SAARLAND UNIVERSITY

Faculty of Natural Sciences and Technology I
Department of Computer Science
Bachelor's thesis

Formalised Set Theory:

Well-Orderings and the Axiom of Choice

Dominik Kirst
Bachelor's Program in Computer Science

August 2014

Advisor:
Jonas Kaiser, Programming Systems Lab,
Saarbrücken, Germany

Supervisor:
Prof. Gert Smolka, Programming Systems Lab,
Saarbrücken, Germany

Reviewers
Prof. Gert Smolka, Programming Systems Lab,
Saarbrücken, Germany

Prof. Holger Hermanns, Dependable Systems and Software,
Saarbrücken, Germany

Submitted
11th September, 2014

Saarland University
Faculty of Natural Sciences and Technology I
Department of Computer Science
Campus - Building E1.1
66123 Saarbrücken
Germany

Statement in Lieu of an Oath:

I hereby confirm that I have written this thesis on my own and that I have not used any other media or materials than the ones referred to in this thesis.

Saarbrücken, 11th September, 2014

Declaration of Consent:

I agree to make both versions of my thesis (with a passing grade) accessible to the public by having them added to the library of the Computer Science Department.

Saarbrücken, 11th September, 2014

Acknowledgments

First of all, I owe my full gratitude to my advisor, Jonas Kaiser. Patience, rigour and fascination are only a few of his attributes that made my work on this thesis an instructive and unique experience. In our meetings, I could benefit from his enthusiasm in teaching and constructive feedback. His contribution to this thesis is remarkable.

Moreover, I would like to thank my supervisor, Prof. Gert Smolka, who opened my eyes to the fascinating topic of computational logic and who made this great project possible. He supported me throughout my full bachelor course and I am glad about the inspiring atmosphere at his Programming Systems Lab.

I am very grateful to all the people in my vicinity that share my interest for foundational mathematics and other scientific topics. In stimulating discussions about logic and nearly everything else, I could gain insights from the collective knowledge of both students and teachers. In particular, I benefitted from the intellectual exchange of the "Studienstiftung des deutschen Volkes" during my studies.

Last but not least, I want to thank my family and friends, who supported me throughout writing this thesis with unconditional understanding and patience.

Abstract

In this thesis, we give a substantial formalisation of classical set theory in the proof system Coq. We assume an axiomatisation of ZF and present a development of the theory containing relations, functions and ordinals. The implementation follows the structure of standard text books. In the context of this theory, we prove Zermelo's Well-Ordering Theorem and the Axiom of Choice equivalent. In addition, we examine the history and development of modern set theory and compare Zermelo's original versions of the proof. We prove that both of them lead to the same ordering.

Für Sonja

Contents

Chapter 1
Introduction

The topic of this thesis is the formal development of an axiomatised set theory. We discuss the special role of the Axiom of Choice and the equivalent Well-Ordering Theorem in both mathematical and historical context.

We begin with a brief historical survey of modern set theory. The first name to be mentioned is certainly Cantor. In his article "Beiträge zur Begründung der transfiniten Mengenlehre" from 1895 [Can95], Cantor initially defined *sets* as "collections into a whole of definite and separate objects of our intuition or our thought"[1]. He reasoned about collections such as the natural or real numbers in terms of sets and published some pioneering results [Can74]. Peano and Dedekind recognized the potential of the set-theoretic language and constructed theories of natural and real numbers exclusively using Set Theory.

Frege, who comprehensively axiomatised logic in his "Begriffsschrift" from 1879 [Fre79], tried the same with arithmetic [Fre93]. His approach relied on a logical system based on sets and collapsed after Russell discovered his famous antinomy. It thereby turned out that Cantor's *naive* set theory admits certain "too large" sets which lead to contradictions.

Russel's groundbreaking discoveries led to the so-called *Foundational Crisis*, a dispute over how to consistently found Mathematics in the beginning of the 20th century. The research society seperated into two camps: Hilbert and the *formalists* tried to invent a complete and sound formalisation of Mathematics using axioms and inference rules, whereas Brouwer and the *intuitionists* reconsidered Mathematics as a pure result of constructive human mind and labelled the formalistic approach as meaningless syntactic manipulation of symbols.

[1] German original: *"Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen."*

The formalist's point of view has motivated two foundational systems, namely *type theory* and *axiomatic set theory*. The first, already suggested by Russel in 1908 [Rus08], introduced the notion of *types* in the sense of universes to resolve his antinomy by stratifying the construction of sets. This rather complex concept achieved (due to its rival ZF) little reception in the beginning but had a kind of renaissance when it came to proof theory and computational logic (see below).

The first consistent axiomatisation of what is nowadays considered modern set theory was developed by Zermelo and Fraenkel and is therefore denoted ZF. In the formal preface to his 1908 proof of the *Well-Ordering Theorem* [Zer08], Zermelo precisely lists the assumptions upon which his proof is constructed. The resulting system of axioms was expanded by Fraenkel in 1924 [Fra25].

To his basic axioms, Zermelo carefully added the controversial *Axiom of Choice* (AC), which intuitively allows to choose arbitrary elements from non-empty sets. Formal proofs using the Axiom of Choice usually highlight its application, due to rather surprising consequences such as the Banach-Tarski Paradox [Wag85], Zorn's Lemma or the here to be examined Well-Ordering Theorem. The theory of ZF extended with the Axiom of Choice is referred to as ZFC.

With ZF and ZFC, the development of set theory reached the state we present in this work. We formalise the usual foundational constructions of ZF following standard textbook presentations [HJ99, Dev79]. We consider, among others, ordered pairs, relations, functions, ordinals and orderings. The development culminates in the proof of the equivalence of the Axiom of Choice and the Well-Ordering Theorem. An extensive presentation is given in Chapter 4 and full details can be found in the underlying Coq proof scripts and documentations[2].

Moreover, given the context of ZF, it is worth to emphasize the role of the Axiom of Choice. In Chapter 2, we discuss the various forms of AC and give a few examples of its use. Afterwards, in Chapter 3, we pick the Well-Ordering Theorem as one instance of a substantial use of choice and compare the two proofs Zermelo gave in 1904 and 1908 [Zer04, Zer08]. We conclude with a brief discussion of related and future work in Chapter 5.

1.1 Contribution

The claim of this thesis is to give a substantial overview of classical set theory. We try to convey the foundational ideas and to put them into both the historical and the scientific context. Thereby, the connection of the Well-Ordering Theorem and the Axiom of Choice serves as a central theme that guides the way through this work. The final proof is one concluding result but we also want to examine all concepts we encounter with the appropriate amount of effort. Obviously, this approach does not lead to the shortest formalisation of the equivalence of both, a goal which has been widely studied (cf. Section 4.1).

[2] `https://www.ps.uni-saarland.de/~kirst`

In particular, we extensively study the internal representation of relations and functions in set theory, which is typically avoided by using a higher-order meta logic. Since the related text books mostly introduce an embedded notion of these concepts, we consider it worth to make them an independent object of study. Thus our formalisation of ZF is in tighter correspondence with the classical literature [HJ99, Dev79] and composes a library for further formal implementations of set-theoretic concepts.

We can summarise the results of this thesis as the following two: although set theory and its branches constitute a huge field, the key ideas can be formalised in a manageable framework ($\approx$ 2000 lines of Coq scripts). We have implemented roughly a third of Hrbacek & Jech [HJ99] and could formalise some involved theorems without any further assumptions besides the axioms.

Moreover, we formalise the equality of both constructed orderings Zermelo had introduced, which is a result that, although hinted in the literature [Kan04], has, to the best of our knowledge, not been examined in full detail before.

1.2 On Formal Proofs

We conclude this introduction with some modern discussions of the term formalisation. The aim of proving in general can be understood as convincing the reader of the correctness of the writer's thoughts based on logical principles. Since usual readers of mathematical proofs are mathematicians themselves, the writer might hide some formal detail and writes prose to ease the understanding. Hence, a usual proof has certain gaps and the reader is assumed to be experienced enough to fill in the omitted steps on his own.

Occasionally, these informal proofs are too vague or even veil serious errors and thus it becomes necessary to name every implicit step and definition - a formalisation. Using this technique, proofs can be verified objectively and, thus, trustworthiness can be increased. Lamport [Lam95] provides an interesting guideline on how to give formal and comprehensible proofs in this fashion.

On top of that, proof theory has changed a lot since the so called *Curry-Howard Isomorphism* was discovered [GTL89]. It states that propositions can be seen as types in a type theory based on Russell's original idea and that the elements of those types can be interpreted as proofs. Thus, proofs become computational objects and proof checking reduces to type checking. There are many differently expressive type theories, such as Girard's *System F* [GTL89], Martin-Löf's *Predicative Type Theory* [ML75] and Coquand's and Huet's *Calculus of Constructions* (CC) [CH88].

Implementations of type theories yield interactive proof assistants which give much support to their users. There are plenty of different assistants with unique designs, each based on a given type theory, such as *Agda*[3], *Isabelle*[4] and *Coq*[5], to name only a few. They all provide a certain degree of assistance for the construction of proof terms. Due to standardised implementations, a modern formalised proof is fully objective and even exceeds Lamport's ideal.

In our case, we work with a derivative of CC called the *Calculus of Inductive Constructions* (CiC) [Luo94, PPM89] implemented in the proof assistant Coq. In our development, we call all constructs of CiC the *meta-level*, meaning the level of reasoning, and refer to the embedded definitions of ZF as the *object-level*.

[3] http://wiki.portal.chalmers.se/agda/pmwiki.php

[4] http://www.cl.cam.ac.uk/research/hvg/Isabelle/

[5] http://coq.inria.fr

Chapter 2
The Axioms

The first rigorous axiomatisation was given by Euclid at about 300 BC. In his foundational work “Elements”, he constructed a profound theory of geometry based on only five postulates. These state some simple properties of the concepts of points and straight lines that were all intended to express some *absolute truths* about reality. From these axioms, all other theorems of euclidean geometry can be derived and thus have to be accepted once the axioms are. It is essential that these consequences do not contain contradictions - a property which is called *consistency*.

In the 19th century, it turned out that modifications of Euclid’s set of axioms, namely the negation of the so-called parallel postulate, do not yield an inconsistent theory but even allow for a precise model of a number of phenomena in physics [PM06]. This discovery led to a variety of independent theories and the notion of truth lost its claimed absoluteness. Nowadays, the axiomatic method is a key concept in logical reasoning and applied to further mathematical disciplines such as number theory and set theory.

The aim to found the whole construct of mathematics within one single system of axioms was pursued by a vast number of scientists and possibly reached its pinnacle with Whitehead’s and Russell’s “Principia Mathematica” [WR10]. That this approach comes with natural limitations is the famous result of Gödel’s Incompleteness Theorems [Göd31]. A detailed description of both the fascinating history of formalism and the resulting logical systems can be found in [Nor03].

In the following chapters, we use the language of predicate logic to form statements about sets. The *universe of discourse*, that is the range of our meta-level quantifiers, is usually the class of sets and in special cases the class of functions or predicates on sets. We omit the explicit annotation of the appropriate class wherever it can be inferred from the context. We use the two relations $\in$ and $\subseteq$

and some common abbreviations of logical terms. In particular, we write

$$\begin{aligned} \exists\, x \in A.\, P\, x \quad &\text{for} \quad \exists\, x.\, x \in A \wedge P\, x \\ \forall\, x \in A.\, P\, x \quad &\text{for} \quad \forall\, x.\, x \in A \Rightarrow P\, x \end{aligned}$$

and any identifiers which are not explicitly quantified should be understood as universally quantified on the outer-most level. We present rather complex statements in prose if the intended meaning is unambiguous. The usual notation for operations on sets will be introduced together with the respective axioms and definitions.

2.1 The Axioms of ZF

The first property our sets should satisfy is the *Axiom of Extensionality*:

Axiom 1 (Extensionality)**.** $\forall\, A\, B.\, A \subseteq B \Rightarrow B \subseteq A \Rightarrow A = B$

Sets are considered equal if they contain the same elements. This allows the general definition of sets via their elements and the common related notation. Consider for example the set $M := \{A, B\}$ defined as the unique set containing exclusively A and B. Then we can establish equalities such as $\{B, A\} = M = \{A, B, B\}$.

The majority of the upcoming axioms state the unique existence of certain sets specified via their elements. The claimed uniqueness is already a consequence of the pure existence of the set together with the Axiom of Extensionality. To give a clear intuition, however, we prefer the stronger statements.

In order to prevent a vacuous universe of discourse, the existence of at least one set has to be explicitly assumed from the beginning. The reasonable candidate is the empty set, which leads to the crucial *Axiom of Existence*:

Axiom 2 (Existence)**.** $\exists!\, Z.\, \forall\, A.\, A \notin Z$

With this unique empty set, usually denoted $\emptyset$, our theory contains a starting point where further constructions can be based on.

The next axioms all define operations to obtain new sets once some previous sets are given. We begin with the usual operations already introduced in naive set theory [Can74]. We first encounter the *Axiom of Pairing*:

Axiom 3 (Pairing)**.** $\forall\, A\, B.\, \exists!\, Z.\, \forall\, x.\, x \in Z \Leftrightarrow x = A \vee x = B$

Given two sets A and B, this axiom justifies the existence of the set $\{A, B\}$.

The next construction is induced by the following *Axiom of Union*:

Axiom 4 (Union)**.** $\forall\, S.\, \exists!\, Z.\, \forall\, x.\, x \in Z \Leftrightarrow \exists\, A.\, x \in A \wedge A \in S$

We write $\bigcup S$ for the union over the system of sets S.

The last explicit operator we introduce is given by the *Axiom of the Power Set*:

Axiom 5 (Power Set)**.** $\forall\, A.\, \exists!\, Z.\, \forall\, x.\, x \in Z \Leftrightarrow x \subseteq A$

We use $\mathcal{P}(A)$ as the notation for the power set of A. Clearly $\mathcal{P}(A)$ contains all subsets of A.

The next two axioms come with a slightly different effect since they use functions and relations in addition to sets and thus allow certain transformations. The first to consider is the following *Axiom of Replacement*:

Axiom 6 (Replacement)**.** $\forall\, A\, F.\, \exists!\, Z.\, \forall\, y.\, y \in Z \Leftrightarrow \exists\, x.\, x \in A \wedge y = F\, x$

It allows to collect the images $F\, x$ for all $x \in A$ into one set. The resulting set is referred to as $\{\, F\, x \mid x \in A \,\}$. There are stronger forms of replacement which are not phrased with a meta-level function F but instead use a functional relation P which may or may not be total. However, we prefer the functional form of replacement over its relational variants as it is more convenient. We do not loose any expressive strength [Bro13] because of the following *Axiom of Specification*:

Axiom 7 (Specification)**.** $\forall\, A\, P.\, \exists!\, Z.\, \forall\, x.\, x \in Z \Leftrightarrow x \in A \wedge P\, x$

Given a predicate P, we write $\{\, x \in A \mid P\, x \,\}$ to refer to the subset Z where all elements taken from A satisfy P. The similar Axiom of Comprehension in naive set theory is an unrestricted version of specification, since it allows to construct the set $\{\, x \mid P\, x \,\}$. Without the bounding set A, comprehension allows to collect all sets satisfying a predicate into a new set. Now with a trivial choice of P as constantly true, we can directly construct the inconsistent set of all sets. So the Axiom of Specification clearly illustrates that ZF excludes Russel's antinomies as no "too-large" sets can be proven to exists (cf. Lemma 1.7). Hence, it is usually listed as an independent axiom although it follows from the stronger forms of the Axiom of Replacement.

The last two axioms do not construct new sets but state some properties about the nature of sets. With specification, ZF already reaches a consistent state with regard to large sets, but usually a further restrictive axiom is included to make sets regular in terms of membership. One way to do so, is to assume the *Axiom of Regularity*:

Axiom 8 (Regularity)**.** $\forall\, A.\, A \neq \emptyset \Rightarrow \exists\, B \in A.\ (\forall\, x \in B.\, x \notin A)$

This axiom ensures that all sets are regular in the sense that they do not contain cycles of the form $x \in x_1 \in \ldots \in x_k \in x$. With this claim, however, we actively exclude some sets from our theory and thus reach an implicit stratification since now every set can be identified by an ordinal level. We examine this in detail in Section 4.6.

Another way to make sets regular is to opt for the even stronger Axiom of Well-Foundation, which prohibits all sets with infinite chains of membership. If we were to include neither of the two, we obtain a very different theory containing irregular sets such as quines of the form $x = \{x\}$ [Qui37].

In general, it is very interesting to consider the class of sets as partitioned into two subclasses. On the one side, we have the existing empty set and many operations that construct new sets. The first class now contains all sets we can define inductively from the empty set and the operations and hence we call them *accessible*.

On the other side, there are sets with undecidable existence. Apart from the proper classes such as the set of all sets, whose non-existence follows from the axioms, there are remarkably many sets we can not prove not to exist. The majority of them can not be reached inductively on the other hand, which leaves their existence somewhat unspecified and which is why we call this class *inaccessible*. In particular, any infinite set is inaccessible unless we assume the following *Axiom of Infinity*:

Axiom 9 (Infinity). $\exists\, A.\, \emptyset \in A \land (\forall\, x \in A.\, \bigcup\{x, \{x\}\} \in A)$

This inductive set contains the empty set $\emptyset$ and for every element x the from x distinguishable set $\bigcup\{x, \{x\}\}$, which we call the *successor* of x. The smallest such set can be used to define the set $\mathbb{N}$ of all natural numbers. We return to this notion in Section 4.3.

With this axiom, the boundary between the two classes of sets has moved an immense way but the existence of certain sets specified via comprehension is still not decidable. However, with Axiom 9, we have reached the usual scope of ZF and only leave it as a remark, that ZF can be expanded to contain further groups of sets such as Grothendieck-Universes [Kai12b] or the related Inaccessible Cardinals.

We conclude this section with some facts concerning the redundancy of the chosen axiomatisation. Clearly, once we have assumed the infinite set from Axiom 9, the existence of the empty set follows from specification. Furthermore, we can construct unordered pairs (and so make Axiom 2 admissible) by replacing the two elements of the set $\mathcal{P}(\mathcal{P}(\emptyset))$ with the given sets A and B. We have already mentioned that stronger forms of replacement make specification a consequence. So the set of axioms presented here is clearly not minimal but it represents a good compromise between conciseness and usability.

As is common in axiomatic set theory, we treat further operations such as intersections, binary operators and ordered pairs as defined entities rather than introducing them with the help of extra axioms. In the following section and Chapter 3, we assume these operations informally to focus on the ideas and postpone their explicit derivation until Chapter 4.

2.2 The Axiom of Choice

Consider a finite system S of non-empty sets M_i. We can imagine to go through S and pick one element from each M_i. This procedure ends after finitely many steps and constructs a function f with $f(M_i) \in M_i$ for all M_i. We call all f with this property a *choice function*. In particular, if $|M_i|$ denotes the cardinality of M_i, there exist $\prod_S |M_i|$ choice functions on S. Now let S be infinite. Then the intuitive approach of stepwise collection does not terminate any more and it arises the general question, whether there exist choice functions for infinite systems S.

It turned out, that this statement is neither provable [Coh66], nor refutable [Göd40] from the axioms of ZF. Hence it can be assumed independently in the form of a further axiom, which is typically denoted the *Axiom of (Full) Choice* and results in the stronger theory of ZFC. Zermelo was the first to mention its use explicitly. In both his proofs, the existence of choice functions is an essential assumption. Moreover, he defended its use as unproblematic since it was an "unobjectionable logical principle" [Zer08].

There is clear motivation for ZFC. First, we can raise the combinatory argument: If there are $|M_i| > 0$ possibilities to choose one element each $M_i \in S$, the intuition might suggest that there is at least one way to do so for all M_i simultaneously. Furthermore, there are traditional results that are not provable without the assumption of a choice principle, such as the trichotomy of cardinals or the existence of at least one basis for each vector space.

However, there are rather controversial consequences. First of all, the Well-Ordering Theorem itself can be considered at least unexpected. We will discuss this in the introduction of Chapter 3. Furthermore, theorems like the Banach-Tarski Paradox [Wag85] seem to contradict the intuition. To be more precise, the choice principle implies the existence of non-measurable sets, which are responsible for certain surprising properties of measure functions. This is one reason why the axiom is subject to ongoing discussions. Moreover, ZFC is incompatible with the school of intuitionism. This is due to Diaconescu, who proved that full choice implies excluded middle [Dia75]. So a constructivist has to reject the Axiom of Choice.

Due to the criticism, there are weaker forms of the axiom formulated, that still allow to prove some common results but exclude the most unexpected consequences. The *Axiom of Dependent Choice* allows to construct infinite sequences for total binary relations. Even weaker is the *Axiom of Countable Choice* that only admits choice functions on countable sets S. We have already seen that the *Axiom of Finite Choice* is a provable theorem of ZF.

Furthermore, there are some equivalent formulations of the Axiom of Full Choice itself. Instead of posing the existence of choice functions for arbitrary systems S of non-empty sets, one could alternatively claim the existence of a set I such that I shares exactly one element with each member M_i of S. This variant requires the sets M_i to be pairwise disjoint. Only a minor deviation is the assumption of a choice function on the power set $\mathcal{P}(M)$ without $\emptyset$, which is the formulation we will actually use in Section 4.7.

We conclude with a remark regarding the "external" choice operator, frequently called *Hilbert's epsilon*. Given a predicate P, the function ϵ establishes the following equivalence:

$$(\exists\, x.\, P\, x) \Leftrightarrow P\, (\epsilon\, P)$$

One could develop a similar intuitive justification for ϵ as for the choice principle in ZFC. Moreover, there is an actual connection of the two concepts: Let S be a system of non-empty sets M_i and let $P_i\, x$ denote the proposition $x \in M_i$. We can prove the existence of an x_i with $P_i\, x_i$ classically (Lemma 1.2). Therefore, $\epsilon\, P_i$ refers to an actual element of M_i. Then the collection of all $\epsilon\, P_i$ defines a choice function on S. So Hilbert's ϵ implies the Axiom of Choice. Note that logical choice is even strictly stronger than the choice principle on sets, since it allows a statement about proper classes of the form $\{\, x \mid P\, x\, \}$.

This consequence together with Diaconsescu's theorem clarifies, that the assumption of an epsilon-operator induces classical assumptions and full choice on sets. However, we will make use of a much weaker form, called description, in Chapter 4.

Chapter 3
Well-Orderings

Before we state the Well-Ordering Theorem and analyse some proofs of it, we introduce the key notion of orderings motivated by an example. One of the best-known well-orderings is the less-than relation on the set $\mathbb{N}$ of natural numbers. Throughout the intro of this chapter, "$<$" denotes this particular relation, before we generalise it in later sections. This relation allows for the act of *comparing* in various contexts and hence serves as a familiar subject of study.

We can observe some basic facts from our experience:

- A number is not less than itself.
- If $x < y$ and $y < z$, then $x < z$.
- All numbers are comparable.

We name these properties *irreflexivity*, *transitivity* and *linearity*. Moreover, there is a more involved characteristic: the ordering $<$ contains no infinite descending chains or, in other words, all non-empty subsets of $\mathbb{N}$ contain a least element. We call $<$ and all other relations with this feature *well-founded* and a relation satisfying all four properties a *well-ordering*. The formal definitions of these keywords can be found in Section 4.2.

In general, the properties of well-orderings are the essence of our natural feeling of "before and after" or "less and greater". In terms of set theory, these concepts are used whenever we write $M = \{m_1, m_2, m_3 \ldots\}$. Then we assume an implicit ordering of M and enumerate all elements m_i correspondingly. We can visualize this transformation for both collections of natural objects and lager sets of numbers like $\mathbb{Z}$ and $\mathbb{Q}$, but, at the latest, if it comes to $\mathbb{R}$, our intuition is exhausted. It arises the question whether *every set can be well-ordered*, which is formulated in the Well-Ordering Theorem. Since the notion of sets is a foundational concept of our mind, a general answer to this question would mean a great insight into our own thought.

Moreover, the powerful techniques of both induction and recursion can be applied to well-ordered sets. The former allows for concise proofs of properties of all elements of the set and the latter is a helpful instrument to construct functions with the well-ordered set as domain. These are only a few reasons why this questioning is of immense significance for mathematicians.

Already Cantor was convinced that every set can be well-ordered in this manner which is why he called this theorem a "fundamental principle of thought". It became an issue of high interest to give either a proof of the theorem or a counter-example.

In this rather controversial atmosphere, Zermelo came up with a first proof of the Well-Ordering Theorem [Zer04]. Since his first attempt to convince his contemporaries was rather unsuccessful, Zermelo gave a second proof in 1908, in which he presented the formal assumptions in detail and invalidated the criticism of his opponents [Zer08]. It was this second proof where he introduced the axiomatic constructions needed for the development and the "unobjectionable logical principal" of the Axiom of Choice.

In the next two sections, we outline a modern translation of the two proofs. A similar work was done by Kanamori [Kan04]. In both proofs, we assume M to be an arbitrary set and γ to be a choice function on $\mathcal{P}(M)$. In Section 3.3, we will see that the actual γ determines the ordering we obtain.

For sets $A \subseteq M$ we write A° to denote the set $A \setminus \{\gamma(A)\}$. Moreover, we will use the symbol $<$ for abstract orderings and define the *initial segment* of a set A as $A[x]_< := \{\, y \in A \mid y < x \,\}$.

3.1 Zermelo's 1904 Proof

The following is the basic definition we use in the first proof:

Definition. We call a set $M_\gamma \subseteq M$ a *γ-set*, if the following hold:

(1) there exists a well-ordering $<$ on M_γ

(2) $a = \gamma(M \setminus M_\gamma[a]_<)$ for all $a \in M_\gamma$.

We define $\Gamma := \{\, M_\gamma \in \mathcal{P}(M) \mid M_\gamma \text{ is a } \gamma\text{-set} \,\}$ and $L_\gamma := \bigcup \Gamma$.

The proof consists of the following steps:

1. *There exist γ-sets in $\mathcal{P}(M)$:*

   A vacuous witness is $\emptyset$ but we can give even more examples such as $\{\gamma(M)\}$ and $\{\gamma(M), \gamma(M \setminus \{\gamma(M)\})\}$. This illustrates that the γ-sets form initial segments of the resulting ordering.

2. *If M_γ and M'_γ are γ-sets, then one is an initial segment of the other:*
   Assume $a \in M_\gamma$ and $b \in M'_\gamma$ with $M_\gamma[a]_< = M'_\gamma[b]_{<'}$. Then we have $M \setminus M_\gamma[a]_< = M \setminus M'_\gamma[b]_{<'}$ and thus $\gamma(M \setminus M_\gamma[a]_<) = \gamma(M \setminus M'_\gamma[b]_{<'})$. The definition of γ-sets implies $a = b$. We repeat this argument inductively and obtain the equality of all corresponding initial segments. Then the first γ-set to exhaust is an initial segment of the other.

3. *If two γ-sets contain a and b with $a \neq b$, then in both either $a < b$ or $b < a$:*
   This is a direct consequence of 2.

4. *L_γ is well-ordered:*
   For $a, b \in L_\gamma$, we write $a <_1 b$ if $a < b$ in some γ-set. The above results imply that this ordering is irreflexive, transitive and linear. To obtain well-foundation, let L be a non-empty subset of L_γ and $a \in L$. Then there exists a γ-set M_γ with $a \in M_\gamma$ and the subset $L' := \{\, x \in L \mid x \leq a \,\}$ of M_γ has a $<$-least element m. It follows from the properties of $<_1$, that m is the $<_1$-least element of L.

5. *L_γ is a γ-set:*
   Let a be an element of L_γ. Then $L_\gamma[a]_{<_1} = M_\gamma[a]_<$ holds for all M_γ that contain a. There is at least one M_γ with $a \in M_\gamma$ and we conclude $a = \gamma(M \setminus L_\gamma[a]_{<_1})$. Together with step 4, this shows that L_γ is a γ-set.

6. *$L_\gamma = M$:*
   Assume the set $D := M \setminus L_\gamma$ is not empty. Then we can define $a := \gamma(D)$ and obtain a new γ-set $L_\gamma \cup \{a\}$. This implies the contradiction $a \in L_\gamma$.

Note that, in the first proof, the ordering is constructed *bottom-up* by successive choices. It is characterised by the special set $\Gamma \subseteq \mathcal{P}(M)$ which is the set of all initial segments of the final ordering.

3.2 Zermelo's 1908 Proof

The second proof is also based on an essential, albeit different, definition:

Definition 2.1. We call a set $\theta \subseteq \mathcal{P}(M)$ a θ-chain, if all the following hold:

(1) $M \in \theta$

(2) $A \in \theta \Rightarrow A^\circ \in \theta$

(3) $S \subseteq \theta \Rightarrow \bigcap S \in \theta$

We define $\Theta := \bigcap \{\, \theta \subseteq \mathcal{P}(M) \mid \theta \text{ is a } \theta\text{-chain} \,\}$.

Now we can sketch the respective proof:

1. *There exist θ-chains in $\mathcal{P}(\mathcal{P}(M))$.*
   It is obvious that $\mathcal{P}(M)$ is a θ-chain.

2. *Θ is a θ-chain.*

   Since all θ-chains satisfy the defining properties, so does the intersection Θ.

3. *If $A, B \in \Theta$ with $A \neq B$, then $A \subseteq B^\circ$ or $B \subseteq A^\circ$.*

   This is justified by an inductive argument.

4. *For non-empty $P \subseteq M$ there exist unique $\mathcal{R} \in \Theta$ with $P \subseteq \mathcal{R}$ and $\gamma(\mathcal{R}) \in P$.*

   Let P be not empty and $\mathcal{R}$ the intersection of all $M' \in \Theta$ with $P \subseteq M'$. Then $\gamma(\mathcal{R}) \in P$ must hold, since $P \subseteq \mathcal{R}^\circ$ otherwise. Let $\mathcal{S} \in \Theta$ be another element with $P \subseteq \mathcal{S}$. Then $\mathcal{R} \subset \mathcal{S}$ by the definition of $\mathcal{R}$ and $\mathcal{R} \subseteq \mathcal{S}^\circ$ by step 3. We conclude $\gamma(\mathcal{S}) \notin P$.

5. *For every $a \in M$ there exists a unique $\mathcal{R}(a) \in \Theta$ with $\gamma(\mathcal{R}(a)) = a$.*

   This is a corollary of step 4. Set $P := \{a\}$.

6. *Θ induces a well-ordering on M.*

   We write $a <_2 b$ whenever $b \in \mathcal{R}(a)$ and $b \neq a$. By definition, $<_2$ is irreflexive and transitive. It is linear due to step 3. Now let P be a non-empty subset of M. Step 4 yields a related $\mathcal{R}$ with $\mathcal{R} = \mathcal{R}(\gamma(\mathcal{R}))$. Thus all elements of P are contained in $\mathcal{R}(\gamma(\mathcal{R}))$ and so $\gamma(\mathcal{R})$ is the $<_2$-least element of P. So $<_2$ is well-founded.

In contrast to the first proof, the reasoning presented in the second proof follows a *top-down* approach. It is characterised by the set Θ which contains all rests of the final ordering.

3.3 Comparison

In his second article, Zermelo also justifies that Θ is the only θ-chain with the property described in step 4 above. The following indirect proof illustrates the underlying idea:

Let $\Theta' \neq \Theta$ be a second θ-chain of this quality. Since Θ is the smallest θ-chain, we have $\Theta \subset \Theta'$ and thus there exists a non-empty $D \in \Theta' \setminus \Theta$. First, from the property of Θ, there exists a corresponding rest $\mathcal{R} \in \Theta$ for D. Secondly, the set D itself clearly fulfils the same features since $D \in \Theta'$, $D \subseteq D$ and $\gamma(D) \in D$. This contradicts the uniqueness of $\mathcal{R}$.

Now let $<_1$ and $<_2$ be the well-orderings constructed in the 1904 and 1908 article respectively. We first introduce some shorthands:

$$a{\downarrow} := M[a]_{<_1} \text{ and } a{\uparrow} := M \setminus a{\downarrow}$$

$$a{\Downarrow} := M[a]_{<_2} \text{ and } a{\Uparrow} := M \setminus a{\Downarrow}$$

We use the uniqueness result of Θ to prove that both orderings are equivalent. This means, for $a, b \in M$, we prove:

$$a <_1 b \Leftrightarrow a <_2 b$$

To do so, we first consider simple characterisations of the respective orderings:

$$a <_1 b \Leftrightarrow \exists\, M_\gamma \in \Gamma .\, a \in M_\gamma \wedge b \notin M_\gamma$$

Let $a <_1 b$. Then the set $b{\downarrow}$ is a possible witness. On the other hand, let $M_\gamma \in \Gamma$ with $a \in M_\gamma$ and $b \notin M_\gamma$. Since $M = L_\gamma$, we can find a γ-set M'_γ with $b \in M'_\gamma$. Because of step 2 of the 1904 proof, M_γ is an initial segment of M'_γ and thus $a <_1 b$.

$$a <_2 b \Leftrightarrow \exists\, \mathcal{R} \in \Theta .\, a \notin \mathcal{R} \wedge b \in \mathcal{R}$$

Let $a <_2 b$. Then the set $b{\Uparrow}$ is a possible witness. On the other hand, let $\mathcal{R} \in \Theta$ with $a \notin \mathcal{R}$ and $b \in \mathcal{R}$. From the linearity of $<_2$, either $a <_2 b$ or $b <_2 a$ and hence either $b \in \mathcal{R}(a)$ or $a \in \mathcal{R}(b)$ must hold. If we assume the latter case, we obtain $\mathcal{R}(b) \subseteq \mathcal{R} \subseteq \mathcal{R}(a)$ from step 3 of the 1908 proof and thus the contradiction $b \in \mathcal{R}(a)$.

Now we find that the sets Γ and Θ are *dual* in the sense that the complements $A^{\mathrm{c}} := M \setminus A$ of the elements of the former are the members of the latter. To make this more explicit, we define

$$\tilde{\Gamma} := \left\{\, M_\gamma^{\mathrm{c}} \in \mathcal{P}(M) \mid M_\gamma \text{ is a } \gamma\text{-set} \,\right\}$$

and prove that $\tilde{\Gamma} = \Theta$. Once this equality is established, the equivalence of the orderings is a trivial consequence, since the complement of a witness in the $<_1$-characterisation serves as a witness in the $<_2$-characterisation and vice versa.

So it remains to show $\tilde{\Gamma} = \Theta$ which reduces, due to the uniqueness result, to proving that the property of step 4 holds for $\tilde{\Gamma}$ and that $\tilde{\Gamma}$ is a θ-chain. The latter is trivial and we omit the mechanical proof here. So let P be a non-empty subset of M. We have to find the related rest $\mathcal{R} \in \tilde{\Gamma}$. Since $<_1$ is a well-ordering, there exists a $<_1$-least element a of P. Now set $\mathcal{R} := a{\uparrow}$ and consider the three required properties:

- The complement $\mathcal{R}^{\mathrm{c}} = a{\downarrow}$ is a γ-set, since it is an initial segment of the γ-set $L_\gamma = M$. Hence we have $\mathcal{R} \in \tilde{\Gamma}$.

- Let $b \in P$. Since a is the $<_1$-least element of P, we know $a \leq b$ and thus $b \in \mathcal{R}$. We conclude $P \subseteq \mathcal{R}$.

- Consider the γ-set $L_\gamma = M$. Since $a \in M$, we infer $a = \gamma(M \setminus a{\downarrow}) = \gamma(\mathcal{R})$ from the definition of γ-sets and conclude $\gamma(\mathcal{R}) \in P$.

Now assume that $\mathcal{R}' \neq \mathcal{R}$ satisfies the same three properties. Thus we have $\mathcal{R}' \in \tilde{\Gamma}$ and $P \subseteq \mathcal{R}'$. Since $a\downarrow = \mathcal{R}^{\mathrm{c}}$ is the largest γ-set not containing a, the complement $(\mathcal{R}')^{\mathrm{c}}$ must be a strict subset of $a\downarrow$. Now let $D := a\downarrow \setminus (\mathcal{R}')^{\mathrm{c}}$ be the non-empty difference and $b \neq a$ the $<_1$-least element of D. Then $(\mathcal{R}')^{\mathrm{c}} = b\downarrow$ and from the properties of γ-sets, we derive $\gamma(\mathcal{R}') = c(M \setminus b\downarrow) = b \notin P$. This contradicts the third property of R'.

This shows that, although the two constructions are rather different, the resulting ordering is the same. A formalisation of the equality can be found as appendix in our related development. It is based on an implementation of the 1904 proof by Ilik / Kaiser [Ili06, Kai12a] and, respectively, the 1908 proof by Brown [Bro14]. In the formal development, we use an alternative approach that leads to a very short justification. It, however, does not show all details of the observed duality of Θ and Γ, which is why we present both variants.

In Chapter 4, we examine a proof of the Well-Ordering Theorem which is a more abstract version of Zermelo's 1904 proof and a third way to obtain the same ordering. It uses the concept of ordinal numbers to construct the function of "successive choices", which allows for a very strong intuition.

Chapter 4
Formalisation of ZF

Our formalisation follows the usual *classical* (i.e. non-constructive) mathematical presentation [HJ99, Dev79]. In order to do so, we extend our meta-theory with the *Law of Excluded Middle* and the *Axiom of Description*.

The Law of Excluded Middle is a logical principle, which claims that for every proposition p there exists a proof of either p or $\neg p$. The assumption is intuitive but if one requires fully constructive proofs, as Brouwer and his contemporaries did in the early 20th century [Bro23], then it is not clear where either of the proofs should be coming from. This led to the intuitionistic school, where the principle is rejected.

The type theory we use in this work, namely CiC, is such a constructive system and excluded middle is not included by default. The principle is, however, independent of CiC and can thus be assumed consistently.

The assumption of a restricted description operator allows to define sets via proving the unique existence of a set fulfilling some property. Thus we can turn unique witnesses into proper objects of the meta theory. While a full choice operator does the same without requiring uniqueness it is obviously too strong for our purpose. Full choice at the meta-level would directly imply the Axiom of Choice in our object-level set theory (cf. Section 2.2).

As mentioned before, the majority of ZF-Axioms state the existence of some unique sets like the unordered pair or the power set and only the use of the Axiom of Description permits us to introduce names for these sets (in the sense of functions operating on sets). Furthermore, in Section 4.6, we will need description to complement our rather weak replacement axiom in order to construct *Ordertypes* and *Hartogs Numbers*.

The following presentation closely corresponds to the related formalisation given in Coq. We discuss the most interesting definitions and theorems and give a comprehensive walkthrough of the development. Sections 4.1 to 4.4 outline the development of a basic set library, from the axioms up to a fully-fledged ordinal theory, whereas Sections 4.5 and 4.6 provide the infrastructure particular to the proof of the Well-Ordering Theorem in Section 4.7.

4.1 Basic ZF

4.1.1 The Framework

To begin, we set up the embedding of ZF into CiC. We initially pose set as a type equipped with an element-relation el of type $set \Rightarrow set \Rightarrow Prop$. As usual, we will write $x \in A$ for $el\,x\,A$. Now we can define the subset-relation $subs$:

Definition 1.1. $subs\ (A\colon set)\ (B\colon set) := \forall\, x \in A.\, x \in B$

So $subs$ has type $set \Rightarrow set \Rightarrow Prop$ as expected and again we write $A \subseteq B$ instead of $subs\,A\,B$. Note that $A \subset B$ indicates strict subsets.

Once we have defined the type of sets, we can formulate the description operator mentioned above. Since description restricted to sets is enough for our purpose, it suffices to assume an operator $desc$ of type $(set \Rightarrow Prop) \Rightarrow set$ together with the following *Axiom of Description*:

Axiom 10 (Description). $\forall\ (P\colon set \Rightarrow Prop)\,.\ (\exists!\, x.\, P\,x) \Rightarrow P\ (desc\,P)$

The expression $desc\,P$ denotes the unique set satisfying the "description" induced by the predicate P and it is easy to prove the characteristic property:

Lemma 1.1. $\forall\ (P\colon set \Rightarrow Prop)\ (A\colon set)\,.\ (\exists!\, x.\, P\,x) \Rightarrow (P\,A \Leftrightarrow A = desc\,P)$

Proof. *Let P be a uniquely satisfied predicate on sets and A an arbitrary set. We assume $P\,A$ and prove $A = desc\,P$. From the Axiom of Description, it follows that $P\ (desc\,P)$. Now we have two sets satisfying P and obtain their equality from the assumed uniqueness. If we assume $A = desc\,P$ on the other hand, we immediately obtain $P\,A$ from the Axiom of Description.* □

Next we assume the axioms of ZF in their existential form (see Section 2.1). Since the Axioms 2 to 7 allow for constructing new unique sets, we can use $desc$ to obtain the related operations. With the common notation for the operations introduced in Section 2.1, we can reformulate the corresponding axioms as provable lemmas with more convenient application.

For instance, we define the operation for the Axiom of Replacement as follows. With the predicate $P := \lambda\, A\, R\, Z.\, \forall\, y.\, y \in Z \Leftrightarrow \exists\, x.\, x \in A \wedge y = R\,x$ we obtain the defining description:

Definition. $replacement\ (A\colon set)\ (R\colon set \Rightarrow set) := desc\ (P\,A\,R)$

As motivated before, we write $\{R\,x \mid x \in A\}$ instead of *replacement* $A\,R$. Now we can use Axiom 10 to prove the characteristic property of *replacement*:

Lemma. $\forall\, A\, R\, y.\, y \in \{R\,x \mid x \in A\} \Leftrightarrow \exists\, x.\, x \in A \wedge y = R\,x$

Proof. *Let A be a set and R a function from set to set. With the Axiom of Description we can derive that $P\ \{R\,x \mid x \in A\}$ holds. We satisfy the necessary premise $\exists!\, Z.\, P\, A\, R\, Z$ with an instance of the Axiom of Replacement.* □

The proofs for the other operations work in the same manner and we obtain six lemmas replacing the six respective axioms. For convenience, we will hereafter refer to the actual axioms whenever using the characteristic properties of the defined operators. Together with the unaltered Axioms 1 and 7 to 9 we finish our basic framework and begin developing the theory.

Before we define further simple operations on sets, we prove some basic facts we frequently need. First, we consider two instances, where classical reasoning is essential:

Lemma 1.2. $\forall\, A.\, A \neq \emptyset \Leftrightarrow \exists\, x.\, x \in A$

Proof. *Let A be a non-empty set. Instantiating excluded middle with $P := \exists\, x.\, x \in A$ enables an indirect proof. If P holds, we have nothing left to show. If $\neg P$ holds, we can prove $A = \emptyset$ in contradiction to our assumption. Application of Lemma 1.1 reduces proving the equality to proving the uniqueness of the defining description of $\emptyset$ and proving that A satisfies this description. The former is the Axiom of Existence, the latter a simple consequence of the assumption $\neg P$.*

Now let x be an element of A. Regarding the definition of $\neg$ in constructive theories, we prove $A \neq \emptyset$ by assuming $A = \emptyset$ and concluding a contradiction. Indeed we have $x \in \emptyset$, contradicting the Axiom of Existence. □

This is a typical lemma not provable in a constructive setting, since the "witness" x needed for the first direction is not a computational object we can refer to. Another classical-only result is the following fact:

Lemma 1.3. $\forall\, A\, B.\, A \not\subseteq B \Leftrightarrow \exists\, x.\, x \in A \wedge x \notin B$

Proof. *Let A and B be sets with $A \not\subseteq B$. Again we use indirect reasoning: The negated claim implies $\forall\, x.\, \neg\, (x \in A \wedge x \notin B)$. From this we derive $A \subseteq B$ and obtain a contradiction.*

Given x with $x \in A$ and $x \notin B$ and the assumption $A \subseteq B$ on the other hand, we have $x \in B$ by instantiating $A \subseteq B$. □

We continue with four direct consequences of the assumed axioms. The first example follows from the Axiom of Specification:

Lemma 1.4. $\forall\ (A\colon \mathit{set})\ (P\colon \mathit{set} \Rightarrow \mathit{Prop})\,.\ \{x \in A \mid P\,x\} = A \Leftrightarrow (\forall\, x \in A.\, P\,x)$

Proof. *Let A be a set and P a predicate. We assume the equality $\{x \in A \mid P\,x\} = A$ and consider an arbitrary $x \in A$. From the assumption we know $x \in \{x \in A \mid P\,x\}$ and with the Axiom of Specification we conclude $P\,x$.*

Let now $P\,x$ hold for every element x of A. We use the Axiom of Extensionality to show the equality of both sets. Clearly $\{x \in A \mid P\,x\} \subseteq A$ since specifications are subsets. With $x \in A$ we prove $x \in \{x \in A \mid P\,x\}$ for the second inclusion. The Axiom of Specification reduces the claim to $x \in A \wedge P\,x$. Both parts are assumptions. □

A second result is a property of power sets:

Lemma 1.5. $\forall\, A\, B\, C.\, A \subseteq B \Rightarrow B \in \mathcal{P}(C) \Rightarrow A \in \mathcal{P}(C)$

Proof. *Let A, B and C be sets with $A \subseteq B$ and $B \in \mathcal{P}(C)$. With the Axiom of the Power Set instantiated for the latter assumption, we obtain $B \subseteq C$. Now transitivity of $\subseteq$ yields $A \subseteq C$ and another use of the Axiom of the Power Set finishes the proof.* □

With the Axiom of Regularity, we can exclude the existence of *one-cycles*:

Lemma 1.6. $\forall\, A.\, A \notin A$

Proof. *Let A be a set with $A \in A$. Consider the set $B := \{A, A\}$. The Axiom of Regularity implies, that there exists $C \in B$ such that C and B are disjoint. As a consequence of the Axiom of Pairing, we infer $C = A$. We conclude the contradiction, that A and B are not disjoint, since $A \in A$ is an assumption and $A \in B$ comes from the Axiom of Pairing.* □

The last result is the important insight that there exists no set of all sets. It is clearly a direct consequence of Lemma 1.6 but we can give a more independent proof that does not need regularity:

Lemma 1.7. $\neg\exists\, A.\, \forall\, a.\, a \in A$

Proof. *Assume the all-set A to exists. We then construct the set $R := \{\, a \in A \mid a \notin a \,\}$ via specification. By excluded middle there are two cases, either $R \in R$ or $R \notin R$. In the former, the Axiom of Specification implies that $R \notin R$, in the latter, it implies that $R \in R$. Both are contradictions.* □

The used construction is exactly Russell's famous antinomy.

4.1.2 Binary Union and Intersection

Next we construct common derived operations to form new sets. We begin with binary union, denoted $A \cup B$. From now on, our definitions will directly use mathematical notation wherever possible.

Definition 1.2. $A \cup B := \bigcup \{A, B\}$

A typical way to justify the correctness of new operations is to describe the intended semantics in terms of introduction and elimination rules. In the case of binary union, we prove the following:

Lemma 1.8. $\forall\, A\, B\, x.\, x \in A \vee x \in B \Rightarrow x \in A \cup B$

Proof. *Let A, B and x be sets with $x \in A$. We proof $x \in A \cup B$. With the definition of binary union and the Axiom of Union, we have to find a set C with $x \in C$ and $C \in \{A, B\}$. With the choice $C := A$ the former is an assumption and the latter an application of the Axiom of Pairing. The second case where $x \in B$ is analogous.* □

We obtain a full characterisation if we add the following elimination rule:

Lemma 1.9. $\forall\, A\, B\, x.\, x \in A \cup B \Rightarrow x \in A \vee x \in B$

Proof. *With arbitrary sets A, B and x satisfying $x \in A \cup B$, the definition of $\cup$ and the Axiom of Union give a set C with $x \in C$ and $C \in \{A, B\}$. With the Axiom of Pairing, we obtain $A = C \vee B = C$ and hence $x \in A \vee x \in B$.* □

Therefore, the set $A \cup B$ contains exactly the elements we expect, namely all elements of A and B.

The dual to arbitrary union is arbitrary intersection defined in terms of union and specification:

Definition 1.3. $\bigcap S := \{\, x \in \bigcup S \mid \forall\, A \in S.\, x \in A \,\}$

This definition is intuitively clear, since for non-empty S surely $\bigcap S$ is the subset of all elements of $\bigcup S$ appearing in every member of S. Again we justify correctness by proving introduction and elimination rules which look as expected and are omitted here. Binary intersection is constructed similarly to binary union:

Definition 1.4. $A \cap B := \bigcap \{A, B\}$

With the operation $A \setminus B$ called "difference" or "relative complement" we reach the extent of common Venn-Diagrams. We merely give the definition for completeness:

Definition 1.5. $A \setminus B := \{\, x \in A \mid x \notin B \,\}$

We write A^{c} for $B \setminus A$ wherever the set B is clear from the context.

4.1.3 Ordered Pairs and Cartesian Product

In order to formulate a theory of relations and functions, we require a notion of ordered pairs. We do not have to axiomatise them, but can choose from a number of encodings. Here we opt for so-called Kuratowski Pairs [Kur21]:

Definition 1.6. $(A, B) := \{\{A\}, \{A, B\}\}$

where $\{A\}$ is a shorthand for the pair $\{A, A\}$.

In contrast to unordered pairs, ordered pairs support a notion of first and second component and we can define corresponding projection operations. The simpler case is the first projection since every element in (A, B) contains the set A:

Definition 1.7. $\pi_1\, p \coloneqq \bigcup \bigcap p$

If p is a pair, we obtain $\{A\}$ by $\bigcap p$. With the outer union we end up with A as desired. We now prove the correctness of π_1 formally:

Lemma 1.10. $\forall\, A\, B.\, \pi_1\, (A, B) = A$

Proof. *Let A and B be sets. With the Axiom of Extensionality, we have to prove two inclusions. So let $x \in \pi_1\,(A, B)$. After deconstructing π_1 with the Axiom of Union and the elimination rule for intersections, we have a set C containing x with the property that $C \in D$ for every element $D \in (A, B)$. So in particular, C is an element of $\{A\}$, as $\{A\} \in (A, B)$ from the definition. Since the only element of $\{A\}$ is A itself, we obtain $C = A$ and hence $x \in A$.*

Now let $x \in A$. To show $x \in \pi_1\,(A, B)$ we can apply the Axiom of Union and have to find a set C with $x \in C$ and $C \in \bigcap (A, B)$. With $C \coloneqq A$ and the introduction rule for intersections we have to show $A \in D$ for every element $D \in (A, B)$. From the Axiom of Pairing follows that $D = \{A\}$ or $D = \{A, B\}$ and in both cases we obtain $A \in D$ by another use of the axiom. □

The definition of the second projection is a little more involved since we have to find the set occurring in only one of the pair's elements (unless both are equal). Exploiting the fact that $A = B$ whenever $\bigcup (A, B) = \bigcap (A, B)$ we can use the following definition:

Definition 1.8. $\pi_2\, p \coloneqq \bigcup \{\, x \in \bigcup p \mid x \in \bigcap p \Rightarrow \bigcup p = \bigcap p \,\}$

Now π_2 yields the one element of the union only being element of the intersection if both components of the pair are the same. With this intuition, we consider the formal proof:

Lemma 1.11. $\forall\, A\, B.\, \pi_2\, (A, B) = B$

Proof. *For arbitrary sets A and B we again have to show two inclusions. The assumption $x \in \pi_2\,(A, B)$ together with the Axiom of Union and the Axiom of Specification yield a set C with $x \in C \in \bigcup (A, B)$ and $C \in \bigcap (A, B) \Rightarrow \bigcup (A, B) = \bigcap (A, B)$. Now we eliminate the union and obtain the two cases $C \in \{A\}$ and $C \in \{A, B\}$. The two cases only allow $C = A$ or $C = B$ whereof the second case directly leads to $x \in B$. In the case $C = A$, the specific property of C yields $\bigcup (A, B) = \bigcap (A, B)$ since $A \in \bigcap (A, B)$ as shown in the proof of Lemma 1.10. Now from the fact mentioned above, $A = B$ follows and hence $x \in B$ is proven.*

Let now $x \in B$. To prove $x \in \pi_2\,(A, B)$ we eliminate the outer union and specification and reduce to $B \in \bigcup (A, B)$ and $B \in \bigcap (A, B) \Rightarrow \bigcup (A, B) = \bigcap (A, B)$. The first *property follows from $B \in \{A, B\} \in (A, B)$ coming from the Axiom of Pairing. The second property is another consequence of the fact above, since $B \in \bigcap \{A, B\}$ implies $A = B$ using $B \in \{A\} \in (A, B)$.* □

Given the two projections, we are able to prove a common characterisation of orderer pairs:

Lemma 1.12. $\forall\, A\, B\, C\, D.\ (A, B) = (C, D) \Leftrightarrow A = C \wedge B = D$

Proof. *Let A, B, C and D be sets with $(A, B) = (C, D)$. With the correctness of π_1 we can reduce $A = C$ to $\pi_1\,(A, B) = \pi_1\,(C, D)$. This equality follows from the assumed equality of the pairs. The same works with $B = D$ and π_2 respectively. If we assume $A = C$ and $B = D$ on the other hand, the related pairs are equal.* □

We close this section with the introduction of the cartesian product $A \times B$. Usually, the product $A \times B$ is defined as the set of all pairs with left component in A and right component in B. Unfortunately we have no means to directly translate this intuition into a proper definition, as the "set of all pairs" is an inconsistent concept. So we have to use another definition and put a little formal effort into obtaining the desired results:

Definition 1.9. $A \times B := \bigcup\limits_{x \in A} \{\, (x, y) \mid y \in B \,\}$

First of all, we have to justify the concept of an indexed union. In the usual case of $\bigcup A$, the operation simply collects all $s \in S \in A$. Given the set A, we can also apply a replacement first, that transforms the elements $x \in A$ into sets S_x - in the given example this is $x \mapsto \{\, (x, y) \mid y \in B \,\}$. Now the indexed union is the collection of all $s \in S_x \in A'$, where A' is the resulting set after the replacement.

With the given definition, the components now have proper bounds and the resulting product only contains pairs. We prove the introduction and elimination rule of the new definition in one go:

Lemma 1.13. $\forall\, A\, B\, p.\, p \in A \times B \Leftrightarrow \exists\, x\, y.\, x \in A \wedge y \in B \wedge p = (x, y)$

Proof. *Let A and B be sets and $p \in A \times B$. A first application of the Axiom of Union and the Axiom of Replacement yields a set C of the form $\{\, (x, y) \mid y \in B \,\}$ for an $x \in A$ with $p \in C$. A second application of the Axiom of Replacement for $p \in C$ yields the corresponding $y \in B$ with $p = (x, y)$.*

Let now $x \in A$, $y \in B$ and $p = (x, y)$. With the similar applications of the same axioms in inverse order, we first obtain $p \in \{\, (x, y) \mid y \in B \,\}$ for our particular x and finally $p \in A \times B$. □

Now it is a consequence that ordered pairs respect the bounds of the product:

Lemma 1.14. $\forall\, A\, B\, x\, y.\ (x, y) \in A \times B \Leftrightarrow x \in A \wedge y \in B$

Proof. *Let A and B be sets and $(x, y) \in A \times B$. Lemma 1.13. yields sets a and b with $a \in A$, $b \in B$ and $(x, y) = (a, b)$. From the last equation and Lemma 1.12 it follows that $x = a$ and $y = b$. We derive $x \in A$ and $y \in B$. If we assume $x \in A$ and $y \in B$ we directly obtain $(x, y) \in A \times B$ from Lemma 1.13.* □

The common notation $A \times B = \{ (x, y) \mid x \in A \wedge y \in B \}$ is now sufficiently justified. These results together with the correctness of the projections allow to reformulate the characteristic rules:

Lemma 1.15. $\forall A\, B\, p.\, p \in A \times B \Leftrightarrow \pi_1\, p \in A \wedge \pi_2\, p \in B \wedge p = (\pi_1\, p, \pi_2\, p)$

Proof. *Let A and B be sets and $p \in A \times B$. Lemma 1.13 yields sets $x \in A$ and $y \in B$ with $p = (x, y)$. We obtain $\pi_1\, p = x$ from Lemma 1.10 and $\pi_2\, p = y$ from Lemma 1.11 and conclude $\pi_1\, p \in A$ and $\pi_2\, p \in B$. Finally $p = (x, y) = (\pi_1\, p, \pi_2\, p)$ with Lemma 1.12. Now let $\pi_1\, p \in A$, $\pi_2\, p \in B$ and $p = (\pi_1\, p, \pi_2\, p)$. A single use of Lemma 1.13 justifies $p \in A \times B$.* □

The last property $p = (\pi_1\, p, \pi_2\, p)$ can be considered as the η-law of ordered pairs. As a direct consequence, we obtain monotonicity of the product operation:

Lemma 1.16. $\forall A\, B\, C\, D.\, A \subseteq C \Rightarrow B \subseteq D \Rightarrow A \times B \subseteq C \times D$

Proof. *Let $A \subseteq C$, $B \subseteq D$ and $p \in A \times B$. The first direction of Lemma 1.15 yields $\pi_1\, p \in A$, $\pi_2\, p \in B$ and $p = (\pi_1\, p, \pi_2\, p)$. From the assumptions we obtain $\pi_1\, p \in C$ and $\pi_2\, p \in D$ and the inverse direction of the same lemma gives $p \in C \times D$.* □

Up to this point, our theory contains all usual constructions of pure set theory. We have considered some formalized proofs in detail and illustrated the role of classical reasoning in this setting. In the following sections, we extend our development to include orderings, functions and ordinals. The corresponding proofs will be given at a higher level of abstraction to emphasize the mathematical content and not to get bogged down with low-level details.

4.2 Relations and Functions

4.2.1 Definitions and Properties

We begin this section with the general definition of relations:

Definition 2.1. Let A and B be sets. We call a set $R \subseteq A \times B$ a *(binary) relation* on $A \times B$. We call A the *set of departure* and B the *set of destination*. We define the *domain*, *range* and *field* of R as follows:

(1) $\mathit{dom}\, R := \{ \pi_1\, p \mid p \in R \}$

(2) $\mathit{ran}\, R := \{ \pi_2\, p \mid p \in R \}$

(3) $\mathit{field}\, R := \mathit{dom}\, R \cup \mathit{ran}\, R$

We consider a number of standard properties:

Definition 2.2. Let R and A be sets. We define the following:

(1) R is *symmetric* $:= \forall\, a\, b.\ (a, b) \in R \Rightarrow (b, a) \in R$

(2) R is *asymmetric* $:= \forall\, a\, b.\ (a, b) \in R \Rightarrow (b, a) \notin R$

(3) R is *antisymmetric* $:= \forall\, a\, b.\ (a, b) \in R \Rightarrow (b, a) \in R \Rightarrow a = b$

(4) R is *transitive* $:= \forall\, a\, b\, c.\ (a, b) \in R \Rightarrow (b, c) \in R \Rightarrow (a, c) \in R$

(5) R is *reflexive* on $A := \forall\, a \in A.\ (a, a) \in R$

(6) R is *irreflexive* $:= \forall\, a.\ (a, a) \notin R$

(7) R is *linear* on $A := \forall\, a, b \in A.\ (a, b) \in R \vee (b, a) \in R \vee a = b$

We can form different combinations of those properties and thus obtain two special kinds of relations:

Definition 2.3. We call every symmetric, reflexive and transitive relation on $A \times A$ an *equivalence* on A. We use the symbol $\equiv_A$ for equivalences on A or simply $\equiv$ whenever the carrier is clear from the context.

While equivalence relations are not going to play a major role in the following formalisation, we do take a closer look at orderings:

Definition 2.4. We call every asymmetric, transitive and linear relation on $A \times A$ a *(linear) ordering* on A. We use the symbol $<_A$ for orderings on A or simply $<$ whenever the carrier is clear from the context.

Note that we use asymmetry instead of the more common properties antisymmetry and reflexivity. This causes our orderings to be strict since asymmetry implies irreflexivity and antisymmetry (Lemma 2.1), which has several consequences. Somewhat adversely is the fact that we loose the equality of the field of the ordering and the ordered set itself. For instance, the empty ordering with empty field becomes an ordering for every singleton in our case. However, since our main focus is on well-orderings and one prominent well-ordering will turn out to be set-membership in a regular set theory, we are primarily interested in the strict case. Clearly we can transform one into the other via union or complement with the identity relation.

We clarify the dependencies with the following lemma:

Lemma 2.1. Let R be a set. The following statements hold:

(1) R is asymmetric $\Rightarrow$ R is irreflexive and antisymmetric

(2) R is irreflexive and antisymmetric $\Rightarrow$ R is asymmetric

(3) R is irreflexive and transitive $\Rightarrow$ R is asymmetric

We omit the simple proofs and remark that the third statement allows for the alternative approach to demand irreflexivity instead of asymmetry. Now we can define well-orderings:

Definition 2.5. We call every well-founded ordering $<_A$ a *well-ordering* on A. An ordering $<_A$ is *well-founded* if every non-empty subset $B \subseteq A$ has a unique $<_A$-least element. A set $x \in B$ is $<_A$*-least* for B, if for every element $y \in B$ either $x = y$ or $x <_A y$ holds.

We write $\mathcal{WO}\,(A, <)$ to indicate that $<$ is a well-ordering on A. We write $\mathcal{WO}\;A$ if there exists an ordering that is a well-ordering on A.

Well-orderings are a key concept of this thesis. We call the resulting sets *embedded relations*, since they encode the abstract notion of a relation on sets as sets. The embedded definition allows to give the proof of the Well-Ordering Theorem exclusively at the object-level which allows us to study the proof strategies given in common textbooks. An alternative approach would consider meta-theoretic relations of type $set \Rightarrow set \Rightarrow Prop$ which lead to a more concise development (see Section 5.1). These can be re-embedded into the object-theory, a method we will later demonstrate with meta-level functions. However, the idea is to stay at the object-level, to formalise the embedded theory of relations and functions and to obtain a result of ZF and not of CiC.

Consequently, we move on to the relevant properties that will allow us to define an embedded notion of functions:

Definition 2.6. Let f, A and B be sets. We define the following:

(1) f is *total* on $A \times B := \forall\, x \in A.\, \exists\, y \in B.\ (x, y) \in f$

(2) f is *functional* $:= \forall\, a\, b\, b'.\ (a, b) \in f \Rightarrow (a, b') \in f \Rightarrow b = b'$

(3) f is *surjective* on $A \times B := \forall\, y \in B.\, \exists\, x \in A.\ (x, y) \in f$

(4) f is *injective* $:= \forall\, a\, a'\, b.\ (a, b) \in f \Rightarrow (a', b) \in f \Rightarrow a = a'$

(5) f is *bijective* on $A \times B := f$ is surjective and injective

It is clear that the domain of total relations is the full set of departure and the range of surjective relations is the full set of destination respectively. Different combinations of these properties lead to a number of particular kinds of functions. We add helpful notation and obtain the common results:

Definition 2.7. Let f, A and B be sets. We define the following:

(1) f is a *function* from A to $B := f\colon A \to B := f$ is a total functional relation

(2) f is a *surjection* from A to $B := f\colon A \twoheadrightarrow B := f$ is a surjective function

(3) f is an *injection* from A to $B := f\colon A \hookrightarrow B := f$ is a injective function

(4) f is a *bijection* from A to $B := f\colon A \xrightarrow{\sim} B := f$ is a bijective function

As an essential terminology, we call two sets A and B *equipotent* and write $A \sim B$, whenever there exists a bijection from A to B. The meta-relation $\sim$ is an equivalence on the type set and the respective equivalence classes form the basic concept of *cardinal numbers*.

We prove two lemmas that specify how the properties of functions are preserved whenever we expand the set of departure or the set of destination. The easy case is the expansion of the set of destination, since it is only a bound for the actual range:

Lemma 2.2. $(f\colon A \to B) \Rightarrow B \subseteq B' \Rightarrow (f\colon A \to B')$

Proof. *Let $f\colon A \to B$ and $B \subseteq B'$. From our definition, we know that f is a relation on $A \times B$, total on $A \times B$ and functional. We have to prove the same for the expanded set of destination. Lemma 1.16 yields that f is a relation on $A \times B'$. Totality is trivial since we simply use the same $y \in B$ for every $x \in A$ and functionality is already an assumption.* □

Clearly the same idea does not work with the set of departure because we demand all functions to be total. We preserve totality, however, if we add pairs to the function:

Lemma 2.3. $(f\colon A \to B) \Rightarrow x \notin A \Rightarrow y \in B \Rightarrow (f \cup \{(x, y)\} : A \cup \{x\} \to B)$

Proof. *Let $f\colon A \to B$, $x \notin A$ and $y \in B$. We set $f' := f \cup \{(x, y)\}$ and $A' := A \cup \{x\}$. Again we have to prove the three properties of our definition.*

Let $p \in f'$. Lemma 1.9 allows two cases. In the case $p \in f$ we have $p \in A \times B$ since f is a relation on $A \times B$. From Lemma 1.16 we know $A \times B \subseteq A' \times B$ and thus $p \in A' \times B$. In the case $p = (x, y)$ we obtain $p \in A' \times B$ from Lemma 1.14. Totality and functionality both follow from similar case distinctions of $x \in A'$. □

4.2.2 Application and Restriction

Once we have a representation of functions, we can move to the basic operations on functions. The key-concept of a function is surely the application to arguments. Informally, it is enough to introduce the value $f(x)$ as the unique y with $(x, y) \in f$. With description we could give a corresponding definition, but there is a more constructive way. We first define the application function:

Definition 2.8. $@\, f\, x := \bigcup \{\, \pi_2\, p \mid p \in f \wedge \pi_1\, p = x \,\}$

Note that we define $@\, f\, x$ for every f and x and do not care how the function behaves on ill arguments. We simply identify $f(x)$ with $@\, f\, x$ and proof the following correctness lemma:

Lemma 2.4. $(f\colon A \to B) \Rightarrow x \in A \Rightarrow (x, f(x)) \in f \wedge f(x) \in B$

Proof. *Let $f\colon A \to B$ be a function and $x \in A$. Since f is total, we have $y \in B$ with $(x, y) \in f$. It remains to show that $y = f(x)$. Since f is functional, the p with $\pi_1\, p = x$ is unique and thus equal to (x, y). Hence the only element of $\{\, \pi_2\, p \mid p \in f \wedge \pi_1\, p = x \,\}$ is y and we obtain $f(x) = \bigcup\{y\} = y$. The second part $f(x) \in B$ is an instance of Lemma 1.14.* □

We conclude a further possible transformation of the set of destination:

Lemma 2.5. $(f\colon A \to B) \Rightarrow (\forall\, a \in A.\, f(a) \in C) \Rightarrow (f\colon A \to C)$

Another important operation is the *restriction* of functions and relations to subsets of their set of departure or field respectively. Intended for functions, we define the following:

Definition 2.9. $f|_A := \{\, p \in f \mid \pi_1\, p \in A \,\}$

We can proof that functional restriction respects all properties but surjectivity:

Lemma 2.6. The following hold:

(1) $(f\colon A \to B) \Rightarrow A' \subseteq A \Rightarrow (f|_{A'}\colon A' \to B)$

(2) $(f\colon A \hookrightarrow B) \Rightarrow A' \subseteq A \Rightarrow (f|_{A'}\colon A' \hookrightarrow B)$

Proof. *Let $f\colon A \to B$ be a function and $A' \subseteq A$. Then the demanded properties of $f|_{A'}$ are trivial consequences of the respective features of f. If f is injective, so is $f|_{A'}$.* □

In the case of relations, we define the restriction for equal set of departure and destination since our main focus is on orderings:

Definition 2.10. $R|_A := \{\, p \in R \mid p \in A \times A \,\}$

When forming a relational restriction, all properties of orderings are presevered:

Lemma 2.7. $\mathcal{WO}\,(A, <) \Rightarrow A' \subseteq A \Rightarrow \mathcal{WO}\,(A', <|_{A'})$

Proof. *Let $<$ be a well-ordering on A and $A' \subseteq A$. The respective properties of $<_{A'}$ are obviously inherited.* □

Using restriction, we can lift functional application to sets of arguments:

Definition 2.11. $f\{A\} := \{\, \pi_2\, p \mid p \in f|_A \,\}$

We call the set $f\{A\}$ the *image* of A under f. It is easy to see that the image is bounded by the set of destination, whenever f is a function:

Lemma 2.8. $(f\colon A \to B) \Rightarrow \forall\, C.\, f\{C\} \subseteq B$

Proof. *Let $f\colon A \to B$ be a function, C an arbitrary set and $y \in f\{C\}$. We obtain $p \in f$ with $y = \pi_2\, p$ from the definition of the image. Since f is a relation on $A \times B$, we conclude $p \in A \times B$ and hence $y \in B$.* □

Note that we can make every function surjective by shrinking its set of destination to the image of its set of departure. Moreover, we preserve bijectivity if we restrict both the function and its bounding sets to the respective subsets:

Lemma 2.9. The following hold:

(1) $(f\colon A \to B) \Rightarrow (f\colon A \twoheadrightarrow f\{A\})$

(2) $(f\colon A \xrightarrow{\sim} B) \Rightarrow A' \subseteq A \Rightarrow (f|_{A'}\colon A' \xrightarrow{\sim} f\{A'\})$

Proof. *Let $f\colon A \to B$ be a function. Due to the definition of $f\{A\}$ it is obvious that f is a surjection from A to $f\{A\}$. Now let $f\colon A \overset{\sim}{\to} B$ be a bijection and $A' \subseteq A$. By Lemma 2.6, the set $f|_{A'}$ defines an injection from A' to B. Then (1) concludes the proof.* □

A direct consequence is the following property of equipotent sets:

Lemma 2.10. $A \sim B \Rightarrow A' \subseteq A \Rightarrow \exists\, B' \subseteq B.\, A' \sim B'$

Proof. *Let $f\colon A \overset{\sim}{\to} B$ be a bijection and $A' \subseteq A$. We set $B' := f\{A'\}$. Lemma 2.8 states that $B' \subseteq B$ and Lemma 2.9 states that $f|_{A'}\colon A' \overset{\sim}{\to} B'$.* □

4.2.3 Inverse, Composition and Identity

Next we want to prove the three equivalence properties of $\sim$. In the following paragraphs, we introduce the three necessary constructions. Given some preconditions, we can form the *inverse* and *composition* of functions. We define the inverse via replacement:

Definition 2.12. $f^{-1} := \{\, (\pi_2\, p, \pi_1\, p) \mid p \in f \,\}$

The properties of f and f^{-1} are obviously connected: f^{-1} is functional, whenever f is injective. Moreover, f^{-1} is total if f is surjective. We summarise these dualities in the following lemma:

Lemma 2.11. $(f\colon A \overset{\sim}{\to} B) \Rightarrow \big(f^{-1}\colon B \overset{\sim}{\to} A\big)$

Proof. *Let f be a bijection from A to B. As mentioned above, all properties of f^{-1} are trivially derived from the features of f.* □

We define the *composition* via specification:

Definition 2.13. $f \circ g := \{\, p \in \mathit{dom}\, g \times \mathit{ran}\, f \mid \exists\, b.\ (\pi_1\, p, b) \in g \wedge (b, \pi_2\, p) \in f \,\}$

To obtain a non-empty function $f \circ g$, *dom* f clearly should share some elements with *ran* g. In general, all interesting properties are preserved:

Lemma 2.12. $(f\colon B \overset{\sim}{\to} C) \Rightarrow (g\colon A \overset{\sim}{\to} B) \Rightarrow (f \circ g\colon A \overset{\sim}{\to} C)$

Proof. *Let f be a bijection from B to C and g a bijection from A to B. It is obvious that $f \circ g$ defines a bijection from A to C.* □

By now, we know how to specify functions and how to operate with some simple concepts. Let us now consider a first actual example of an embedded function, namely the canonical *identity function*:

Definition 2.14. $\mathcal{ID}_A := \{\, p \in A \times A \mid \pi_1\, p = \pi_2\, p \,\}$

It is easy to see that $\mathcal{ID}_A$ defines a bijection from A to A.

Lemma 2.13. $(\mathcal{ID}_A \colon A \xrightarrow{\sim} A)$

Proof. *All demanded properties are trivial consequences of the definition of* $\mathcal{ID}_A$. □

Now Lemma 2.11, 2.12 and 2.13 imply the desired result:

Corollary 2.14. The following hold:

(1) $A \sim A$
(2) $A \sim B \Rightarrow B \sim A$
(3) $A \sim B \Rightarrow B \sim C \Rightarrow A \sim C$

Moreover, $\mathcal{ID}_A$ induces a new strategy to prove the equality of sets:

Lemma 2.15. $(\mathcal{ID}_A \colon A \xrightarrow{\sim} B) \Rightarrow A = B$

Proof. *Let* $(\mathcal{ID}_A \colon A \xrightarrow{\sim} B)$ *and* $x \in A$. *By Lemma 2.4,* $\mathcal{ID}_A(x) \in B$. *Now clearly* $\mathcal{ID}_A(x) = x$, *thus we conclude* $A \subseteq B$. *The second inclusion* $B \subseteq A$ *follows analogously with* $(\mathcal{ID}_A)^{-1}$. □

4.2.4 Meta-Functions and Object-Functions

Another thing we have not mentioned so far, is how to compare functions. The typical embedding of functions in ZF implies that they are extensional:

Lemma 2.16. $(f \colon A \to B) \Rightarrow (g \colon A \to C) \Rightarrow (\forall\, x \in A.\, f(x) = g(x)) \Rightarrow f = g$

Proof. *Let* f *be a function from* A *to* B *and* g *a function from* A *to* C *with* $f(x) = g(x)$ *for all* $x \in A$. *Furthermore, let* $(x, y) \in f$. *Since* g *is total, there exists a* $y' \in C$ *with* $(x, y') \in g$. *Now* $y = f(x) = g(x) = y'$ *and hence we conclude* $f \subseteq g$. *The derivation of the second inclusion is analogous.* □

Note that functions can be equal without sharing the same set of destination. The observation of extensionality is very interesting since the type-theoretic functions are usually intensional.

We conclude this section with further remarks concerning the interplay of functions at the two levels. If we reconsider the operation @ from above, we notice that it actually transforms ZF-functions to CiC-functions since it takes a set f as argument and returns the related function F of type $set \Rightarrow set$. A way to construct a transformation in the other direction is the following:

Definition 2.15. $\Lambda\, F\, A := \{\, (a, F\, a) \mid a \in A \,\}$

Since the functions in ZF have to be defined on an existing set whereas the functions in CiC are total on the class of all sets, we have to provide an upper bound A for Λ to obtain the representation f of F. This representation then is a ZF-function from A to a superset of the image of A under F. To make this more precise, we prove the following lemma:

Lemma 2.17. $(\forall\, x \in A.\, F\, x \in B) \Rightarrow (\Lambda\, F\, A \colon A \to B)$

Proof. *Let B be a superset of the image of A under F. Pose $f := \Lambda\, F\, A$. Clearly, f is a relation on $A \times B$. Totality and functionality are obvious consequences of the respective properties of F.*

Now it is easy to infer that related functions at both levels agree on their values:

Lemma 2.18. $(\forall\, x \in A.\, F\, x \in B) \Rightarrow x \in A \Rightarrow F\, x = (\Lambda\, F\, A)\,(x)$

Proof. *Let $F\, x \in B$ for all $x \in A$ and $x \in A$. Lemma 2.17 implies that $f := \Lambda\, F\, A$ is a function from A to B. It thus suffices to show that $(x, F\, x) \in f$ which is justified by the definition of Λ.* □

An interesting property is the following:

Lemma 2.19. $A' \subseteq A \Rightarrow (\Lambda\, F\, A)|_{A'} = \Lambda\, F\, A'$

Proof. *Let $A' \subseteq A$. We apply the Axiom of Extensionality to prove the equality of $(\Lambda\, F\, A)|_{A'}$ and $\Lambda\, F\, A'$. Then both inclusions are trivial. Another equally simple approach is to apply Lemma 2.16 with a short justification of the demanded precondition.* □

Another helpful fact is that transitivity and (bounded) surjectivity of CiC-functions are preserved under embedding into ZF. We will illustrate this strategy with an instance in Section 4.6.

4.3 Ordinal Theory

In this section, we examine a common way to construct ordinals in ZF. We begin with some thoughts on natural numbers and extract their essence to obtain a generalized concept. We discuss several approaches and select one for our formal development.

The original motivations for natural numbers are the two tasks of *counting* (something has n elements) and *ordering* (something is the n^{th} element). The two tasks result in the notion of cardinal and ordinal numbers, which agree in the natural case. With the equipotency relation $\sim$ we have already encountered the generalization of counting. In order to develop a proper definition of ordinals, we first establish a clear definition of the natural numbers that reflects their inductive nature with the first number 0 and a *successor* function S.

In his scientific work, Peano gave an axiomatic characterization of the natural numbers. The respective statements translate the intuition of counting and ordering and yield a formal theory independent from set theory. Frege and Russell defined a number n as the set of all sets with n elements [WR10]. This concept was the first to yield numbers as sets and it is powerful enough to prove Peano's axioms. However, the related formal definition especially of the successor is rather inconvenient, wherefore other constructions are preferred.

In all cases, it is an intuitive choice to define $0 := \emptyset$. A possible successor function S could be $S\,n := \{n\}$. With that function, we obtain the sequence $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\ldots$ where every number is the set of its predecessor. This, however, does not establish the equality of the cardinality of the set and the represented number. The latter property brings some considerable advantages, which is why we actually opt for the following definition:

Definition 3.1. $S\,n := n \cup \{n\}$.

The resulting sequence can be written as $\emptyset, \{0\}, \{0, 1\}\ldots$ to underline that every number is the set of *all* its predecessors.

We now reconsider our Axiom of Infinity. It states the existence of an *inductive* set A, which we required to contain $\emptyset$ and $S\,x$ for all $x \in A$. The smallest such set is exactly the set $\mathbb{N}$ of all natural numbers.

On top of that, we can observe two properties of our natural numbers:

1. Let $n \in \mathbb{N}$ be a natural number. Then for every $m \in n$ we have $m \subseteq n$. We call this property *(set-)transitivity*. The word transitivity is justified since for $m' \in m$ we can conclude $m' \in n$.

2. Every natural number $n \in \mathbb{N}$ is well-ordered by the $\in$-relation. To be more precise, the relation $\in_n := \{\, p \in n \times n \mid \pi_1\, p \in \pi_2\, p \,\}$ is a well-ordering on n. We call the relation $\in_n$ the *membership-ordering* of n.

In a formal setting, one has to distinguish the meta-relation $\in$ from the set $\in_n$ carefully. The former has expressiveness for the class of all sets, the latter only within a given bound. However, we will prove that both relations share the same properties on ordinals. Now we can introduce the announced generalization:

Definition 3.2. We call a set α an *ordinal*, if

(1) α is transitive.

(2) $\in_\alpha$ is a well-ordering on α.

We use the symbol $\mathcal{O}$ for the class of all ordinals and the notation $\alpha \in \mathcal{O}$ for an ordinal α. Consequently, we write $A \subseteq \mathcal{O}$ if A is a set of ordinals. We call $\alpha \in \mathcal{O}$ a *successor* ordinal, whenever there exists an ordinal β with $\alpha = S\,\beta$. Otherwise, we call α a *limit* ordinal.

This is the definition Von Neumann suggested [vN23] and we will encounter one of the multiple alternatives in Section 4.4, where we examine the close correspondence of ordinals and well-orderings.

We have seen that every natural number is an ordinal. Furthermore, even $\mathbb{N}$ is an ordinal and in this context the same set is usually denoted as ω. Now we can construct $S\,\omega$, $S\ (S\,\omega)\ldots$ until we reach the next limit and still obtain ordinals - a *transfinite* generalization of the procedure we know from the natural numbers.

In Section 4.5, we will see that both concepts of induction and recursion apply to ordinals as well.

We now develop the basic features of ordinal theory. We begin with a simple but important property of the membership-ordering:

Lemma 3.1. $\forall\, a, b \in A.\, a \in_A b \Leftrightarrow a \in b$

Proof. *Let $a, b \in A$. The definition of $\in_A$ trivially implies the claimed equivalence.* □

We will use this statement implicitly to give rather concise proofs in the following. The next lemma states that all properties of well-orderings are preserved whenever we shrink a membership-ordering to a subset:

Lemma 3.2. $B \subseteq A \Rightarrow \mathcal{WO}\,(A, \in_A) \Rightarrow \mathcal{WO}\,(B, \in_B)$

Proof. *Let A, B be sets with $B \subseteq A$ and $\in_A$ a well-ordering on A. Since $\in_B = \in_A|_B$ it suffices to show, that $\mathcal{WO}\,(B, \in_A|_B)$. This is an instance of Lemma 2.7.* □

The consequence is the following statement:

Lemma 3.3. $\alpha \in \mathcal{O} \Rightarrow \beta \in \alpha \Rightarrow \beta \in \mathcal{O}$

Proof. *Let $\beta \in \alpha$ for an ordinal α. Lemma 3.2 shows that $\in_\beta$ is a well-ordering on β, which is property (2) of the definition. For property (1), let $\delta \in \gamma \in \beta$. Since α is an ordinal and thus transitive, we know $\beta \subseteq \alpha$ and hence $\gamma \in \alpha$. For the same reason, we obtain $\delta \in \alpha$. We conclude that $\delta \in_\alpha \gamma \in_\alpha \beta$ and end with $\delta \in_\alpha \beta$ since $\in_\alpha$ is transitive. Now we see, that $\delta \in \beta$ and hence $\gamma \subseteq \beta$.* □

A third fact states that proper subsets of ordinals must be elements:

Lemma 3.4. $\alpha \in \mathcal{O} \Rightarrow \beta \in \mathcal{O} \Rightarrow \alpha \subset \beta \Rightarrow \alpha \in \beta$

Proof. *Let $\alpha \subset \beta$ for ordinals α and β. Then $\beta \setminus \alpha$ is a non-empty subset of β and thus has a $\in_\beta$-least element γ. We show that $\alpha = \gamma$ by the two inclusion $\alpha \subseteq \gamma$ and $\gamma \subseteq \alpha$:*

Let $\delta \in \alpha$ and we assume $\delta \notin \gamma$. Since $\in_\beta$ is linear, it must be the case that either $\gamma \in \delta$ or $\gamma = \delta$. Now α is transitive and thus we obtain $\gamma \in \alpha$ in both cases. This contradicts the assumption $\gamma \in \beta \setminus \alpha$.

Assume $\gamma \nsubseteq \alpha$. Then there is $\delta \in \gamma \setminus \alpha$ and hence $\delta \in \beta \setminus \alpha$, but this contradicts that γ was the $\in_\beta$-least element of $\beta \setminus \alpha$. □

We summarize the ordering properties of the membership-relation:

Theorem 3.5. Let α, β and γ be ordinals. The following hold:

(1) $\alpha \notin \alpha$

(2) $\alpha \in \beta \Rightarrow \beta \in \gamma \Rightarrow \alpha \in \gamma$

(3) $\alpha \in \beta \Rightarrow \beta \notin \alpha$

(4) $\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha$

(5) $A \subseteq \mathcal{O} \Rightarrow A \neq \emptyset \Rightarrow \exists\, \alpha \in A.\, \forall\, \beta \in A.\, \alpha \in \beta \vee \alpha = \beta$

Proof. *We successively prove the respective statements:*

(1) *Statement (1) is an instance of Lemma 1.6. However, we can justify (1) without the use of the Axiom of Regularity: If $\alpha \in \alpha$ we have $\alpha \in_\alpha \alpha$ which contradicts the irreflexivity of $\in_\alpha$.*

(2) *Let $\alpha \in \beta$ and $\beta \in \gamma$. Then the transitivity of γ implies $\alpha \in \gamma$.*

(3) *Assume $\alpha \in \beta$ and $\beta \in \alpha$. From (2) we have $\alpha \in \alpha$, which contradicts (1).*

(4) *Consider $\gamma := \alpha \cap \beta$. It is easy to see that γ is an ordinal with $\gamma \subseteq \alpha$ and $\gamma \subseteq \beta$. If $\gamma = \alpha$ or $\gamma = \beta$ we have $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$ respectively. We conclude with Lemma 3.4, that eiter $\alpha = \beta$ or one of $\alpha \in \beta$ and $\beta \in \alpha$ holds. The case $\gamma \subset \alpha$ can not occur together with $\gamma \subset \beta$ since it leads to the contradiction $\gamma \in \gamma$.*

(5) *Let A be a non-empty set of ordinals. Lemma 1.2 allows to pick an $\alpha \in A$. Consider $\lambda := A \cap \alpha$. It holds either $\lambda = \emptyset$ or $\lambda \neq \emptyset$. In the first case, $\beta \notin \lambda$ forall $\beta \in A$. So only the cases $\lambda \in \beta$ and $\lambda = \beta$ of (4) can occur. Hence λ is the least element of A. In the second case, let λ' be the $\in_\alpha$-least element of λ. Now λ' is the $\in$-least element of A.* □

Altogehter, Theorem 3.5 shows that the class of all ordinals is well-ordered by the meta-relation $\in$. The obvious question is whether there exists a set of all ordinals and we thus can construct an object-relation with the same properties. The following lemma shows that there is none:

Lemma 3.6. There exists no set of all ordinals.

Proof. *Suppose $\mathcal{O}$ is a set. The usual strategy is to consider the set $\alpha := S\left(\bigcup \mathcal{O}\right)$, prove it to be an ordinal and to derive $\alpha \notin \mathcal{O}$. If we apply the upcoming Theorem 3.7, however, we can give a much more concise proof.*

Assert that the set $\mathcal{O}$ must be an ordinal itself: $\mathcal{O}$ is transitive since for every $\beta \in \alpha \in \mathcal{O}$ we know $\beta \in \mathcal{O}$ from Lemma 3.3. The hinted theorem yields that the element-ordering of $\mathcal{O}$ is a well-ordering. The consequence is the contradiction $\mathcal{O} \in \mathcal{O}$. □

We conclude this section with two theorems that indicate key strategies for further proofs. The first of them helps to prove that certain sets are ordinals:

Theorem 3.7. $A \subseteq \mathcal{O} \Rightarrow \mathcal{WO}\left(A, \in_A\right)$

Proof. *Let A be a set of ordinals. We prove the five properties of well-orderings:*

(1) *Clearly $\in_A$ is a relation on $A \times A$.*

(2) *Let $\alpha, \beta \in A$ with $\alpha \in_A \beta$ and $\beta \in_A \alpha$. We derive $\alpha \in \beta$ and $\beta \in \alpha$ which is a contradiction to Theorem 3.5. Hence, $\in_A$ is asymmetric.*

(3) *Let now $\alpha, \beta, \gamma \in A$ with $\alpha \in_A \beta$ and $\beta \in_A \gamma$. Then $\alpha \in \beta$ and $\beta \in \gamma$ and thus $\alpha \in \gamma$ from Theorem 3.5. We conclude $\alpha \in_A \gamma$, and so $\in_A$ is transitive.*

(4) *Since all element-ordering are linear, so is $\in_A$.*

(5) *It remains to show that $\in_A$ is well-founded. Therefore, let $\emptyset \neq B \subseteq A$. We apply Theorem 3.5 for B and obtain an $\in$-least $\alpha \in B$. Now α is also $\in_A$-least for B.* □

Now it is easy to proof that the class of ordinals is closed under S and $\bigcup$:

Corollary 3.8. $\alpha \in \mathcal{O} \Rightarrow S\,\alpha \in \mathcal{O}$

Proof. *Let α be an ordinal. We can apply Theorem 3.7 since for every $\beta \in S\,\alpha$ either $\beta \in \alpha$ or $\beta = \alpha$ holds. In the first case, we can use Lemma 3.3 and the second comes from $\alpha \in \mathcal{O}$. So $S\,\alpha$ is well-ordered. The transitivity result is trivial.* □

Corollary 3.9. $A \subseteq \mathcal{O} \Rightarrow \bigcup A \in \mathcal{O}$

Proof. *Let $A \subseteq \mathcal{O}$. We can apply Theorem 3.7 since for every $\beta \in \bigcup A$ there exists an ordinal $\alpha \in A$ with $\beta \in \alpha$. By Lemma 3.3, β is an ordinal and $\bigcup A$ is well-ordered by its element-ordering. The transitivity result is trivial again.* □

These two facts justify that, indeed, the transfinite counting procedure from above, which sequentially forms successors and unions to obtain larger sets, yields ordinals again.

We need the definition of a special ordering to state the second theorem:

Definition 3.3. Let M, α and f be sets. We call the set:

$$<_f := \{\, p \in M \times M \mid f(\pi_1\, p) \in_\alpha f(\pi_2\, p) \,\}$$

the *induced ordering* of f. We do not name the sets M and α explicitly since the ordering $<_f$ will exclusively appear in the context of a function $f\colon M \to \alpha$.

Notice that we will use the letter M to indicate sets of which we examine particular ordering properties. We still use the Letters $A, B, C \ldots$ if we introduce more general concepts. Now we state the following:

Theorem 3.10. $\alpha \in \mathcal{O} \Rightarrow (f\colon M \xrightarrow{\sim} \alpha) \Rightarrow \mathcal{WO}\,(M, <_f)$

Proof. *Let M be a set, α an ordinal and f a bijection from M to α. First, we notice that $<_f$ is a specification of $M \times M$ and hence a relation. All the other properties of a well-ordering can be reduced to the corresponding features of $\in_\alpha$.* □

We instantly obtain a sufficient criterion for well-ordered sets:

Corollary 3.11. $(\exists\, \alpha \in \mathcal{O}.\, M \sim a) \Rightarrow \mathcal{WO}\, M$

In fact, this is the strategy we will use to proof the Well-Ordering Theorem in Section 4.7. In the following section, we set up the framework for the proof of the inverse of Corollary 3.11 that will be given in Section 4.5.

4.4 Order Isomorphy

This section is dedicated to a profound examination of the notion of order isomorphisms. We will first give an abstract theory that will deepen our understanding of orderings. Then we will notice that all results of order isomorphisms yield respective results for ordinal numbers. We begin with the formal definition of *initial segments*:

Definition 4.1. $M[x]_< \coloneqq \{ y \in M \mid y < x \}$

We omit the index $<$ whenever we can infer the right ordering from the context. The following lemma states some basic properties of initial segments:

Lemma 4.1. Let $<$ be a well-ordering on M and $x, y \in M$. The following hold:

(1) $x \notin M[x]$

(2) $x < y \Rightarrow M[x] \subseteq M[y]$

(3) $y < x \Rightarrow (M[x])[y] = M[y]$

(4) $M[x] = M[y] \Rightarrow x \not< y$

(5) $M[x] = M[y] \Rightarrow x = y$

Proof. *We prove the respective statements successively:*

(1) Let $x \in M[x]$. Then $x < x$ is a consequence of the definition. This contradicts the assumption that $<$ is a well-ordering and hence irreflexive.

(2) Let $x < y$ and $z \in M[x]$. Then $z < x$ comes from the definition. The transitivity of $<$ yields $z < y$ and thus $z \in M[y]$.

(3) Let now $y < x$ and $z \in (M[x])[y]$. It follows that $z \in M$ and both $z < x$ and $z < y$ hold. So $z \in M[y]$. Let now $z \in M[y]$. Then $z \in M$ and $z < y$. Transitivity yields $z < x$ and thus $z \in (M[x])[y]$.

(4) Let $M[x] = M[y]$ and assume $x < y$. We have $x \in M[y]$ and therefore $x \in M[x]$ in contradiction to (1).

(5) Let again $M[x] = M[y]$. Since $<$ is linear on M, either $x < y$, $y > x$ or $x = y$ holds. Statement (4) excludes the first two cases. □

In the special case of ordinals, we obtain two more properties:

Lemma 4.2. Let α and β be ordinals. The following hold:

(1) $\beta \in \alpha \Rightarrow \alpha[\beta]_{\in_\alpha} = \beta$

(2) $\alpha = \beta[\alpha]_{\in_\beta} \vee \beta = \alpha[\beta]_{\in_\alpha}$

Proof. *Consider the following:*

(1) Let $\beta \in \alpha$ and $\gamma \in \alpha[\beta]_{\in_\alpha}$. Then $\gamma \in_\alpha \beta$ and thus $\gamma \in \beta$. Let now $\gamma \in \beta$. Since α is an ordinal and hence transitive, we have $\beta \subseteq \alpha$ and hence $\gamma \in \alpha$ and $\gamma \in_\alpha \beta$. So $\gamma \in \alpha[\beta]_{\in_\alpha}$.

(2) By Lemma 3.5, one of the following holds: $\alpha < \beta$, $\alpha = \beta$ or $\alpha > \beta$. The case $\alpha = \beta$ is clear, since $A = A[A]_{\in_A}$ holds for every set A. The two other cases are instances of statement (1). □

If we lift the second statement to the meta-relation $\in$, we obtain that, given two ordinals α and β, one is an initial segment of the other. This is a key insight since it justifies the above intuition of ordinals as the "sets of all its predecessors". Moreover, the fact might remind the reader of the equivalent property of the

γ-sets in Zermelo's first proof. We will encounter more correlations once we approach the last section.

Now we can introduce the announced order isomorphisms:

Definition 4.2. We call $f\colon\ (A,<_1) \xrightarrow{\approx} (B,<_2)$ an *(order) isomorphism*, if

(1) $f\colon A \xrightarrow{\sim} B$

(2) $\forall\, a,b \in A.\, a <_1 b \Leftrightarrow f(a) <_2 f(b)$

Note that we do not demand $<_1$ and $<_2$ to be orderings. We say f is *order-preserving* on A, whenever f satisfies (2). If not declared otherwise, $f\colon A \xrightarrow{\approx} B$ expresses the same for default $<_1$ and $<_2$. We call the pairs $(A,<_1)$ and $(B,<_2)$ *order-isomorphic* and write $(A,<_1) \approx (B,<_2)$ if there exists an isomorphism from A to B and simplify to $A \approx B$ if the respective $<_1$ and $<_2$ exist. Note that $\approx$ is a second meta-equivalence on sets.

At first, we prove the correctness of the last remark:

Lemma 4.3. The following hold:

(1) $(A,<) \approx (A,<)$

(2) $(A,<_1) \approx (B,<_2) \Rightarrow (B,<_2) \approx (A,<_1)$

(3) $(A,<_1) \approx (B,<_2) \Rightarrow (B,<_2) \approx (C,<_3) \Rightarrow (A,<_1) \approx (C,<_3)$

Proof. *It suffices to prove the functions in Lemma 2.14 to be order-preserving:*

(1) This is clear for $\mathcal{ID}_A$, since $\mathcal{ID}_A(a) = a$ for all $a \in A$.

(2) Let $f\colon\ (A,<_1) \xrightarrow{\approx} (B,<_2)$ be the isomorphism from A to B. We prove that f^{-1} respects $<_1$ and $<_2$. Let $a',b' \in B$ with $a' <_2 b'$. Now it remains to show that $f^{-1}(a') <_1 f^{-1}(b')$. Since f is surjective, there are $a,b \in A$ with $f(a) = a'$ and $f(b) = b'$. Now $a <_1 b$ is a consequence because f is order-preserving. As $a = f^{-1}(a')$ and $b = f^{-1}(b')$ we obtain the desired result. The other direction is similar.

(3) Let now f be the isomorphism from A to B and g the isomorphism from B to C. We have to show that $g \circ f$ is order-preserving on A. Let $a,b \in A$ with $a <_1 b$. Since f and g respect the orderings, we obtain $f(a) <_2 f(b)$ and $g(f(a)) <_3 g(f(b))$. We conclude $(g \circ f)(a) <_3 (g \circ f)(b)$. The other direction is again similar. □

Next we encounter an extension of Lemma 2.9:

Lemma 4.4. $\big(f\colon A \xrightarrow{\approx} B\big) \Rightarrow A' \subseteq A \Rightarrow \big(f|_{A'}\colon A' \xrightarrow{\approx} f\{A'\}\big)$

Proof. *Let $f\colon A \xrightarrow{\approx} B$ be an isomorphism with $<_1$ and $<_2$ as related parameters and $A' \subseteq A$. Lemma 2.9 justifies that $f|_{A'}$ is a bijection from A' to $f\{A'\}$. So it remains to show that $f|_{A'}$ is order-preserving. Let $a,b \in A'$ with $a <_1 b$. Since f respects the orderings, we know $f(a) <_2 f(b)$. This is the same as $f|_{A'}(a) <_2 f|_{A'}(b)$ since f and $f|_{A'}$ agree on A'.* □

We conclude with a pending remark concerning the definition of ordinal numbers. In Section 4.3, we announced the existence of at least one alternative. Equipped with the idea of order isomorphy, we can now identify ordinals with the equivalence classes of the relation $\approx$. From this view, we expose ordinals as the abstract "essence" of orderings and thus, in Section 4.6, we will see that, up to isomorphy, *every well-ordered set* is an ordinal.

Furthermore, $\approx$ is clearly a strict refinement of $\sim$. This allows for the insight, that the class of cardinal numbers is a proper subclass of the class of ordinal numbers.

4.5 Induction and Recursion

In this section, we develop two powerful methods that allow substantial reasoning about sets. First, we encounter three versions of the transfinite induction principle and give two application examples. Then we develop a transfinite recursion principle that yields both meta- and object-functions.

4.5.1 Transfinite Induction

The principle of *induction* can be motivated with the following example: Consider a (potentially transfinite) line of dominoes. We are interested in "proving" that *every stone can tip over (1)*. This reduces to a much easier proof obligation, namely that the distance between the stones is small enough, or, more precisely, that *every domino tips over if all its predecessors did so (2)*. Once this condition is fulfilled, we can prove the above claim indirectly: Assume there exist some dominoes that remain upright, then there is a *first one that breaks the cascade (3)*. However, due to the assertion that the fall of all predecessors causes the next stone to tip over, this least unaffected stone must have fallen as well. *Thus the existence of such dominoes has to be rejected (4).*

The above description applies to all well-ordered sets. So proving a certain property of all members of this set can be reduced to proving the *inductive step*, namely that the property holds for an arbitrary member under the assumption that all predecessors already satisfy it. This additional assumption is called *inductive hypothesis*.

It is easy to translate the intuitive concept of dominoes into a formal language: Let M be a set, $<$ an associated well-ordering and P a predicate on sets. We want to prove that *P holds for every x in M (1)*. Assume we have proven that *P holds for x, whenever it holds for every $y < x$ (2)*. Then we can construct the subset $E \subseteq M$ of all x that do not satisfy P. If this set is not empty, it contains, due to the well-foundation property, a *$<$-least element m (3)*. Now it is the case that every predecessor y of m satisfies P and the inductive hypothesis implies $P\,m$ *- a contradiction (4).*

Notice that both the property of well-foundation and the assumption of excluded middle are essential. Moreover, it is possible to generalise the statement to non-linear orderings. What we have just seen, is the proof of the *well-order version* of the induction principle:

Lemma 5.1. $\mathcal{WO}\,(M,<) \Rightarrow (\forall\, x \in M.\ (\forall\, y \in M[x].\, P\, y) \Rightarrow P\, y) \Rightarrow (\forall\, x \in M.\, P\, x)$

The formal proof does not carry further interesting information and we thus prefer to consider one very important instance of Lemma 5.1:

Lemma 5.2. $\alpha \in \mathcal{O} \Rightarrow (\forall\, \beta \in \alpha.\ (\forall\, \gamma \in \beta.\, P\, \gamma) \Rightarrow P\, \beta) \Rightarrow (\forall\, \beta \in \alpha.\, P\, \beta)$

Due to the bound α, we call this principle *bounded transfinite induction*. Note that the phrase "transfinite" indicates the generalised counting we obtain from the ordinal numbers. It is an obvious question whether we can drop the bound and establish an *unbounded transfinite induction* on the proper class $\mathcal{O}$. Theorem 3.5 already states that $\in$ is a linear ordering on $\mathcal{O}$ (parts 1 to 4) that is well-founded on subsets of $\mathcal{O}$ (part 5). Now we generalize (5) to *subclasses* and study the formal proof:

Lemma 5.3. $\neg\,(\forall\, \alpha \in \mathcal{O}.\, P\, \alpha) \Rightarrow \exists\, \alpha \in \mathcal{O}.\, \neg P\, \alpha \wedge \forall\, \beta \in \alpha.\, P\, \alpha$

Proof. *Assume the premise $\neg\,(\forall\, \alpha \in \mathcal{O}.\, P\, \alpha)$. So there exists $\alpha \in \mathcal{O}$ with $\neg P\, \alpha$ and we pose $E := \{\, \beta \in \alpha \mid \neg P\, \alpha \,\}$. Then two cases are possible. In the case $E = \emptyset$, we know that α is the $\in$-least ordinal not satisfying P. So let $E \neq \emptyset$. The ordering $\in_\alpha$ is well-founded and thus there exists a $\in_\alpha$-least element $\lambda \in E$. Now Lemma 3.3 justifies that λ is an ordinal and by construction of E and minimality of λ, every $\beta \in \lambda$ satisfies P.* □

The actual induction principle is now rather simple to justify:

Theorem 5.4. $(\forall\, \alpha \in \mathcal{O}.\ (\forall\, \beta \in \alpha.\, P\, \beta) \Rightarrow P\, \alpha) \Rightarrow (\forall\, \alpha \in \mathcal{O}.\, P\, \alpha)$

Proof. *Assume not all ordinals satisfy P. Lemma 5.3 yields the $\in$-least α with that property. We can derive the contradiction $P\, \alpha$ from the inductive hypothesis.* □

Now we illustrate the application of both well-order induction and bounded transfinite induction. We utilise them to establish that order isomorphy of initial segments and repectively, order isomorphy of ordinals, each imply equality. We begin with the more general statement concerning initial segments:

Lemma 5.5. $\mathcal{WO}\,(M,<) \Rightarrow x, y \in M \Rightarrow (M[x],<) \approx (M[y],<) \Rightarrow M[x] = M[y]$

Proof. *Let M be well-ordered by $<$, $x, y \in M$ and $f\colon (M[x],<) \xrightarrow{\approx} (M[y],<)$ a corresponding isomorphism. We apply Lemma 2.15 and thus have to show that $\mathcal{ID}_{M[x]}$ is a bijection to $M[y]$. We use functional extensionality (Lemma 2.16) to prove that f equals $\mathcal{ID}_{M[x]}$. This means we have to prove $f(z) = z$ for all $z \in M[x]$.*

Consider that, by Lemma 2.7, $M[x]$ is well-ordered by $<|_{M[x]}$. So we can apply the well-order induction principle to the desired goal. Now let $z \in M[x]$. The inductive hypothesis implies $M[z] = M[f(z)]$ and finally part (5) of Lemma 4.1 yields $f(z) = z$. □

Similar as presented in the proof of the induction principles itself, the ordinal statement is a mere consequence. However, we give an independent derivation to allow a better comparison:

Lemma 5.6. $\alpha, \beta \in \mathcal{O} \Rightarrow (\alpha, \in_\alpha) \approx (\beta, \in_\beta) \Rightarrow \alpha = \beta$

Proof. *Let α and β be ordinals and $f\colon (\alpha, \in_\alpha) \xrightarrow{\approx} (\beta, \in_\beta)$ a corresponding isomorphism. As above, it suffices to show $\forall\, \gamma \in \alpha.\, f(\gamma) = \gamma$. We prove this by bounded transfinite induction and therefore we can assume $f(\delta) = \delta$ for all $\delta \in \gamma$. This assumption implies that the initial segments of γ and $f(c)$ are equal, which is equivalent to $f(\gamma) = \gamma$ by Lemma 4.2.* □

We finish the investigation of transfinite induction with a simple corollary that will be of importance in Section 4.6. It states that ordered sets can only be isomorphic to one single ordinal:

Corollary 5.7. $(\exists\, \alpha \in \mathcal{O}.\, (\alpha, \in_\alpha) \approx (M, <)) \Rightarrow (\exists!\, \alpha \in \mathcal{O}.\, (\alpha, \in_\alpha) \approx (M, <))$

Proof. *Let α be an ordinal with $(\alpha, \in_\alpha) \approx (M, <)$. Let β be another ordinal with $(\beta, \in_\beta) \approx (M, <)$. Then the transitivity of $\approx$ yields $(\alpha, \in_\alpha) \approx (\beta, \in_\beta)$ and we conclude $\alpha = \beta$ with Lemma 5.6. So α is unique.* □

4.5.2 Transfinite Recursion

Consider the typical example of a recursive definition, the Fibonacci sequence:

$$f(x) = \begin{cases} 1 & \text{if } x < 2, \\ f(x-1) + f(x-2) & \text{else.} \end{cases}$$

It describes a function $f\colon \mathbb{N} \to \mathbb{N}$ *recursively*, which means that the already assigned values are used to construct the upcoming successors. In our formal context, we clearly do not deal with a proper definition but a kind of algorithmic specification. In this paragraph we address the question of whether the existence of a function f can be derived from a recursive description.

The concept of recursion is closely related to induction. While the goal of induction is the derivation of a *proof* from the corresponding proofs for the predecessors, recursion allows to construct a *function* from partial definitions of earlier stages. In a type theory, induction becomes a mere instance of recursion since the proofs are computational functions as well.

As we have seen above, induction applies to all well-ordered classes. Following the above duality we should also expect the principle of recursive function definitions to apply to these classes. The instances we are about to study here are the sets $\alpha \in \mathcal{O}$ and the class $\mathcal{O}$ itself. We begin with the *unbounded recursion principle* which yields meta-functions on $\mathcal{O}$ and subsequently derive the *bounded* case to obtain proper object-functions. Recall that function on $\mathbb{N}$ are often referred to as *sequences*. We extend this terminology to ordinal domains and frequently add the word *transfinite* to emphasize the generalisation.

Let $G\colon set \Rightarrow set$ be an operation on sets. Our aim is to define a function $F\colon set \Rightarrow set$ with the property:

$$\forall\, \alpha \in \mathcal{O}.\, F\,\alpha = G\,(F|_{\alpha})$$

If we define G as the function that takes a sequence as argument and returns 1 if the length of the sequence is less than 2 or the sum of the two last values otherwise, we obtain exactly the Fibonacci sequence f. Notice the connection between the inductive hypothesis we obtain when we apply an induction principle and the recursive pre-definition $F|_{\alpha}$.

First we have do define the expression $F|_{A}$:

Definition 5.1. $F|_{A} \coloneqq \Lambda\, F\, A$

The basic concept of the recursion theorem will be the notion of computations:

Definition 5.2. Let α and B be sets. We call a function $t\colon (S\,\alpha) \to B$ a *computation of length* α, if for all $\beta \in S\,\alpha$ the equality $t(\beta) = G(t|_{\beta})$ holds. Moreover, we write $t\colon (S\,\alpha) \xrightarrow{\rhd} B$ to indicate this property and $t \rhd \alpha$ if a suitable B exists.

The big picture is to prove by induction, that for all ordinals a unique computation with the respective length exists. Then we can define F with the corresponding images. However, we have to put some effort into maintaining the correct bounds B. We will omit some very technical detail but try to call attention to the formal problems involved.

The first helpful fact we can prove is the equality of computations of same length:

Lemma 5.8. $\alpha \in \mathcal{O} \Rightarrow t \rhd \alpha \Rightarrow u \rhd \alpha \Rightarrow t = u$

Proof. *Let α be an ordinal and $t \rhd \alpha$ and $u \rhd \alpha$ two computations of length α. Recall that both t and u are functions with domain $S\,\alpha$. By Lemma 2.16, it suffices to show $t(\beta) = u(\beta)$ for all $\beta \in S\,\alpha$. We apply bounded transfinite induction (Lemma 5.2) and thus assume for $\beta \in S\,\alpha$ that $t(\gamma) = u(\gamma)$ for all $\gamma \in \beta$. Now we use the property of computations that reduces $t(\beta) = u(\beta)$ to $G\,t|_{\beta} = G\,u|_{\beta}$. This equality holds because of $t|_{\beta} = u|_{\beta}$ which is a consequence of the inductive hypothesis.* □

Now the uniqueness of computations is justified and only the existence remains to be proven. Therefore, we define how to construct computations using the predecessors:

Definition 5.3. Let α be a set, we introduce the following:

(1) $t_{\alpha} \coloneqq desc\ (\lambda\, t.\, t \rhd \alpha)$

(2) $\tau'_{\alpha} \coloneqq \bigcup \{\, t_{\beta} \mid \beta \in \alpha \,\}$

(3) $\tau_{\alpha} \coloneqq \tau'_{\alpha} \cup \{(\alpha, G\,\tau'_{\alpha})\}$

The set τ_α is the continuation of all shorter computations. Once we have ensured the existence of all shorter computations by the inductive hypothesis, τ_α defines an actual computation of length α itself.

We next define appropriate bounds for the two sets τ'_α and τ_α that will serve as the respective sets of destination in the next proofs:

Definition 5.4. Let α be a set, we introduce the following:

(1) $\mathcal{B}_1\,\alpha := \{\,\pi_2\,p \mid p \in \tau'_\alpha\,\}$

(2) $\mathcal{B}_2\,\alpha := (\mathcal{B}_1\,\alpha) \cup \{G\,\tau'_\alpha\}$

Now we can prove that τ'_α is a function and that τ_α even defines a computation. We separate the argumentation into two halves, the first to examine the inductive step and the second to draw the general conclusion via unbounded transfinite induction.

Lemma 5.9. Let $\alpha \in \mathcal{O}$ and $T_\beta \rhd \beta$ a unique computation for all $\beta \in \alpha$.

(1) $\tau'_\alpha \colon \alpha \to \mathcal{B}_1\,\alpha$

(2) $\tau_\alpha \colon (S\,\alpha) \xrightarrow{\rhd} \mathcal{B}_2\,\alpha$

Proof. *Consider the following:*

(1) From the assumption, T_β is the unique computation of length β for all $\beta \in \alpha$. Thus τ'_α is the union of relations on $S\,\beta \times \mathcal{B}_1\,\beta$ and therefore itself a relation on $\alpha \times \mathcal{B}_1\,\alpha$. It is total since for $\beta \in \alpha$, the image $T_\beta(\beta)$ is in $\mathcal{B}_1\,\alpha$ due to $(\beta, T_\beta(\beta)) \in \tau'_\alpha$. Now let $\beta \in \alpha$ and t and u be two computations with length between β and α. Then the images $t(\beta)$ and $u(\beta)$ are equal since computations agree on their arguments. Thus τ'_α is also functional.

(2) By Lemma 2.2, we first derive $\tau'_\alpha \colon \alpha \to \mathcal{B}_2\,\alpha$. We apply Lemma 2.3 and obtain that $\tau_\alpha \colon S\,\alpha \to \mathcal{B}_2\,\alpha$ since it is a one-point expansion of τ'_α. Let β be in $S\,\alpha$. It remains to show that $\tau_\alpha(\beta) = G(\tau_\alpha|_\beta)$. From the construction of τ_α, this is trivial for $\beta = \alpha$. So we can assume $\beta \in \alpha$. Then $\tau_\alpha(\beta) = G\,\tau_\alpha|_\beta$ reduces to $T_\beta(\beta) = G\,T_\beta|_\beta$ which is justified since T_β is a computation itself. □

We finally consider the consequence:

Corollary 5.10. Let α be an ordinal. The following hold:

(1) $\tau'_\alpha \colon \alpha \to \mathcal{B}_1\,\alpha$

(2) $\tau_\alpha \colon (S\,\alpha) \xrightarrow{\rhd} \mathcal{B}_2\,\alpha$

Proof. *We prove the statements in reversed order:*

(2) We apply the unbounded induction principle (Lemma 5.4). Then for all $\beta \in \alpha$ we know $\tau_\beta \colon (S\,\beta) \xrightarrow{\rhd} \mathcal{B}_2\,\beta$. Due to Lemma 5.8, this computation is unique and thus in particular $T_\beta = \tau_\beta$. So we can apply Lemma 5.9 and obtain $\tau_\alpha \colon (S\,\alpha) \xrightarrow{\rhd} \mathcal{B}_2\,\alpha$.

(1) From (2) follows that there exists a unique computation of length α, namely τ_α, for every ordinal α. So the condition of Lemma 5.9 is fulfilled and the statement thus yields $\tau'_\alpha \colon \alpha \to \mathcal{B}_1\,\alpha$ without any further assumptions. □

Now we are able to define the recursive function F:

Definition 5.5. $F\,\alpha := \tau_\alpha\,(\alpha)$

We assert two properties of the restriction $F|_\alpha$:

Lemma 5.11. Let α be an ordinal. Then the following hold:

(1) $F|_\alpha \colon \alpha \to \mathcal{B}_1\,\alpha$

(2) $F|_\alpha = \tau_\alpha|_\alpha$

Proof. *We justify the respective statements:*

(1) We apply Lemma 2.17. Then we have to show that $F\,\beta \in \mathcal{B}_1\,a$ for all $\beta \in \alpha$ which is a simple consequence of the definitions.

(2) Once we have established $F|_\alpha$ as an embedded function in (1), we can apply functional extensionality to prove $F|_\alpha = \tau_\alpha|_\alpha$. So Let β be in α. We have to show that $F|\alpha(\beta) = \tau_\alpha|_\alpha(\beta)$. Due to Lemma 2.18, the left-hand side equals $F\,\beta$ and since computations agree on their arguments, the right-hand side equals $\tau_\beta(\beta)$. Now $F\,\beta = \tau_\beta(\beta)$ is the actual definition of F. □

The remaining proof of the transfinite recursion theorem is rather simple:

Theorem 5.12. $\forall\,G.\,\exists\,F.\,\forall\,\alpha \in \mathcal{O}.\,F\,\alpha = G\,(F|_\alpha)$

Proof. *Let α be an ordinal. With the definition of F and Lemma 5.11 part (2), we have to show $\tau_\alpha(\alpha) = G\,\tau_\alpha|_\alpha$. This is simply the defining property of the computation τ_α.* □

In the last part of this section, we aim to obtain a similar result for embedded functions. This means we assume a set g and construct a second set f such that $f(\beta) = g(f|_\beta)$ for all β in some ordinal α. Note that the object-function f will not be defined for every ordinal, since the domain has to be a set and $\mathcal{O}$ is a proper class (Lemma 3.6). Moreover, obtaining an object-function means to establish a bound B for $f \colon \alpha \to B$. Then g has to be defined on the set of all transfinite sequences with length up to α with values in B. This leads to the following definition of the *sequence space* of α and B:

Definition 5.6. $B^\alpha := \bigcup\limits_{\beta \in \alpha} \{\, f \in \mathcal{P}(\beta \times B) \mid f \colon \beta \to B \,\}$

Now we assume $g \colon B^\alpha \to B$ to be a function with $\alpha \in \mathcal{O}$ and pose $G := @\,g$. Then Theorem 5.12 yields a related function F with $F\,\alpha = G\,F|_\alpha$ for all ordinals α. If we convert this meta-function to object-level, we obtain the function f:

Definition 5.7. $f := F|_\alpha$

Next, we study important properties of our constructs. The first lemma states that f is a function from α to B:

Lemma 5.13. $(f \colon \alpha \to B)$

Proof. *By Lemma 5.11, we obtain $f\colon \alpha \to \mathcal{B}_1\,\alpha$. So it suffices to show that $f(\beta) \in B$ for all $\beta \in \alpha$ (Lemma 2.5). We assert by bounded induction that $\tau_\beta\colon S\,\beta \to B$. From the definition of f and F, we obtain $f(\beta) = \tau_\beta(\beta) \in B$.* □

Then we can justify that f satisfies the recursive characteristic:

Lemma 5.14. $\beta \in \alpha \Rightarrow f(\beta) = g(f|_\beta)$

Proof. *Consider that $f(\beta) \overset{2.18}{=} F\,\beta \overset{5.12}{=} G\,F|_\beta \overset{def}{=} g(F|_\beta) \overset{2.19}{=} g(\Lambda\,F\,\alpha|_\beta) \overset{def}{=} g(f|_\beta)$ holds for every $\beta \in \alpha$.* □

Moreover, f is the only function with this feature:

Lemma 5.15. $(f'\colon \alpha \to B) \wedge (\forall\,\beta \in \alpha.\, f'(\beta) = g(f'|_\beta)) \Rightarrow f = f'$

Proof. *Let f' be a second function of the above behaviour. We apply Lemma 2.16 and thus it remains to show that $f(\beta) = f'(\beta)$ for all $\beta \in \alpha$. So let $\beta \in \alpha$. The bounded induction principle yields $f(\gamma) = f'(\gamma)$ for all $\gamma \in \beta$. We derive $f|_\beta = f'|_\beta$ from functional extensionality. This implies $g(f|_\beta) = g(f'|_\beta)$ which is equivalent to $f(\beta) = f'(\beta)$ due to the characteristics of f and f'.* □

We can now formulate the full theorem:

Theorem 5.16. $\alpha \in \mathcal{O} \Rightarrow (g\colon B^\alpha \to B) \Rightarrow \exists!\, f\colon \alpha \to B. \forall\,\beta \in \alpha.\, f(\beta) = g(f|_\beta)$

Now we are equipped with recursion for both meta- and object-functions. Given the function G or g respectively, we obtain functions F and f that take into account their behaviour on preceding arguments. Defining the Fibonacci sequence as in the introduction becomes possible due to the opportunity to define the algorithmic description with a function that adds the two previous values. In Section 4.7, we will study another function that defines a recursive bijection from an ordinal α to a set M. This will prove the Well-Ordering Theorem.

4.6 Order Types and Hartogs Numbers

In order to establish the main result, we exploit two further concepts, order types and hartogs numbers, which, in addition, provide further insights into the interplay of orderings and ordinals.

Recall that we defined ordinals as transitive sets that are well-ordered by the membership-relation. As announced in Section 4.4, the equivalence classes of $\approx$ are suitable for an alternative definition of ordinals. The concept of order types now yields the connection of both approaches: we will prove that every well-ordered set M is isomorphic to an unique ordinal, the order type o of M. Hence, every well-ordered $\approx$-class contains exactly one ordinal, which can be considered as a highlighted representative.

The hartogs number of a set M is commonly defined as the least ordinal not equipotent ($\sim$) to any subset of M [HJ99]. So the hartogs numbers form special representatives of the $\sim$-classes. They simply denote the next cardinal with respect to a given set in a given equivalence class, which has consequences for the accessibility of ordinals: so far, we only know the successor operation S and its limits to construct new ordinals. While all these successors remain countable, the hartogs numbers form jumps into higher cardinalities. This is the dedicated property we need in Section 4.7.

We remark that we invert the typical way both concepts are introduced. In common text books, order types and hartogs numbers are defined by their characteristic properties. Then their existence is proven. In contrast, we directly give the definition via the corresponding sets and subsequently prove them to satisfy the characterisations. This is possible, since all constituents we make use of are computational objects, partially due to description. So we obtain two independent ordinals that satisfy some interesting properties which are not simply ensured by definition.

4.6.1 Order Types

We define the order type of a set M with respect to $<$ in two steps. First, we specialise M to the set of all $x \in M$ whose initial segments are isomorphic to an ordinal. Then we collect the corresponding ordinals into one set $o\,(M, <)$:

Definition 6.1. Let M and $<$ be sets. We define the following:

(1) $o_x\,(M, <) := desc\ (\lambda\, \alpha.\, \alpha \in \mathcal{O} \wedge (M[x], <) \approx (\alpha, \in_\alpha))$

(2) $M_< := \{\, x \in M \mid \exists\, \alpha \in \mathcal{O}.\ (M[x], <) \approx (\alpha, \in_\alpha) \,\}$

(3) $o\,(M, <) := \{\, o_x\,(M, <) \mid x \in M_< \,\}$

If the set sets M and $<$ are clear from the context, we simply write o_x to indicate $o_x\,(M, <)$ and o to denote the order type $o\,(M, <)$. We use the notation $o_{(\cdot)}$ for the corresponding function of type $set \Rightarrow set$.

Note that this definition unveils the difference of functional and relational replacement, since we have to define the meta-function o_x via description and can not apply the underlying functional relation directly.

We first prove that the order type of a well-ordered set is an ordinal:

Lemma 6.1. $\mathcal{WO}\,(M, <) \Rightarrow o\,(M, <) \in \mathcal{O}$

Proof. *Clearly, o is a set of ordinals. Thus we can apply Lemma 3.7 and obtain that the order type is well-ordered by its membership-relation. So it remains to show that o is transitive. Therefore let $\alpha \in o$ and $\beta \in \alpha$. We want to prove $\beta \in o$. From $\alpha \in o$ it follows that there exists $x \in M$ with an isomorphism $f\colon M[x] \xrightarrow{\approx} \alpha$. Since f is surjective, there exists $y \in M[x]$ such that $f(y) = \beta$. Then Lemma 4.4 justifies that the restriction $f|_{M[y]}$ is an isomorphism from $M[y]$ to β. Now β equals o_y due to the uniqueness of isomorphic ordinals (Corollary 5.7), which results in $\beta \in o$.* □

As announced, we want to justify that the order type $o\,(M,<)$ is the unique ordinal isomorphic to M for well-ordered sets M. The uniqueness already follows from Corollary 5.7. The proof of the isomorphy will be presented in two halves: We first construct an isomorphism from the specification $M_<$ to the order type $o\,(M,<)$. Then we prove that $M_< = M$.

Consider the following definition of the *replacement function* r:

Definition 6.2. $r_{(M,<)} \coloneqq \Lambda\, o_{(\cdot)}\, M_<$

When applied to an $x \in M_<$, the object-function $r_{(M,<)}$ returns the related ordinal o_x which is isomorphic to $M[x]$. In the context of a set $(M,<)$ we also write r for the function $r_{(M,<)}$. If $(M,<)$ is well-ordered, the function r is an isomorphism as announced:

Lemma 6.2. $WO\,(M,<) \Rightarrow \big(r\colon\ (M_<,<) \xrightarrow{\approx} (o,\in_o)\big)$

Proof. *We prove the related properties:*

(1) *Let $(M,<)$ be well-ordered. We first apply Lemma 2.17 to show that r is a function $r\colon M_< \to o$. The set o is defined as the image of $M_<$ under the function $o_{(\cdot)}$ and so it is a correct set of destination for r.*

(2) *We reduce surjectivity and transitivity of r to the same properties of $o_{(\cdot)}$: For every $\alpha \in o$ there exists an $x \in M_<$ such that $o_x = \alpha$ by definition. Hence $o_{(\cdot)}$ is surjective with respect to o. Now let $x, y \in M_<$ with $o_x = o_y$. This means $(M[x],<) \approx o_x = o_y \approx (M[y],<)$. Then the transitivity of $\approx$ (Lemma 4.3) implies that $(M[x],<) \approx (M[y],<)$. We apply Lemma 5.5, obtain $M[x] = M[y]$ and we conclude $x = y$ by Lemma 4.1. Thus r is a bijection.*

(3) *It remains to show that r is order-preserving. So let $x, y \in M_<$. We first assume $x < y$ and justify $o_x \in o_y$. Since $\in$ is linear for ordinals (Lemma 3.5), we only have to reason that the cases $o_x = o_y$ and $o_y \in o_x$ can not occur. As shown above, $o_x = o_y$ implies $x = y$ which contradicts the irreflexivity of $<$. From $o_y \in o_x$ we can derive a contradiction: Let f be the isomorphism from $M[y]$ to o_y. Then the image $f\{M[x]\} \subseteq o_y$ is an ordinal isomorphic to $M[x]$ and thus must be equal to o_x. Since $o_x \neq o_y$, Lemma 3.4 implies $o_x \in o_y$ and the transitivity of o_y results in the inconsistency $o_x \in o_x$.*

(4) *For the inverse direction, let $o_x \in o_y$. The case $x = y$ is impossible since it implies $o_x = o_y$. Moreover, we refute $y < x$ with the same argument as above. Thus $x < y$ must hold and therefore r is an isomorphism as expected.* □

We can now establish the equality of $M_<$ and M:

Lemma 6.3. $\mathcal{WO}\,(M,<) \Rightarrow M_< = M$

Proof. *Let $(M,<)$ be a well-ordered set. Recall that $M_< \subseteq M$. Assume $M_< \neq M$ and x to be the $<$-least element of the non-empty set $M \setminus M_<$. Then $M_< = M[x]$ since $M_<$ contains all elements $z < y$ for $y \in M_<$. This leads to a contradiction: Lemma 6.2 states that $(M_<,<)$ and therefore $(M[x],<)$ is isomorphic to $(o,\in_o)$. So there is an ordinal* *isomorphic to the initial segment $M[x]$, which implies $x \in M_<$ from the definition of $M_<$. Then $x \in M[x]$ holds in contradiction to statement (1) of Lemma 4.1. Thus $M_< = M$ must hold.* □

We combine the results to obtain the actual theorem:

Theorem 6.4. $WO\,(M,<) \Rightarrow \exists!\,\alpha \in \mathcal{O}.\ (M,<) \approx (\alpha, \in_\alpha)$

Proof. *Let $(M,<)$ be a well-ordered set. Then $o\,(M,<)$ is an ordinal isomorphic to $M_<$ (Lemma 6.2) and thus to M itself (Lemma 6.3). The uniqueness is justified by Corollary 5.7.* □

As a consequence, we derive the inverse direction of Corollary 3.11:

Corollary 6.5. $\mathcal{WO}\,(M,<) \Rightarrow \exists\,\alpha \in \mathcal{O}.\, M \sim \alpha$

This concludes our examination of the correspondence of well-ordered sets and ordinal numbers.

4.6.2 Hartogs Numbers

We define the hartogs number h of a set M as the collection of all order types of well-ordered subsets of M. This can be done as follows:

Definition 6.3. Let M be a set. We define *order-space* and *hartogs number*:

(1) $s\,M := \{\, (M',<) \in \mathcal{P}(M) \times \mathcal{P}(M \times M) \mid \mathcal{WO}\,(M',<) \,\}$
(2) $h\,M := \{\, o\,(M',<) \mid (M',<) \in s\,M \,\}$

Note that, due to Lemma 1.13, the notation of ordered pairs as the only elements of the cartesian product causes no formal trouble. Again, as a first fact we prove that the new construct denotes an ordinal:

Lemma 6.6. $h\,M \in Ord$

Proof. *The elements of $h\,M$ have the form $o\,(M',<)$ for well-ordered sets $(M',<)$ and thus are ordinals due to Lemma 6.1. So we can apply Lemma 3.7 again and it remains to prove $h\,M$ transitive. Let $\alpha \in h\,M$ and $\beta \in \alpha$. Then α must be the order type of some well-ordered $(M',<)$ and therefore there exists an isomorphism $f\colon \alpha \xrightarrow{\approx} M'$ that preserves the respective orderings. Since $\beta \in \alpha$ and thus $\beta \subseteq \alpha$, we can pose $M'' := f\{\beta\}$. By Lemma 2.10, $(M'', <_{M''})$ is well-ordered, therefore a member of $s\,M$ and Lemma 4.4 implies that $f|_{M''}$ is an isomorphism from β to M''. Hence β is the order type of $(M'', <_{M''})$ and we conclude $\beta \in h\,M$.* □

Now we can justify that $h\,M$ is indeed not equipotent to any subset of M:

Theorem 6.7. $M' \subseteq M \Rightarrow h\,M \not\sim M'$

Proof. *Let $M' \subseteq M$ be a subset of M with $h\,M \sim M'$. Then there is a bijection $f\colon A' \xrightarrow{\sim} h\,M$. Recall that f induces a well-ordering $<_f$ on M' (Theorem 3.10). From the definition of $<_f$, the bijection f preserves the orderings on both sides and is thus an isomorphism $f\colon\ (M', <_f) \xrightarrow{\cong} (h\,M, \in_{h\,M})$. Moreover, the pair $(M', <_f)$ is a member of $(s\,M)$. Then $o\,(M', <_f)$ is an element of $(h\,M)$ and since isomorphic ordinals are equal, the equality $o\,(M', <_f) = h\,M$ holds. We conclude $h\,M \in h\,M$ - a contradiction.* □

4.7 The Well-Ordering Theorem

This last section presents the proof that the Axiom of Choice implies the Well-Ordering Theorem. The converse will be treated less detailed since, given a well-ordered set, it is easy to construct a related choice function. The first implication is significantly harder and the proof will rely on most of the concepts we have introduced so far. Due to Corollary 3.11, we only have to find an ordinal equipotent to the set in question. The hartogs number of the set provides an upper bound for this ordinal and the requisite bijection can be constructed via transfinite recursion. In the following, we formalise this idea.

First of all, we determine the variant of choice we use:

Definition 7.1. Let M be a set. We define the following:

(1) $\mathcal{P}'(M) := \mathcal{P}(M) \setminus \{\emptyset\}$

(2) $\mathcal{AC}\,M\ := \exists\ (f_\gamma\colon \mathcal{P}'(M) \to M)\,.\forall M' \in \mathcal{P}'(M).\, f_\gamma(M') \in M'$

So we introduce the Axiom of Choice via embedded choice functions.

In order to simplify the upcoming statements, we fix some parameters and abbreviations. We assume M to be a set with $\mathcal{AC}\,M$ and f_γ to be the corresponding choice function. Moreover, we introduce some shorthands:

Definition 7.2. Consider the following definitions:

(1) $\mathcal{B} := S\,M$

(2) $\mathcal{D} := S\,(h\,M)$

(3) $\mathcal{S} := \mathcal{B}^{\mathcal{D}}$

These three sets will serve as bound, domain and space for the next two definitions. Now the idea is to construct a function f that describes the sequence of successive choices we already know from Section 3.1. This means that $f(0)$ shall denote the choice on complete M, $f(1)$ the choice on $M \setminus f(0)$ and so on. To put this more precise, consider the following recursive characterisation:

$$f(\alpha) = \begin{cases} f_\gamma(M \setminus \mathit{ran}\,(f|_\alpha)) & \text{if } M \setminus \mathit{ran}\,(f|_\alpha) \neq \emptyset, \\ \quad M & \text{otherwise.} \end{cases}$$

Then, indeed, the sequence begins with the elements we expect:

$$f \triangleq f_\gamma(M),\ f_\gamma(M \setminus \{f(0)\}),\ f_\gamma(M \setminus \{f(0), f(1)\}) \ldots$$

We have to justify that this sequence exhausts M at some stage $\zeta \in \mathcal{O}$. This means that we define ζ as the first ordinal α with $f(\alpha) = M$, or equivalently $\mathit{ran}\, f|_\alpha = M$, and prove its existence. Then it remains to show that $f|_\zeta$ defines a bijection from ζ to M.

Consider that the values of f are either elements of M or M itself. Hence, the set $\mathcal{B}$ is an appropriate set of destination. Furthermore, we have to pick some ordinal as set of departure. We will see that $\mathcal{D}$ suffices to exhaust M. This is enough to define the function recursively:

Definition 7.3. In the given context, we define

(1) $g := \{\, (f, x) \in \mathcal{S} \times \mathcal{B} \mid (\mathit{ran}\, f)^{\mathsf{c}} \neq \emptyset \wedge x = f_\gamma((\mathit{ran}\, f)^{\mathsf{c}}) \vee (\mathit{ran}\, f)^{\mathsf{c}} = \emptyset \wedge x = M \,\}$

(2) $f := \mathit{desc}\,(\lambda\, f.\ (f \colon \mathcal{D} \to \mathcal{B}) \wedge \forall\, \alpha \in \mathcal{D}.\ f(\alpha) = g(f|_\alpha))$

where $(\mathit{ran}\, f)^{\mathsf{c}}$ denotes the complement of $\mathit{ran}\, f$ relative to M.

Note that g is a function which takes some transfinite sequence f shorter than $\mathcal{D}$ and returns the next suitable element x. By Theorem 5.2, the existence of a unique sequence f that has length $\mathcal{D}$ and agrees with g is justified. We now prove this formally:

Lemma 7.1. All the following hold:

(1) $g \colon \mathcal{S} \to \mathcal{B}$

(2) $f \colon \mathcal{D} \to \mathcal{B}$

(3) $\forall\, \alpha \in \mathcal{D}.\ f(\alpha) = g(f|_\alpha)$

Proof. *We prove the respective statements:*

(1) The set g is clearly a relation on $\mathcal{S} \times \mathcal{B}$ since it is a specification of the product. Now let $f \in \mathcal{S}$. Then either $(\mathit{ran}\, f)^{\mathsf{c}} \neq \emptyset$ or $(\mathit{ran}\, f)^{\mathsf{c}} = \emptyset$ and the pair $\big(f, f_\gamma((\mathit{ran}\, f)^{\mathsf{c}})\big)$ or (f, M) is an element of g, respectively. Hence g is total. Moreover, if $f \in \mathcal{D}$ and $x, x' \in \mathcal{B}$ with both $(f, x)\,, (f, x') \in g$, then either $x = f_\gamma((\mathit{ran}\, f)^{\mathsf{c}}) = x'$ or $x = M = x'$. Thus g is functional and therefore a function.

(2) Note that Lemma 6.6 and 3.8 imply that $\mathcal{D}$ is an ordinal. Then we can apply Theorem 5.16 and obtain the unique existence of a transfinite sequence on $\mathcal{D}$. By the use of description, we give it the name f in the above definition. Then the recursion principle states that $f \colon \mathcal{D} \to \mathcal{B}$.

(3) This is just the second statement of Theorem 5.16. □

An important observation is the following criterion for injectivity of f:

Lemma 7.2. $f|_\alpha$ is injective if $(\mathit{ran}\, f|_\beta)^{\mathsf{c}} \neq \emptyset$ for all $\beta \in \alpha$.

Proof. *Let $(\beta, x)\,, (\beta', x) \in f|_\alpha$. Then $\beta, \beta' \in \mathcal{D}$ since f is a function with domain $\mathcal{D}$ (Lemma 7.1). Since $\mathcal{D}$ is an ordinal, so are β and β'. Lemma 3.5 implies that either $\beta \in \beta'$ or $\beta' \in \beta$ or $\beta = \beta'$. Now assume the case $\beta \in \beta'$. Then $x \in \mathit{ran}\, f|_{\beta'}$ and equivalently $x \notin (\mathit{ran}\, f|_{\beta'})^{\mathsf{c}}$. The assumption $\big(\mathit{ran}\, f|_{\beta'}\big)^{\mathsf{c}} \neq \emptyset$ implies $x = f(\beta') = f_\gamma\big(\big(\mathit{ran}\, f|_{\beta'}\big)^{\mathsf{c}}\big)$,* *which leads to the contradiction $f_\gamma(\big(\mathit{ran}\, f|_{\beta'}\big)^{\mathrm{c}}) \notin \big(\mathit{ran}\, f|_{\beta'}\big)^{\mathrm{c}}$. We refute the case $\beta' \in \beta$ analogously and hence conclude $\beta = \beta'$.* □

Next we define ζ as the $\in$-least ordinal α with $f(\alpha) = \alpha$:

Definition 7.4. We introduce the following:

(1) $E := \{\, \alpha \in \mathcal{D} \mid f(\alpha) = M \,\}$

(2) $\zeta := \mathit{desc}\,(\lambda\, \alpha.\, \alpha \in E \wedge \forall \beta \in E.\, \alpha = \beta \vee \alpha \in \beta)$

Again, we first have to justify ζ to be well-defined. This means that we prove ζ to satisfy the used characterisation:

Lemma 7.3. All the following hold:

(1) $E \neq \emptyset$

(2) $\zeta \in E$

(3) $\forall\, \alpha \in E.\, \zeta = \alpha \vee \zeta \in \alpha$

Proof. *Consider the following:*

(1) We prove that $h\, M \in E$. Assume the opposite. First of all, $f' := f|_{h\, M}$ is a surjection $f' \colon h\, M \twoheadrightarrow f\{h\, M\}$ due to Lemma 2.9. The assumption $h\, M \notin E$ implies $f(h\, M) \neq M$ and hence $f(\alpha) \neq M$ for all $\alpha \in h\, M$. We derive that $M' := f\{h\, M\}$ is a subset of M. Moreover, Lemma 7.2 states that f' is injective. Then f' denotes a bijection from $h\, M$ into a subset M' of M which contradicts Theorem 6.7. Hence, at least $h\, M \in E$

(2) Recall that $\mathcal{D}$ is an ordinal. Thus it is well-ordered and there exist unique $\in_{\mathcal{D}}$-least elements for all non-empty subsets of $\mathcal{D}$. Now (1) justifies that E is such a non-empty subset and hence there exists also the $\in$-minimum. Since it is unique, we can use description to turn it into an object with name ζ, as we have done in the above definition. Then ζ denotes the $\in$-least element of E and thus $\zeta \in E$.

(3) This follows from the second half of the definition of ζ. □

Now we can prove the desired bijectivity of $f|_\zeta$:

Lemma 7.4. $(f|_\zeta \colon \zeta \xrightarrow{\sim} M)$

Proof. *Lemma 2.6 yields $f|_\zeta \colon \zeta \to \mathcal{B}$, since $f \colon \mathcal{D} \to \mathcal{B}$ (Lemma 7.1) and $\zeta \subseteq \mathcal{D}$ (transitivity of $\mathcal{D}$). Now ζ is defined as the least element $\alpha \in \mathcal{D}$ with $f(\alpha) = M$, which is why $f(\alpha) \neq M$ for all $\alpha \in \zeta$. Together with Lemma 7.2, we obtain $f|_\zeta \colon \zeta \hookrightarrow M$. Finally $f(\alpha) = M$ implies $\mathit{ran}\, f|_\zeta = M$ because of Lemma 7.1 and therefore $f|_\zeta$ is surjective.*

We conclude this development with the final theorem:

Theorem 7.5. $\forall\, M.\, \mathcal{AC}\, M \Leftrightarrow \mathcal{WO}\, M$

Proof. *Let M be a set with $\mathcal{AC}\,M$. Let f_γ be the corresponding choice function and f and ζ defined as above. We apply Corollary 3.11 and thus have to give an ordinal that is equipotent to M. Lemma 7.4 justifies that ζ fulfils this property.*

Let now M be well-ordered by $<$. Then there exists a unique $<$-least element $x_{M'}$ for every non-empty subset M' of M. The function f_γ, that maps all M' to the respective $x_{M'}$, obviously defines a choice function. □

Chapter 5
Discussion

5.1 Related Work

Formalised set theory is an ongoing topic in the scientific community. In particular, the respective embeddings of types in sets and vice versa are extensively researched. Werner worked on a general formal approach [Wer97]. He describes a bidirectional encoding of CiC into a stronger form of ZF, where the existence of inaccessible cardinals is assumed, and proved them essentially equivalent. A specific implementation was given by Barras [Bar10], who used Coq to formalise his results about intuitionistic set theory (IZF). Further fundamental work was done by Paulson [Pau93, Pau95] and Aczel [Acz78, Acz98]. Kaiser gave a type-theoretic embedding of Tarski-Grothendieck set theory in Coq [Kai12b].

Moreover, there is some work on the Well-Ordering Theorem done. A formalisation of Zermelo's 1904 proof was given by Ilik in the proof system Agda [Ili06]. This development was translated by Kaiser into Coq [Kai12a]. Zermelo's second proof was found to contain an inductive type by Brown, which lead to a very concise formulation, also in Coq [Bro14]. Both these proofs illustrate the generalisation from well-orderings of sets to well-orderings of types.

Paulson et al proved further equivalences in the surroundings of AC using the assistant Isabelle [PG96]. Besides the approach of formal examinations, Kanamori discusses both proofs and their relevance for set theory and related topics [Kan04, Kan97].

5.2 Future Work

In our development, we have implemented a core library of basic ZF. This allows for extensions in at least two directions. First, we have introduced ordinals but left the definition of cardinals implicitly hidden in the notion of equipotency. This can be changed to study the connection of the two classes of sets. Moreover, both concepts are suitable to examine formal arithmetic. Given our notion of embedded functions and recursion, the algebraic operations like sums and products can be discussed as objects of ZF. Thereby, one could study the relation of embedded ordinals to the naturals in Coq and deepen the interplay of functions at both levels.

Secondly, it is also possible to follow the guideline of Russell's "Principia" and to enlarge the scope of the formalisation. Next conceivable steps are the real numbers, calculus and complex analysis. Once these theories are integrated into a formal development and serve as stable foundations, it would be interesting to investigate formal proofs of further important theorems of mathematics.

We conclude with the remark, that the work concerning the Axiom of Choice itself can be continued. The proof that we have presented in Section 4.7 is in close connection to Zermelo's first proof from 1904 and it should again be possible to justify the equality of the resulting orderings. Lastly, there are further well-known equivalences to the Axiom of Choice, such as Zorn's Lemma. It might allow for interesting insights to formalise the corresponding proofs as well.

Bibliography

[Acz78] Peter Aczel. The Type Theoretic Interpretation of Constructive Set Theory. In Angus Macintyre, Leszek Pacholski, and Jeff Paris, editors, *Logic Colloquium '77*, volume 96 of *Studies in Logic and the Foundations of Mathematics*, pages 55–66. Elsevier, 1978.

[Acz98] Peter Aczel. On relating Type Theories and Set Theories. In *TYPES*, pages 1–18, 1998.

[Bar10] Bruno Barras. Sets in Coq, Coq in Sets. *Formalized reasoning*, 3(1), 2010.

[Bro23] Luitzen E. J. Brouwer. *On the Significance of the Principle of Excluded Middle in Mathematics, Especially in Function Theory*, pages 334–345. toExcel, Lincoln, NE, USA, 1923.

[Bro13] Chad E. Brown. Three Forms of Replacement, 2013. Formal development: http://www.ps.uni-saarland.de/settheory.html.

[Bro14] Chad E. Brown, 2014. Coq scripts received in private communication.

[Can74] Georg Cantor. Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen. *Journal für die reine und angewandte Mathematik*, 77:258–262, 1874.

[Can95] Georg Cantor. Beiträge zur Begründung der transfiniten Mengenlehre. *Mathematische Annalen*, 46(4):481–512, November 1895.

[CH88] Thierry Coquand and Gérard P. Huet. The Calculus of Constructions. *Information and Computation*, 76:95–120, 1988.

[Coh66] Paul J. Cohen. *Set Theory and the Continuum Hypothesis*. Benjamin, 1966.

[Dev79] Keith J. Devlin. *Fundamentals of Contemporary Set Theory*. Springer, 1st edition, 1979.

[Dia75] Razvan Diaconescu. Axiom of Choice and Complementation. *Proceedings of the American Mathematical Society*, 51:176–178, 1975.

[Fra25] Abraham Fraenkel. Untersuchungen über die Grundlagen der Mengenlehre. *Mathematische Zeitschrift*, 22:250–273, 1925.

[Fre79] Gottlob Frege. *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*. Verlag von Louis Nebert, Halle, 1879.

[Fre93] Gottlob Frege. *Grundgesetze der Arithmetik*, volume I. Verlag Hermann Pohle, Jena, 1893.

[Göd31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38(1):173–198, 1931.

[Göd40] Kurt Gödel. The Consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis with the Axioms of Set Theory. *Annals of Mathematical Studies*, 3, 1940.

[GTL89] Jean-Yves Girard, Paul Taylor, and Yves Lafont. *Proofs and Types*. Cambridge University Press, New York, NY, USA, 1989.

[HJ99] Karel Hrbacek and Thomas Jech. *Introduction to Set Theory*. Marcel Dekker Inc, 3rd edition, 1999.

[Ili06] Danko Ilik. Zermelo's Well-Ordering Theorem in Type Theory. In Thorsten Altenkirch and Conor McBride, editors, *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers*, volume 4502 of *Lecture Notes in Computer Science*, pages 175–187. Springer, 2006.

[Kai12a] Jonas Kaiser, 2012. Coq scripts received in private communication.

[Kai12b] Jonas Kaiser. Formal Costruction of a Set Theory in Coq. Master's thesis, Programming Systems Lab, Saarland University, 2012.

[Kan97] Akihiro Kanamori. The Mathematical Import of Zermelo's Well-Ordering Theorem. *The Bulletin of Symbolic Logic*, 3:281–311, 1997.

[Kan04] Akihiro Kanamori. Zermelo and Set Theory. *The Bulletin of Symbolic Logic*, 10:487–553, 2004.

[Kur21] Casimir Kuratowski. Sur la notion de l'ordre dans la Théorie des Ensembles. *Fundamenta Mathematicae*, 2(1), 1921.

[Lam95] Leslie Lamport. How to Write a Proof. *American Mathematical Monthly*, 102:600–608, 1995.

[Luo94] Zhaohui Luo. *Computation and Reasoning: a Type Theory for Computer Science*. Oxford University Press, Inc., New York, NY, USA, 1994.

[ML75] Per Martin-Löf. An Intuitionistic Theory of Types: Predicative Part. *Studies in Logic and the Foundations of Mathematics*, 80:73–118, 1975.

[Nor03] Ulrich Nortmann. *Sprache, Logik, Mathematik*. mentis, 1st edition, 2003.

[Pau93] Lawrence C. Paulson. Set Theory for Verification: I. From Foundations to Functions. *Journal of Automated Reasoning*, 11(3):353–389, 1993.

[Pau95] Lawrence C. Paulson. Set Theory for Verification. II: Induction and Recursion. *Journal of Automated Reasoning*, 15(2):167–215, 1995.

[PG96] Lawrence C. Paulson and Krzysztof Grabczewski. Mechanizing Set Theory. *J. Autom. Reasoning*, 17(3):291–323, 1996.

[PM06] András Prékopa and Emil Molnár. *Non-Euclidean Geometries: János Bolyai Memorial Volume*. Mathematics and its applications. Springer, New York, NY, 2006.

[PPM89] Frank Pfenning and Christine Paulin-Mohring. Inductively Defined Types in the Calculus of Constructions. In *Mathematical Foundations of Programming Semantics*, pages 209–228, 1989.

[Qui37] W. V. Quine. New Foundations for Mathematical Logic. *The American Mathematical Monthly*, 44:70–80, 1937.

[Rus08] Bertrand Russel. Mathematical Logic as based on the Theory of Types. *American Journal of Mathematics*, 30:222–262, July 1908.

[vN23] John von Neumann. *Brief von Johann von Neumann an Ernst Zermelo*. B.I.-Wissenschaftsverlag, 1st edition, 1923.

[Wag85] Stan Wagon. *The Banach-Tarski Paradox*. Cambridge University Press, Cambridge, UK, 1985.

[Wer97] Benjamin Werner. Sets in Types, Types in Sets. In *TACS*, pages 530–346, 1997.

[WR10] Alfred North Whitehead and Bertrand Russell. *Principia Mathematica*. Cambridge University Press, 1st edition, 1910.

[Zer04] Ernst Zermelo. Beweis, daß jede Menge wohlgeordnet werden kann. *Mathematische Annalen*, 59:514–516, 1904.

[Zer08] Ernst Zermelo. Neuer Beweis für die Möglichkeit einer Wohlordnung. *Mathematische Annalen*, 65:107–128, 1908.