then by linearity of P we have $q \subseteq p$ and thus $P{\downarrow}q = (P{\downarrow}p){\downarrow}q$. But then $P{\downarrow}p \preceq (P{\downarrow}p){\downarrow}q$ in conflict with Fact 5.8 □

We now proceed to the *embedding theorem*, stating that well-orders are comparable. Afterwards, this will be the main ingredient to show that the type of well-orders internal to X is itself well-ordered (Theorem 5.13).

Theorem 5.10 (LEM)**.** *If $P : \mathcal{P}^2(X)$ and $Q : \mathcal{P}^2(X)$ are well-founded, then either P and Q are strongly isomorphic or one of them embeds into a proper initial segment of the other:*

$$P \approx Q \vee (\exists q. Qq \wedge P \approx Q{\downarrow}q) \vee (\exists p. Pp \wedge Q \approx P{\downarrow}p)$$

Proof. We employ the relation $p \approx q := Pp \wedge Qq \wedge P{\downarrow}p \approx Q{\downarrow}q$. It is a morphism for inclusion by Fact 5.2, so for its domain $\mathsf{dom} := \lambda p. \exists q. p \approx q$ and range $\mathsf{ran} := \lambda q. \exists p. p \approx q$ it induces an isomorphism $\mathsf{dom} \approx \mathsf{ran}$ via Lemma 5.5. We now employ LEM to distinguish four cases.

- If $\mathsf{dom} = P$ and $\mathsf{ran} = Q$ we can conclude $P \approx Q$.
- If $\mathsf{dom} = P$ but there is q with Qq and $\neg\mathsf{ran}\, q$, we may assume that q is the least such element. It suffices to show that $Q{\downarrow}q = \mathsf{ran}$ since then $P \approx Q{\downarrow}q$ as wished. First, if $(Q{\downarrow}q)\, q'$ we get a the contradiction $q \subseteq q'$ if it were $\neg\mathsf{ran}\, q'$. Conversely, if $\mathsf{ran}\, q'$ we have to justify $q' \subseteq q$ and $q \nsubseteq q'$. The latter holds since $q \nsubseteq q'$ would imply that $\mathsf{ran}\, q$ since ran is downwards closed and then the former follows with linearity.
- This is analogous to the previous case.
- If there are (least) p and q in Q and P but not in ran and dom, respectively, we similarly obtain that $P{\downarrow}p \approx Q{\downarrow}q$. But then $\mathsf{ran}\, p$ and $\mathsf{dom}\, q$, contradiction. □

Corollary 5.11 (LEM)**.** *$P \sim Q$ implies $P \approx Q$.*

Proof. Assume $P \sim Q$. By Theorem 5.10 we obtain either $P \approx Q$ as claimed or w.l.o.g. $P \approx Q{\downarrow}q$ for some q with Qq. But then from $P \sim Q$ we have $Q \preceq P$ and hence $Q \preceq Q{\downarrow}q$ with Fact 5.4, in contradiction to Fact 5.8. □

We can now introduce the notion of (small) ordinals internal to X as equivalence classes of well-orders and prove that they are indeed well-ordered by embeddability.

Definition 5.12. *We call sets of orderings $\alpha : \mathcal{P}^3(X)$ an* ordinal *if $\alpha = [P] := (\lambda Q. P \sim Q)$ for some well-founded P. We further define the canonical ordering on ordinals by*

$$\alpha \leq \beta := \exists P, Q. \alpha P \wedge \beta Q \wedge P \preceq Q$$

and denote the ordinal subtype of $\mathcal{P}^3(X)$ by $H(X)$.

Theorem 5.13 (LEM)**.** *$H(X)$ is well-ordered by $\alpha \leq \beta$.*

Proof. We prove the necessary properties separately.

- Reflexivity and transitivity follow directly from the corresponding facts about order embeddings.
- For antisymmetry, suppose α and β are the equivalence classes of P and Q, respectively. Then from $\alpha \leq \beta$ and $\beta \leq \alpha$ we obtain $P \sim Q$ and thus $\alpha = \beta$.
- Let $A : \mathcal{P}^4(X)$ be an inhabited set of ordinals, i.e. there is $\alpha = [P]$ with $A\alpha$. Now using LEM, either α is already least or there is Q such that $A\beta$ for $\beta = [Q]$ with $P \not\sim Q$. Then by the embedding theorem (Theorem 5.10) we obtain p with Pp such that $Q \approx P{\downarrow}p$. Since P is well-founded, we can further assume that p is the least element with $A[P{\downarrow}p]$.
  We now claim that $[P{\downarrow}p]$ is the least element of A, so for any $\gamma = [R]$ with $A\gamma$ we need to show that $P{\downarrow}p \preceq R$. Suppose otherwise, then again using Theorem 5.10 we obtain that $R \approx (P{\downarrow}p){\downarrow}r = P{\downarrow}r$ for some r with $(P{\downarrow}p)\, r$, contradicting the leastness of p. □

We conclude this section by proving the expected properties regarding the cardinality of $H(X)$.

Theorem 5.14 (LEM). *$H(X) \not\leq X$ but $H(X) \leq \mathcal{P}^3(X)$.*

Proof. The latter follows directly from Fact 2.4. For the former, suppose there were an injection $F : H(X) \to X$. Intuitively, we can derive a contradiction since F induces a (partial) well-order in X that is too big to be accommodated.

Formally, consider $P_F := \lambda p.\, \exists \alpha.\, p = \alpha_\downarrow$ where $\alpha_\downarrow := \lambda x.\, \forall \beta.\, F\beta = x \to \beta \leq \alpha$. Clearly P_F inherits the well-foundedness from $H(X)$, so $\alpha_F := [P_F]$ is an ordinal. Moreover, it is easy to verify that $\alpha \leq \beta \leftrightarrow \alpha_\downarrow \subseteq \beta_\downarrow$, so α_F is isomorphic to the full order on $H(X)$. But then we can show that $P_F \leq P_F{\downarrow}\,\alpha_{F\downarrow}$ witnessed by the function $\lambda p.\, [P{\downarrow}\,p]_\downarrow$ in contradiction to Fact 5.8. □

6 Sierpiński's Result in Coq's Type Theory

In this section, we show that for $\mathrm{GCH}_\mathbb{T}$ and $\mathrm{AC}_\mathbb{T}$ as defined in the introduction, the former implies the latter. Like in the set-theoretic version, we now factor through the well-ordering theorem $\mathrm{WO}_\mathbb{T}$ quantifying over all types by showing that every type X embeds into $H(Y)$ for suitable Y. For the sake of easy definitions of the necessary injections and bijections, we assume a unique choice operator as follows.

$$\mathrm{UC} := \forall X.\, \forall p : X \to \mathbb{P}.\, (\exists! x.\, px) \to \Sigma x.\, px$$

As done with LEM, we will make explicit which statements rely on UC but also show in the next section how to proceed without this assumption. Notably, both assumptions together yield an informative variant of excluded middle.

Fact 6.1 (LEM,UC). *$\mathrm{IEM} := \forall P : \mathbb{P}.\, P + \neg P$ holds.*

Proof. Given $P : \mathbb{P}$ and employing LEM we can show that the predicate $p : \mathbb{B} \to \mathbb{P}$ defined by $p\,\mathrm{tt} := P$ and $p\,\mathrm{ff} := \neg P$ is inhabited. This propositional $\exists$-witnesses cannot be analysed to decide $P + \neg P$ yet but with UC we can turn it into an informative Σ-witness admitting the needed elimination. □

We begin with some elementary bijections concerning the type $\mathbb{B}$ of booleans and the unit type $\mathbb{1}$ needed later.

Fact 6.2. *There are bijections as follows:*

$$|X + X| = |\mathbb{B} \times X| \qquad |\mathbb{N}| = |\mathbb{1} + \mathbb{N}|$$
$$|X| = |\mathbb{1} \to X| \qquad |\mathcal{P}(X + Y)| = |\mathcal{P}(X) \times \mathcal{P}(Y)|$$

Proof. All are obvious, the lower two of course rely on FE. □

Crucial for the proof of Sierpiński's theorem is a criterion for types X satisfying $|X| = |X + X|$. In the presence of AC, this holds for all infinite X. Without AC, we can still obtain this bijection for the power $\mathcal{P}(X)$ of infinite X. To prepare this result, we state some further bijections relying on UC.

Fact 6.3 (LEM,UC). *Assume a predicate $p : X \to \mathbb{P}$ and an injection $f : X \to Y$. There are bijections as follows:*

$$|\mathbb{B}| = |\mathbb{P}| \quad |X| = |\Sigma x.\, px + \Sigma x.\, \neg px| \quad |X| = |\Sigma y.\, \exists x.\, y = fx|$$

Proof. We introduce the three bijections separately.

- The trivial injection defined by $g\,\mathrm{tt} := \top$ and $g\,\mathrm{ff} := \bot$ can be inverted with IEM.
- The easy injection is $(\Sigma x.\, px + \Sigma x.\, \neg px) \to X$ just projecting out the witness. For the inverse we need IEM to decide $px + \neg px$ for a given x.
- The injection $X \to \Sigma y.\, \exists x.\, y = fx$ just supplements fx with the trivial proof of $\exists x'.\, fx = fx'$. We need UC to extract the (unique) preimage from an element y with $\exists x.\, y = fx$. □

The first key lemma $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$ for infinite X is now provable by composing the bijections established.

Lemma 6.4 (LEM,UC). *If X is infinite, then $|X| = |\mathbb{1} + X|$ and $|\mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)|$.*

Proof. Let $f : \mathbb{N} \to X$ be injective and let $rx := \exists n.\, x = fn$ denote its range. Then we deduce:

$$\begin{aligned} |X| &= |\Sigma x.\, rx + \Sigma x.\, \neg rx| = |\mathbb{N} + \Sigma x.\, \neg rx| \\ &= |\mathbb{1} + \mathbb{N} + \Sigma x.\, \neg rx| = |\mathbb{1} + \Sigma x.\, rx + \Sigma x.\, \neg rx| = |\mathbb{1} + X| \end{aligned}$$

Employing this fact, we further deduce:

$$\begin{aligned} |\mathcal{P}(X)| &= |\mathcal{P}(\mathbb{1} + X)| = |\mathcal{P}(\mathbb{1}) \times \mathcal{P}(X)| = |(\mathbb{1} \to \mathbb{B}) \times \mathcal{P}(X)| \\ &= |\mathbb{B} \times \mathcal{P}(X)| = |\mathcal{P}(X) + \mathcal{P}(X)| \end{aligned}$$

Note the LEM and UC were needed only due to Fact 6.3 used to obtain the first claim. □

The second key lemma states that for "big enough" X an injection of $\mathcal{P}(X)$ into $X + Y$ already induces an injection of $\mathcal{P}(X)$ into Y. This holds intuitively since, given Cantor's theorem, X alone cannot contribute enough to the size of $X + Y$ to accommodate $\mathcal{P}(X)$.

Fact 6.5. *For every functional relation $R : X \to \mathcal{P}(X)$ one can construct some $p : \mathcal{P}(X)$ with $\neg Rxp$ for all x.*

Proof. By the diagonalisation $p := \lambda x.\, \forall q.\, Rxq \to \neg qx$. □

Lemma 6.6. *If $|\mathcal{P}(X)| \leq |X + Y|$ and $|X + X| \leq |X|$, then already $|\mathcal{P}(X)| \leq |Y|$.*

Proof. We first deduce $|\mathcal{P}(X) \times \mathcal{P}(X)| = |\mathcal{P}(X + X)| \leq |\mathcal{P}(X)| \leq |X + Y|$ using Fact 2.3 for the second step. Let this be witnessed by an injection $f : \mathcal{P}(X) \times \mathcal{P}(X) \to X + Y$. Then we can define a relation $R : X \to \mathcal{P}(X) \to \mathbb{P}$ by $Rxp := \exists q.\, f(p, q) = i_1 x$. Using Cantor's theorem (Fact 6.5) there is p_c such that $\forall x.\, \neg Rxp_c$.

We can now define an injection $g' : \mathcal{P}(X) \to X + Y$ by $g'q := f(p_c, p)$ and observe that for every q it must be $g'q = i_2 y$ for some y since if it were $g'q = i_1 x$ for some x we would obtain Rxp_c. Thus g' can easily be refined to an injection $g : \mathcal{P}(X) \to Y$. □

With this second key lemma in place, we are now prepared to establish the implication from $\mathrm{GCH}_\mathbb{T}$ to $\mathrm{WO}_\mathbb{T}$.

Theorem 6.7 (LEM,UC). $\mathrm{GCH}_{\mathbb{T}}$ *yields* $|X| \le |H(\mathcal{P}(\mathbb{N}+X))|$, *so* X *can be well-ordered. Thus* $\mathrm{GCH}_{\mathbb{T}}$ *implies* $\mathrm{WO}_{\mathbb{T}}$.

Proof. First note that $\mathbb{N} + X$ is infinite by injectivity of $i_1 : \mathbb{N} \to \mathbb{N} + X$ and hence so is $X' := \mathcal{P}(\mathbb{N} + X)$ by Fact 2.6. Moreover, due to Lemma 6.4, X' satisfies the following:

$$(*) \;:\; \forall n.\, |\mathcal{P}^n(X') + \mathcal{P}^n(X')| \le |\mathcal{P}^n(X')|$$

We now show that every infinite Y satisfying $(*)$ in place of X' with $|H(Y)| \le |\mathcal{P}^k(Y)|$ satisfies $|Y| \le |H(Y)|$ by induction on k. The original claim follows since then $|X| \le |X'| \le |H(X')|$ given that $|H(X')| \le |\mathcal{P}^3(X')|$ by Theorem 5.14.

So first considering $k = 0$ we would have $|H(Y)| \le |Y|$ in direct conflict with Theorem 5.14. Next considering $k = k'+1$ with $|H(Y)| \le |\mathcal{P}^k(Y)|$ we observe

$$|\mathcal{P}^{k'}(Y)| \le |\mathcal{P}^{k'}(Y) + H(Y)| \le |\mathcal{P}^k(Y)|$$

given that $|\mathcal{P}^{k'}(Y) + H(Y)| \le |\mathcal{P}^k(Y) + \mathcal{P}^k(Y)| \le |\mathcal{P}^k(Y)|$ using $(*)$ for k in the last step. We can now apply GCH to this situation and obtain two cases:

- If $|\mathcal{P}^{k'}(Y) + H(Y)| \le |\mathcal{P}^{k'}(Y)|$ we can derive $|H(Y)| \le |\mathcal{P}^{k'}(Y) + H(Y)| \le |\mathcal{P}^{k'}(Y)|$ and thus conclude $|Y| \le |H(Y)|$ with the inductive hypothesis for k'.
- If $|\mathcal{P}^k(Y)| \le |\mathcal{P}^{k'}(Y) + H(Y)|$ we obtain $|\mathcal{P}^k(Y)| \le |H(Y)|$ from Lemma 6.6 using $(*)$ for k' and thus conclude $|Y| \le |H(Y)|$. □

Finally, we complete the proof of Sierpiński's theorem with the type-theoretic variant of the fact that the well-ordering theorem implies the axiom of choice.

Fact 6.8 (UC). $\mathrm{WO}_{\mathbb{T}}$ *implies* $\mathrm{AC}_{\mathbb{T}}$.

Proof. Analogous to Fact 4.2 using UC in place of δ. □

Corollary 6.9 (LEM,UC). $\mathrm{GCH}_{\mathbb{T}}$ *implies* $\mathrm{AC}_{\mathbb{T}}$.

7 Eliminating Unique Choice

We now outline how to reformulate the development in the previous section to avoid UC and refer to the Coq mechanisation for full detail. Recall that the necessity for UC stems from the notion of injections and bijections based on type-theoretic functions, which already renders the bijections in Fact 6.3 undefinable. As a remedy, we now weaken these notions to total functional relations.

Definition 7.1. *We write* $|X| \le_r |Y|$ *if there is a total functional and injective relation* $R : X \to Y \to \mathbb{P}$ *and* $|X| =_r |Y|$ *if* R *is surjective in addition.*

It is clear that $|X| \le |Y|$ and $|X| = |Y|$ imply $|X| \le_r |Y|$ and $|X| =_r |Y|$, respectively, and that the converse directions hold in the presence of UC. Also, it is easy to verify that the relational variants are still respected by sums, products, and powers. Moreover, now the crucial bijections in Fact 6.3 only rely on LEM while injections still transport well-orders:

Fact 7.2 (LEM). *Assume a predicate* $p : X \to \mathbb{P}$ *and an injection* $f : X \to Y$. *There are relational bijections* $|\mathbb{B}| =_r |\mathbb{P}|$, $|X| =_r |\Sigma x.\, px + \Sigma x.\, \neg p|$, *and* $|X| =_r |\Sigma y.\, \exists x.\, y = fx|$.

Proof. It is straightforward to define the bijective functions given in Fact 6.3 as relations without appealing to any axiom. We then employ LEM to verify that those relations indeed have the desired properties. □

Fact 7.3. *If* X *has a (strict) well-order and* $|Y| \le_r |X|$, *then* Y *has a (strict) well-order.*

Proof. If R_X is a well-order on X and $S : Y \to X \to \mathbb{P}$ shows $|Y| \le_r |X|$, then $R_Y yy' := \forall x, x'.\, Syx \to Sy'x' \to R_X xx'$ is a well-order on Y. □

To proceed, we now also need to reformulate GCH since it contributes both positively and negatively to the proof of Theorem 6.7:

$$\begin{aligned}\mathrm{GCH}_{\mathbb{P}} \;:= \forall XY.\, |\mathbb{N}| \le |X| \le_r |Y| \le_r |X \to \mathbb{P}| \\ \to |Y| \le_r |X| \vee |X \to \mathbb{P}| \le_r |Y|\end{aligned}$$

Finally, since the step from $\mathrm{WO}_{\mathbb{T}}$ to $\mathrm{AC}_{\mathbb{T}}$ needed for Corollary 6.9 relies on UC as well, we also need to weaken $\mathrm{AC}_{\mathbb{T}}$

$$\begin{aligned}\mathrm{AC}_{\mathbb{P}} \;:= \forall XY.\, \forall R : X \to Y \to \mathbb{P}.\, (\forall x.\, \exists y.\, Rxy) \\ \to \exists R' \subseteq R.\, \forall x.\, \exists! y.\, R'xy\end{aligned}$$

where we write $R' \subseteq R$ to denote $\forall xy.\, R'xy \to Rxy$. We can then reformulate the main statements as follows:

Theorem 7.4 (LEM). $\mathrm{GCH}_{\mathbb{P}}$ *yields* $|X| \le_r |H(\mathcal{P}(\mathbb{N} + X))|$, *so* X *can be well-ordered. Thus* $\mathrm{GCH}_{\mathbb{P}}$ *implies* $\mathrm{WO}_{\mathbb{T}}$.

Proof. The proof follows exactly the same outline as Theorem 6.7 with all statements recast for functional total relations in the fashion of Fact 7.2. Crucially, it is easy to strengthen Theorem 5.14 to yield $|H(X)| \not\le_r |X|$. We then conclude $\mathrm{WO}_{\mathbb{T}}$ with Fact 7.3. □

Fact 7.5. $\mathrm{WO}_{\mathbb{T}}$ *implies* $\mathrm{AC}_{\mathbb{P}}$.

Proof. As in Fact 6.8 but without using UC to turn the constructed total functional relation into a function. □

Corollary 7.6 (LEM). $\mathrm{GCH}_{\mathbb{P}}$ *implies* $\mathrm{AC}_{\mathbb{P}}$.

We conclude with the fact that, although $\mathrm{AC}_{\mathbb{P}}$ is a rather weak choice axiom, it still implies LEM and hence Corollary 7.6 is still a faithful rendering of Sierpiński's theorem.

Fact 7.7. $\mathrm{AC}_{\mathbb{P}}$ *implies LEM.*

Proof. A proof adapting Diaconescu's theorem that the axiom of choice implies excluded middle can be found in the Coq standard library.[5] For an outline, consider the relation $R : (\Sigma p : \mathbb{B} \to \mathbb{P}.\, \exists b.\, pb) \to \mathbb{B} \to \mathbb{P}$ from inhabited predicates over $\mathbb{B}$ to $\mathbb{B}$ defined by $Rxb := \pi_1 xb$. Since R is easily proven total, $\mathrm{AC}_{\mathbb{P}}$ yields a total functional subrelation $R' \subseteq R$.

[5] https://coq.github.io/doc/master/stdlib/Coq.Logic.Diaconescu.html

Now given an arbitrary proposition $P : \mathbb{P}$, consider the two predicates $Ub := b = \mathrm{tt} \vee P$ and $Vb := b = \mathrm{ff} \vee P$. Since both are inhabited, we obtain unique b and b' with $R'Ub$ and $R'Vb'$. Case analysis on b and b' directly yields P in three cases, in the remaining case where $b = \mathrm{ff}$ and $b' = \mathrm{tt}$ we show $\neg P$. Indeed, assuming P yields $U = V$ but then $\mathrm{ff} = b = b' = \mathrm{tt}$ given that R' is functional. □

8 Discussion

8.1 Comparison

We briefly compare both presented versions of Sierpiński's theorem with respect to their overall strategy as well as the usage of excluded middle (LEM) and unique choice (UC).

In principle, both proof strategies are analogous and in particular the second half of the argument following the construction of the Hartogs numbers as sets $\aleph(A)$ respectively types $H(X)$ is identical up to formulation in the respective framework. The first half differs in the usage of set-theoretic ordinals to directly define $\aleph(A)$, postponing the concrete representation witnessing $|\aleph(A)| \leq |\mathcal{P}^6(A)|$ based on the usual set-theoretic notion of well-orderings as subsets of $A \times A$. Given their natural ordering by membership (Lemma 3.8), the relevant properties of set-theoretic ordinals are easy to mechanise, particularly benefiting from the inductive characterisation available in higher-order set theory. In the type-theoretic version, one could of course approximate ordinals as equivalence classes of abstract well-orders, but already their ordering based on embeddings instead of primitive membership would not be as direct. Therefore we did not introduce those abstract ordinals altogether but only considered the "small" ordinals representable by elements of $\mathcal{P}^3(X)$, hence obtaining the stricter bound $|H(X)| \leq |\mathcal{P}^3(X)|$.

As must be expected, the set-theoretic development heavily relies on LEM, especially to handle ordinals. Worth mentioning is that, in contrast to the usual first-order regularity axiom, the foundation axiom we assume for $\mathcal{S}$ does not imply LEM [30], so our axiomatisation of higher-order ZF, just like the higher-order versions of CZF discussed in [4], can in principle be used to mechanise set theory constructively.

Given the description operator definable from relational replacement (Lemma 3.1), UC is available on sets. Thus, as in first-order set-theory, there is no detectable difference between a total functional relation and a function on sets. On the other hand, if we were to assume UC on all types, the encodings $e_X : X \to \overline{X}$ defined in Definition 3.2 could be lifted to proper bijections $|X| = |\overline{X}|$ and especially eliminators like a recursor on ordinals matching the transfinite induction principle (Lemma 3.14) could be given. Since those properties were not necessary for our purpose, however, we refrained from assuming general UC in the set-theoretic development.

In the type-theoretic development, there are two decisions necessitating LEM early on that could be avoided. First, if we would treat ordinals abstractly as mentioned above, then every ordinal would have a successor and the initial case distinction in Theorem 5.13 to prove that ordinals are well-ordered could be side-stepped. Secondly, instead of directly employing the classical notion of well-foundedness via least elements one could follow the more constructive (but classically equivalent) approach based on termination and extensionality as chosen in the HoTT Book [43]. In this setting, the type of ordinals can be shown to be an ordinal constructively. However, as it still does not seem sufficient for a proof of $\mathrm{AC}_{\mathbb{T}}$ to embed every type into a terminating extensional preorder, LEM would be needed for this final step and therefore we chose the setup as explained. In particular regarding the first point, considering inclusion as the canonical ordering has its advantages since then only requiring well-foundedness is enough to represent the internal well-orders. Nevertheless, we do pay attention to constructivisation where easily possible, most notably by incorporating the weak versions of equipotence and isomorphism so to not depend on the non-constructive Cantor-Bernstein theorem [33].

Regarding UC as a means to better align the type-theoretic and set-theoretic version, we have illustrated that one can avoid this assumption if one is willing to work with total functional relations $X \to Y \to \mathbb{P}$ instead of functions $X \to Y$. However, we are convinced that assuming UC is a good investment to develop a compact and easy-to-explain proof, even if it can be eliminated afterwards. When translating set-theoretic results to dependent type theory, it just seems more natural to let the respective notions of functions coincide. As for LEM, we refrained from using UC where easily possible, for instance in the construction of functions from relations into a power type used in Lemma 5.5. Note that assuming UC only as a proposition in the form of $\mathrm{AC}_{\mathbb{T}}$ would be enough for the existence of the bijections in Fact 6.3 but still does not allow for their canonical definitions.

8.2 Mechanisation Details

The accompanying Coq mechanisation consists of two separate stand-alone developments for the set-theoretic (about 2700 lines) and the type-theoretic (about 1700 lines) versions of Sierpiński's theorem. The shared prelims in Section 2 are mostly linked to the latter. Both developments assume excluded middle as well as functional and propositional extensionality as axioms. Notably, in the set-theoretic development, excluded middle is assumed by importing the `Coq.Logic.Classical` library to make it visible for the standard automation tactics. The set-theoretic development depends on an assumed model of higher-order ZF as axiomatised in a previous development [26].

Especially the set-theoretic development employs a few notable features to ease the mechanisation. First, implementing the identification of classes and types, we employ a coercion from classes to types which allows us to write for example $A \to B$ to express the type of functions from a class A to a class B. Formally, elements of a class A are dependent

pairs consisting of a set x and a proof that $x \in A$. By proof irrelevance, equality of such pairs is equivalent to equality of the first components. We often need to turn elements of classes into sets and sets into elements. For the first direction, we have a simple coercion. To make the other direction more convenient, we treat the element-property with a type class and hide it as an implicit argument. Whenever the element-property cannot be inferred automatically, then we often use the command `Program Definition`. In proof scripts, we achieve a similar effect with tactics like `unshelve eexact`, `unshelve eapply`, and `unshelve eexists`. They introduce the property as an existential variable and then unshelve that variable to turn it into a goal.

Secondly, the formulations of constructors and recursors on sets do not posses any useful conversion properties. Computation has to be done by rewriting. For that purpose, we generally register computation rules with `autorewrite`. This tactic is also useful to apply the defining properties of sets or set operations like the union. The tactics `apply` and `auto` could be used in principle but are less helpful for that purpose since we often rewrite on specific subterms.

The type-theoretic development employs fewer notable features since it is does not add an additional layer of axiomatisation. We only remark that setoid rewriting to handle equivalence relations on types like $|X| = |Y|$ seems not to work well below sum and product types.[6] Moreover, it would have been a minor simplification of subtypes $\Sigma x.\, px$ if proof irrelevance were to hold computationally as implemented in the `SProp` universe of strict propositions [13]. It might be possible to transfer the whole development to `SProp` but this would require to reimplement a logic library in `SProp` first and to check that no large eliminations other than from $\bot$ were used.

8.3 Related Work

Mechanised first-order set-theory involving AC or CH. As mentioned in the introduction, Carneiro [9] mechanises Sierpiński's theorem in Metamath [29], based on an existing library of first-order ZF. The mechanisation in principle follows Specker's local version requiring just two instances of GCH [22, 40] and reimplements one of the library lemmas to avoid a dependency on AC. The present paper differs from Carneiro's work in three ways. First, we used the slightly less local proof variants given in [38] and [14] since they appeared simpler to generalise to type theory. Secondly, our set-theoretic development is based on a higher-order axiomatisation natural to work with in an expressive meta-logic. Concretely, this setting provides the instructive means of inductive definitions for iterative constructions such as ordinals and allows for reusing meta-level notions like function spaces, cardinality, orderings etc. with no need for boilerplate set encodings.[7] Thirdly, our set-theoretic proof serves as a bridge to the additionally presented type-theoretic version, showcasing a new instance of a set-theoretic result abstract enough to apply to dependent type theory.

Regarding work in other proof assistants, in Mizar, AC holds as a consequence of Tarski's axiom A [2]. The Isabelle/ZF library contains many results about ordinals and cardinals as well as proofs of the equivalence between 20 formulations of AC and 7 formulations of WO [32]. Moreover, Paulson [31] mechanises the relative consistency of GCH and AC based on the constructible universe L. Using Coq, Sun and Yu [41] mechanise AC and some of its equivalences in Morse-Kelley set theory. Working in Lean, Han and van Doorn [16, 17] mechanise the independence of CH over ZFC. Notably, they establish the consistency part by σ-closed forcing instead of the classical approaches via constructibility.

Mechanised higher-order set theory. Higher-order versions of ZF and CZF have been formulated using Coq by Werner [45] and Barras [4], respectively, with a focus on model constructions. Kirst and Smolka mechanise a categoricity result for higher-order ZF [24] and construct large models containing finitely many Grothendieck universes [26]. In [25] they illustrate how assuming AC on type-level induces AC on set-level, a property specific to higher-order set theory and also true for GCH. Kirst [23] mechanises an ordinal-theoretic proof that AC implies WO in a comparable setting and Kaiser [21] is concerned with an axiomatisation of higher-order Tarski-Grothendieck set theory in Coq. Brown and Pąk [8] compare the higher-order Tarski-Grothendieck set theory implemented in Egal [6] with its first-order counterpart implemented in Mizar [3]. Brown, Kaliszyk, and Pąk [7] show that higher-order Tarski-Grothendieck set theory can serve as a common foundation of the Isabelle/HOL and Isabelle/Mizar frameworks. The Lean mathematical library [28] contains a model of higher-order ZF with functional replacement.

Set-theoretic results in type theory. Chapter 10 of the HoTT book [43] contains a body of set-theoretic results formulated for the h-set fragment of homotopy type theory, including a type-theoretical proof of the well-ordering theorem. This result was also mechanised in Agda [19] and Coq [37]. De Rauglaudre [10] mechanises the Banach-Tarski Paradox in Coq, stating that the axiom of choice implies that a ball is equidecomposable with two balls of the same size. The development assumes the axiom of choice in the form TTCA formulated by Werner [45] and shows the claim for an axiomatised type of real numbers. Jaber et al. [20] propose a forcing translation for intuitionistic type theory,

[6] For instance the rewriting step in `infinite_unit` only worked after aliasing sums and products and inserting explicit type annotations. This problem has been reported on Coq's issue tracker.

[7] Of course library and tool support help to overcome the drawbacks of first-order axiomatisations but we are convinced that the higher-order approach used in this paper is a worthwhile alternative in a system like Coq.

applied to force the negation of the continuum hypothesis referring to the types $\mathbb{N}$ and $\mathbb{N} \to \mathbb{P}$. Grimm [15] works on a mechanisation of Bourbaki's set theory directly phrased in Coq's type theory.

Sources. Both versions of Sierpiński's theorem discussed in this paper are based on the presentations in [38] and [14]. The set-theoretic version was developed in the second author's master's project [34].

8.4 Future Work

We expect that a mechanisation of Sierpiński's theorem for instance carried out in CoqHoTT [5] or cubical Agda [44] would offer an interesting comparison to our Coq development. Then the assumed axioms hold on a less ad-hoc basis, since the univalence axiom uniformly establishes the needed extensionality and since PI and UC hold by the very notion of mere propositions. Morover, the treatment of isomorphic orders and equipotent types would benefit from the structure identity principle induced by univalence. In particular, the problematic setoid rewriting of bijections $|X| = |Y|$ would be replaced by rewriting with equalities $X = Y$.

Regarding the other prominent proof assistants based on dependent type theory, it is clear that the Coq mechanisation could in principle be ported to Lean. This would simplify the subtyping a bit since PI holds definitionally in Lean but one would have to pay attention not to use Lean's choice operator implicitly to keep the proof meaningful. Bearing a closer connection to constructive rather than classical set theory [1], pure Martin-Löf type theory as implemented in Agda without a universe of propositions does not seem like a well-suited system to even formulate Sierpiński's theorem directly. It is unlikely that approximating the impredicative power set operation predicatively with $X \to \mathbb{T}_i$ for some type level $\mathbb{T}_i$ will work throughout the proof and just considering the decidable subsets $X \to \mathbb{B}$ will complicate if not impede some intermediate constructions.

Secondly, we plan to further investigate the role of LEM at least for the type-theoretical version of Sierpinski's theorem. Although LEM is necessary for some intermediate statements, most notably the embedding theorem, it is not clear whether Sierpinski's theorem itself really relies on it. Following the usual proof strategy, the embedding theorem is needed to establish the type of well-orders as an arbitrarily large well-order, while obtaining the latter might even be possible constructively. Also the second part leading from large enough well-orders to $\mathrm{AC}_{\mathbb{T}}$ might be done without referring to LEM for the construction of the employed bijections. Given that $\mathrm{AC}_{\mathbb{T}}$ implies LEM, a constructive proof of Sierpiński's theorem would in particular yield that $\mathrm{GCH}_{\mathbb{T}}$ implies LEM.

Thirdly, while it is unlikely that a model of higher-order ZF satisfying GCH_S can be constructed given the close connection to $\mathrm{GCH}_{\mathbb{T}}$ (itself independent in Coq's type theory), it would be interesting to mechanise Gödel's original model of first-order ZF satisfying the generalised continuum hypothesis, namely the constructible universe L. It would be worthwhile to compare the existing Isabelle/ZF mechanisation of L to a Coq version, possibly employing MetaCoq [39] support for the central notion of first-order definability.

Fourthly, we plan to mechanise the undecidability of deductive consequence in ZF and other first-order axiom systems in the synthetic framework underlying the growing Coq library of undecidability proofs [11, 12].

Acknowledgments

The authors would like to thank Mario Carneiro, Yannick Forster, Julian Rosemann, Gert Smolka, and the anonymous reviewers for their helpful comments and suggestions.

References

[1] 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. https://doi.org/10.1007/3-540-48167-2_1

[2] Grzegorz Bancerek. 1990. Zermelo theorem and axiom of choice. *Formalized Mathematics* 1, 2 (1990), 265–267.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pak, and Josef Urban. 2015. Mizar: State-of-the-art and beyond. In *Conferences on Intelligent Computer Mathematics*. Springer, 261–279.

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

[5] Andrej Bauer, Jason Gross, Peter LeFanu Lumsdaine, Michael Shulman, Matthieu Sozeau, and Bas Spitters. 2016. The HoTT Library: A formalization of homotopy type theory in Coq. *CoRR* (2016). http://arxiv.org/abs/1610.04591

[6] Chad E. Brown. 2014. *The Egal Manual.* URL: http://grid01.ciirc.cvut.cz/~chad/egalmanual.pdf.

[7] Chad E. Brown, Cezary Kaliszyk, and Karol Pak. 2019. Higher-Order Tarski Grothendieck as a Foundation for Formal Proof. In *10th International Conference on Interactive Theorem Proving (ITP 2019)*.

[8] Chad E. Brown and Karol Pąk. 2019. A Tale of Two Set Theories. In *International Conference on Intelligent Computer Mathematics*. Springer, 44–60.

[9] Mario Carneiro. 2015. GCH implies AC, a Metamath Formalization. In *8th Conference on Intelligent Computer Mathematics (Workshop on Formal Mathematics for Mathematicians)*.

[10] Daniel de Rauglaudre. 2017. Formal Proof of Banach-Tarski Paradox. *Journal of Formalized Reasoning* 10, 1 (Oct. 2017), 37–49. https://doi.org/10.6092/issn.1972-5787/6927

[11] Yannick Forster, Dominik Kirst, and Gert Smolka. 2019. On synthetic undecidability in Coq, with an application to the Entscheidungsproblem. In *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs*. 38–51.

[12] Yannick Forster, Dominique Larchey-Wendling, Andrej Dudenhefner, Edith Heiter, Dominik Kirst, Fabian Kunze, Gert Smolka, Simon Spies, Dominik Wehr, and Maximilian Wuttke. 2020. A Coq library of undecidable problems. In *CoqPL 2020*. https://github.com/uds-psl/coq-libraryundecidability

[13] Gaëtan Gilbert, Jesper Cockx, Matthieu Sozeau, and Nicolas Tabareau. 2019. Definitional proof-irrelevance without K. *Proceedings of the ACM on Programming Languages* 3, POPL (2019), 1–28.

[14] Leonard Gillman. 2002. Two classical surprises concerning the axiom of choice and the continuum hypothesis. *The American Mathematical Monthly* 109, 6 (2002), 544–553.

[15] José Grimm. 2013. *Implementation of Bourbaki's Elements of Mathematics in Coq: Part One, Theory of Sets.* Research Report RR-6999. INRIA. 213 pages. https://hal.inria.fr/inria-00408143

[16] Jesse Han and Floris van Doorn. 2019. A formalization of forcing and the consistency of the failure of the continuum hypothesis. In *International Conference on Interactive Theorem Proving*. Springer, Heidelberg.

[17] Jesse Han and Floris van Doorn. 2020. A formal proof of the independence of the continuum hypothesis. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*. 353–366.

[18] Friedrich Hartogs. 1915. Über das Problem der Wohlordnung. *Math. Ann.* 76, 4 (1915), 438–443.

[19] Danko Ilik. 2006. Zermelo's well-ordering theorem in type theory. In *International Workshop on Types for Proofs and Programs*. Springer, 175–187.

[20] Guilhem Jaber, Nicolas Tabareau, and Matthieu Sozeau. 2012. Extending Type Theory with Forcing. In *LICS 2012 : Logic In Computer Science*. Dubrovnik, Croatia. https://hal.archives-ouvertes.fr/hal-00685150

[21] Jonas Kaiser. 2012. Formal Construction of a Set Theory in Coq. *Master's thesis, Universität des Saarlandes* (2012).

[22] Akihiro Kanamori and David Pincus. 2002. Does GCH imply AC locally. *Paul Erdös and His Mathematics II, Bolyai Society for Mathematical Studies* 11 (2002), 413–426.

[23] Dominik Kirst. 2014. Formalised Set Theory: Well-Orderings and the Axiom of Choice. Bachelor's thesis, Saarland University.

[24] Dominik Kirst and Gert Smolka. 2017. Categoricity Results for Second-Order ZF in Dependent Type Theory. In *Interactive Theorem Proving - 8th International Conference, ITP 2017, Brasilia, Brazil, 2017*.

[25] Dominik Kirst and Gert Smolka. 2018. Categoricity Results and Large Model Constructions for Second-Order ZF in Dependent Type Theory. *Journal of Automated Reasoning* (2018). First Online: 11 October 2018.

[26] Dominik Kirst and Gert Smolka. 2018. Large Model Constructions for Second-Order ZF in Dependent Type Theory. *Certified Programs and Proofs - 7th International Conference, CPP 2018, Los Angeles, USA, 2018* (Jan 2018).

[27] Adolf Lindenbaum and Alfred Tarski. 1926. *Communication sur les recherches de le théorie des ensembles.*

[28] The mathlib Community. 2020. The lean mathematical library. *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs* (Jan 2020). https://doi.org/10.1145/3372885.3373824

[29] Norman D. Megill and David A. Wheeler. 2019. *Metamath: A Computer Language for Mathematical Proofs.* Lulu Press, Morrisville, North Carolina. URL: http://us.metamath.org/downloads/metamath.pdf.

[30] John Myhill. 1973. Some properties of intuitionistic Zermelo-Frankel set theory. In *Cambridge Summer School in Mathematical Logic*. Springer, 206–231.

[31] Lawrence C. Paulson. 2008. The Relative Consistency of the Axiom of Choice – Mechanized Using Isabelle/ZF. In *Proceedings of the 4th Conference on Computability in Europe*. Springer-Verlag, Berlin, Heidelberg, 486–490. https://doi.org/10.1007/978-3-540-69407-6_52

[32] Lawrence C. Paulson and Krzysztof Grabczewski. 1996. Mechanizing set theory. *Journal of Automated Reasoning* 17, 3 (1996), 291–323.

[33] Pierre Pradic and Chad E. Brown. 2019. Cantor-Bernstein implies Excluded Middle. (April 2019). http://arxiv.org/abs/1904.09193

[34] Felix Rech. 2020. *Mechanising Set Theory in Coq.* Master's thesis. Saarland University. www.ps.uni-saarland.de/~rech/master.php

[35] Wacław Sierpiński. 1947. L'hypothèse généralisée du continu et l'axiome du choix. *Fundamenta Mathematicae* 1, 34 (1947), 1–5.

[36] Thoralf Skolem. 1922. Einige bemerkungen zur axiomatischen begründung der mengenlehre. (1922).

[37] Gert Smolka, Steven Schäfer, and Christian Doczkal. 2015. Transfinite constructions in classical type theory. In *International Conference on Interactive Theorem Proving*. Springer, 391–404.

[38] Raymond M. Smullyan and Melvin Fitting. 2010. *Set theory and the continuum problem.* Dover Publications.

[39] Matthieu Sozeau, Abhishek Anand, Simon Boulier, Cyril Cohen, Yannick Forster, Fabian Kunze, Gregory Malecha, Nicolas Tabareau, and Théo Winterhalter. 2020. The MetaCoq Project. *Journal of Automated Reasoning* (Feb. 2020). https://doi.org/10.1007/s10817-019-09540-0

[40] E. Specker. 1990. Verallgemeinerte Kontinuumshypothese und Auswahlaxiom. In *Ernst Specker Selecta*, Gerhard Jäger, Hans Läuchli, Bruno Scarpellini, and Volker Strassen (Eds.). Birkhäuser, Basel, 86–91. https://doi.org/10.1007/978-3-0348-9259-9_8

[41] Tianyu Sun and Wensheng Yu. 2019. Formalization of the Axiom of Choice and its Equivalent Theorems. *arXiv:1906.03930* (2019).

[42] The Coq Development Team. 2020. *The Coq Proof Assistant, version 8.12.0.* https://doi.org/10.5281/zenodo.4021912

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

[44] Andrea Vezzosi, Anders Mörtberg, and Andreas Abel. 2019. Cubical Agda: A Dependently Typed Programming Language with Univalence and Higher Inductive Types. *Proc. ACM Program. Lang.* 3, ICFP, Article 87 (July 2019), 29 pages. https://doi.org/10.1145/3341691

[45] Benjamin Werner. 1997. Sets in types, types in sets. In *International Symposium on Theoretical Aspects of Computer Software*. Springer, 530–546.