Aczel's Type-Theoretic Interpretation of Constructive Zermelo-Fraenkel Set Theory

Dominik Wehr, ILLC, University of Amsterdam
Supervised*by Robert Passmann, ILLC, University of Amsterdam

August 31, 2022†

1 Introduction

In this report, we summarize Peter Aczel's papers [1, 2, 3] on the interpretation of constructive ZF into Martin Löf type theory. We aim to modernize some of the presentation and unify the various constructions into a coherent whole. We begin with a historical overview of intuitionistic logic, based on the article [8] on the same topic of the Stanford Encyclopedia of Philosophy.

In a sense, interest in intuitionistic variants of set theory was sparked by Bishop's "Foundations of constructive analysis" [5]. This work demonstrated how little modification of the definitions and theorems of analysis was required to be able to carry it out in a constructive setting. However, this constructive setting was initially not formally specified in Bishop's work, which motivated multiple logicians to try to fill this gap. The first attempts at this, carried out by Bishop [6] and Goodman and Myhill [14], were closer to systems of arithmetic than set theory. However, these systems were deemed to be unsatisfactory due to their complexity, as expressed by Myhill [19]:

> "We refuse to believe that things have to be this complicated - the argumentation of Bishop [5] looks very smooth and seems to fall directly from a certain concept of what sets, functions, etc. are, and we wish to discover a formalism which isolates the principles underlying this conception in the same way that Zermelo-Fraenkel

*This report was originally created in 2020 in the course of a Master of Logic individual project
†This is an updated version of the report which corrects a mistake in the original version which was pointed out by Hanul Jeon.

set theory isolates the principles underlying classical (nonconstructive) mathematics. We want these principles to be such as to make the process of formalization completely trivial, as it is in the classical case."

While Myhill [18] had already studied some properties of an intuitionistic variant of Zermelo-Fraenkel set theory, this motivation lead Myhill to introduce [19] a novel constructive set theory which was tailored towards Bishop's constructive analysis. Interestingly, this set theory still featured functions and numbers as objects distinct from ordinary sets. Later, Friedman [10] gave various possible set-theoretic foundations for Bishop's constructive analysis. Among them is a system he calls B which is of much weaker proof-theoretic strength than previously considered constructive set theories but can nonetheless be shown to be strong enough to carry out all of Bishop's constructive analysis.

Parallel to this work on set-theoretic foundations for Bishop's "Foundations of Constructive Analysis", Martin-Löf developed a foundation of constructive mathematics on the basis of dependent type theory [16, 17]. This foundation, in a sense which we spell out in Section 2.2, internalized its own Brouwer-Heyting-Kolmogorov interpretation, making its constructivity readily apparent as opposed to the various constructive set-theories where this judgment requires more sophisticated philosophical and mathematical arguments. Aczel's initial work on CZF [1, 2, 3], the subject of this report, can be viewed as an attempt to bridge that gap. He presents a constructive variant of Zermelo-Fraenkel set theory which can be interpreted into a variant of Martin-Löf's dependent type theory, thereby "inhereting" its uncontroversial constructivity.

The remainder of the report is structured as follows: We begin by introducing dependent type theory and constructive Zermelo-Fraenkel set theory in Section 2 and Section 3, respectively. We then split the interpretation of CZF, and its extension, into dependent type theory in a manner similar to Aczel's papers[1, 2, 3]: We begin by interpreting CZF into DTT in Section 4. In Section 5 we cover the interpretation of the regular extension axiom and the associated construction of inductively defined sets. Lastly, Section 6 demonstrates how to interpret various choice principles in DTT. In [3], Aczel gives an inner model construction of CZF with $\Pi\Sigma W I$-PAx over an extension of CZF. We cover this construction in Section 7.

2 Dependent Type Theory

Modern type theory is a field studied in both mathematics and computer science. Broadly, type theories are used to characterize computable functions in terms of their domain and codomain. Mathematicians usually develop type theories to serve as foundations of constructive mathematics whereas computer scientists study type theories in the context of programming language design. As such, there exists a wide range of type theories, each

with different intended applications and thus wildly different properties.

In Section 2.1 we strive to outline the features shared by a class of type theories called dependent type theory. In Section 2.2 we demonstrate how such dependent type theories give rise to foundations of mathematics. We close our exploration of type theory with Section 2.3 by giving the axiomatic definitions of the type theory we employ throughout the rest of this report.

2.1 Naive Dependent Type Theory

As type theories usually focus on computable functions, it is often easier to illustrate their usefulness from the perspective of programming languages. We take this approach to give a "highschool level" overview of dependent types in this section. That is, we give an intuitive introduction to important concepts and constructs, forgoing a proper axiomatization until Section 2.3.

Types are collections of **terms**. We write $t : T$ to mean that the term t is a member of the type T. The internal structure of a type is often very syntactical in nature. As an example, the type of **natural numbers** $\mathbb{N}$ is defined as containing a constant $Z : \mathbb{N}$ and for every $n : \mathbb{N}$ its successor $S\,n : \mathbb{N}$. The natural numbers of type theory can thus be understood as syntactical objects obtained by preceding the letter Z with the letter S finitely many times.

Whenever we have an expression $s(x) : B$ where x is a variable of type A, we can form its **λ-abstraction** $\lambda x.s : A \to B$ inhabiting the type $A \to B$ of functions from type A to type B. A concrete example would be the function $\text{add2} := \lambda x.\, S\,S\,x : \mathbb{N} \to \mathbb{N}$ which increases its argument by 2. In type theory, each kind of type comes equipped with equations which express its **computational behavior**. For example, for $\lambda x.s : A \to B$ and $a : A$ the equation $(\lambda x.s)\,a = s[a/x]$ states that λ-abstractions are applied by replacing the argument variable with the argument in the body of the abstraction. This means, for example, that $\text{add2}\,Z = S\,S\,Z$.

The common notation for a function $f : A \to B$ being applied to an argument $a : A$ in type theory is $f\,a$ instead of the likely more familiar $f(a)$. This stems from how functions with **multiple arguments** usually are formalized in type theory: If $s(x, y) : C$ for $x : A$ and $y : B$ one would define the corresponding function as $\lambda x.\lambda y.s : A \to (B \to C)$. That is, a function mapping values of type A to functions $B \to C$. To apply such an $f : A \to (B \to C)$ to $a : A$ and $b : B$, one can then write $f\,a\,b : C$ instead of the more clumsy $f(a)(b)$.

For any two types A, B we can consider the **product type** $A \times B$ of pairs (a, b) of $a : A$ and $b : B$. It comes equipped with **projections** $\pi_1 : A \times B \to A$ and $\pi_2 : A \times B \to B$ with $\pi_1(a, b) = a$ and $\pi_2(a, b) = b$. Using product types we can recover the more traditional function notation via $\text{uncur} := \lambda f.\lambda p.f\,(\pi_1\,p)(\pi_2\,p) : (A \to B \to C) \to A \times B \to C$. For any $f : A \to B \to C$ we can then compute an $f' := \text{uncur}\,f : A \times B \to C$ which can be

applied as $f'(a,b)$. Note that we have started using the common notational convention that $A \to B \to C$ should be read as $A \to (B \to C)$.

Taking a step back, we can see that a type is characterized by two components. Firstly, some syntactical structure for its members, for example (a,b) for pairs $A \times B$ and λ-abstractions for functions $A \to B$. Secondly, a way of "using" members of the type, such as the π_i of pairs and application of functions, together with equations characterizing their computational behavior. The careful reader might have noticed that we have not yet given the second component for the type $\mathbb{N}$ of natural numbers. It comes with a **recursor** $R_{\mathbb{N}} : A \to (A \to A) \to \mathbb{N} \to A$ for any type A with the equations $R_{\mathbb{N}}\, s\, f\, Z = s$ and $R_{\mathbb{N}}\, s\, f\, (S\, n) = f\, (R_{\mathbb{N}}\, s\, f\, n)$. As the name indicates, it allows us to define functions recursive on the natural numbers. For example, consider the definition of the addition function add on the right-hand side below. The first argument of $R_{\mathbb{N}}$ corresponds to the base case of the usual recursive definition given on the left-hand side. The second argument corresponds to the recursive step of the usual definition, given as a function transforming the result of the recursive call into the desired value.

$$\begin{aligned} \mathrm{add}(0,m) &= m \\ \mathrm{add}(S\,n,m) &= S\,(\mathrm{add}(n,m)) \end{aligned} \qquad\qquad \mathrm{add} := \lambda n.\lambda m.R_{\mathbb{N}}\, m(\lambda x.S\, x)n$$

Note that while $R_{\mathbb{N}}$ may look like primitive recursion, being able to take A to be a function type increases its computational power. For example, the Ackerman function $a : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ can be computed per double-recursion in which the outer recursion computes functions $\mathbb{N} \to \mathbb{N}$ as shown below.

$$\begin{aligned} a\,0\,y &= S\,y \\ a\,(S\,x)\,Z &= a\,x\,1 \\ a\,(S\,x)\,(S\,y) &= a\,n\,(a\,(S\,x)\,y) \end{aligned} \qquad\qquad R_{\mathbb{N}}\,(\lambda y.S\,y)(\lambda f.\lambda n.R_{\mathbb{N}}(f\,1)(\lambda r.f\,r)\,m)\,n$$

Formally, all recursion in type theory is done via recursors such as $R_{\mathbb{N}}$. However, this way of defining is not very friendly to humans as aptly demonstrated by the definition above. We thus opt to give the recursive definitions of this report in the usual equational style while guaranteeing that equivalent definitions can be given via recursors.

So far, the types we have considered are so-called simple types. To be able to form dependent types, we need to add a **type Ty of types**. This means that for example $\mathbb{N} : \mathrm{Ty}$ and if $A, B : \mathrm{Ty}$ then $A \times B, A \to B : \mathrm{Ty}$. An example of a dependent type would then be $\mathrm{vec} : \mathrm{Ty} \to \mathbb{N} \to \mathrm{Ty}$ which is recursively defined via

$$\mathrm{vec}\,A\,Z := I \qquad\qquad \mathrm{vec}\,A\,(S\,n) := A \times \mathrm{vec}\,A\,n$$

where $1 : \mathrm{Ty}$ is the type with exactly one member $I : 1$. The type $\mathrm{vec}\, A\, n$ then describes an n-vector of values of A, for example $\mathrm{vec}\, \mathbb{N}\, 3 = \mathbb{N} \times (\mathbb{N} \times (\mathbb{N} \times 1))$. We call $\mathrm{vec}\, \mathbb{N}\, 3$ a **dependent type** as it *depends* on values of other types, namely $\mathbb{N} : \mathrm{Ty}$ and $3 : \mathbb{N}$. Formally, this means that $A \to B$ is a dependent type as well as it depends on $A, B : \mathrm{Ty}$.

The introduction of dependent types leads us to generalize our notion of functions to **dependent functions**. For $s(x) : B(x)$ with a free variable $x : A$ we define the λ-abstraction $\lambda x.s : \Pi x : A.B(x)$. We can apply $f : \Pi x : A.B$ to an $a : A$ to obtain $f\, a : B[a/x]$. The computational equation is the same as for non-dependent functions. Note that functions $A \to B$ can be expressed as the dependent function $\Pi x : A.B$ where x does not occur in B and are thus subsumed by dependent functions. As an example of a dependent function, consider the function $\mathrm{rep} : \Pi n : \mathbb{N}.A \to \mathrm{vec}\, A\, n$ that, given a natural number n and a value a, generates a vector of length n consisting only of as. To define rep we also need to generalize the type of the recursor of $\mathbb{N}$ to work with types $B(x)$ depending on a parameter from $\mathbb{N}$ to $R_{\mathbb{N}} : B[Z/x] \to (\Pi n : \mathbb{N}.B[n/x] \to B[S\, n/x]) \to \Pi x : \mathbb{N}.B$. Using the generalized recursor, we define $\mathrm{rep} = R_{\mathbb{N}}(\lambda a.I)\ (\lambda n.\lambda v.\lambda a.(a, v\, a)) : \Pi n : \mathbb{N}.A \to \mathrm{vec}\, A\, n$ which corresponds to the recursive equations

$$\mathrm{rep}\, Z\, a = I : \mathrm{vec}\, A\, Z \qquad\qquad \mathrm{rep}\, (S\, n)\, a = (a, \mathrm{rep}\, n\, a) : \mathrm{vec}\, A\, (S\, n)$$

2.2 The Curry-Howard Correspondence

We have observed how different computable functions can be defined in dependent type theory. We now move on to demonstrating how a type-theoretic foundation can reason about them.

We begin with a simple observation: When formalizing the formation and projection rules for members of $A \times B$ the resulting rules look extremely similar to the introduction and elimination rules of $\varphi \wedge \psi$ in a natural deduction system.

$$\frac{a : A \quad b : B}{(a, b) : A \times B} \qquad \frac{p : A \times B}{\pi_1\, p : A} \qquad\qquad \frac{\varphi \quad \psi}{\varphi \wedge \psi} \qquad \frac{\varphi \wedge \psi}{\varphi}$$

Indeed, this similarity extends to other types we have introduced as well: Functions $A \to B$ correspond to implications $\varphi \to \psi$ and the single-value type 1 corresponds to $\top$.

$$\frac{f : A \to B \quad a : A}{f\ a : B} \qquad \frac{\varphi \to \psi \quad \varphi}{\psi}$$

$$\frac{\begin{array}{c}[x : A] \\ \vdots \\ s : B\end{array}}{\lambda x.s : A \to B} \qquad \frac{\begin{array}{c}[\varphi] \\ \vdots \\ \psi\end{array}}{\varphi \to \psi}$$

$$\frac{}{I : 1} \qquad \frac{}{\top}$$

This idea can also used in the other direction: Logical connectives for which we have not yet introduced correspondents for lead us to define new types inspired by the natural deduction rules of said connectives. For example, the correspondent of $\varphi \vee \psi$ is the **sum type** $A + B$ which consists of the members of A and B. The eliminator of $A + B$ then corresponds to the elimination rule of $\varphi \vee \psi$.

$$\frac{a : A}{L\ a : A + B} \qquad \frac{b : B}{R\ b : A + B} \qquad \frac{\varphi}{\varphi \vee \psi} \qquad \frac{\psi}{\varphi \vee \psi}$$

$$\frac{s_l : A \to C \quad s_r : B \to C \quad t : A + B}{R_+\ s_l\ s_r\ t : C} \qquad \frac{\varphi \to \theta \quad \psi \to \theta \quad \varphi \vee \psi}{\theta}$$

Similarly, $\bot$ corresponds to the **empty type** 0, given below. The eliminator R_0 may appear somewhat counterintuitive as it takes a member of 0 as its only argument to produce a member of any type. However, as 0 has no members, this is justified by a similar intuition as the ex falso rule of a natural deduction system: Any context under which it could be used is already in a state of absurdity.

$$\frac{t : 0}{R_0\ t : A} \qquad \frac{\bot}{\varphi}$$

These correspondences together are part of what is called the Curry-Howard correspondence after Haskell Curry and William Howard who are considered the first to observe it[15], although some of the ideas can already be found in Schönfinkel's seminal work [23]. They give rise to the **propositions-as-types interpretation** of logic. The idea is that each type represents a proposition, such as 1 representing $\top$, and each member of a type represents a proof for the represented proposition. As an example, we can consider the term

$$\lambda p.R_+\ (\lambda b.(\pi_1\ p, b))\ (\lambda c.(\pi_1\ p, c))\ (\pi_2\ p) : A \times (B + C) \to (A \times B) + (A \times C)$$

as corresponding to the natural deduction proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\varphi \wedge (\psi \vee \theta)]^{(1)}}{\varphi} \quad [\psi]^{(2)}}{\varphi \wedge \psi}}{(\varphi \wedge \psi) \vee (\varphi \wedge \theta)}}{\psi \to (\varphi \wedge \psi) \vee (\varphi \wedge \theta)} \quad \dfrac{\dfrac{\dfrac{\dfrac{[\varphi \wedge (\psi \vee \theta)]^{(1)}}{\varphi} \quad [\theta]^{(2)}}{\varphi \wedge \theta}}{(\varphi \wedge \psi) \vee (\varphi \wedge \theta)}}{\theta \to (\varphi \wedge \theta) \vee (\varphi \wedge \theta)} \quad \dfrac{[\varphi \wedge (\psi \vee \theta)]^{(1)}}{\psi \vee \theta}}{(\varphi \wedge \theta) \vee (\varphi \wedge \theta)}\,(2)}{\varphi \wedge (\psi \vee \theta) \to (\varphi \wedge \theta) \vee (\varphi \wedge \theta)}\,(1)$$

Indeed, the tree witnessing that the term we gave above has the type $A \times (B + C) \to (A \times B) + (A \times C)$ would be of exactly the same shape as the natural deduction derivation. More generally, one way of looking at the propositions-as-types interpretation is as a compact notation for proofs via typed terms.

If $A, B : \mathrm{Ty}$ represent propositions, then a term of type $P : \mathbb{N} \to \mathrm{Ty}$ can be treated as a **predicate** on the natural numbers. For example,

$$\mathrm{isZero}\ Z := 1 : \mathrm{Ty} \qquad\qquad \mathrm{isZero}\ (S\ n) := 0 : \mathrm{Ty}$$

is the predicate which holds precisely for $Z : \mathbb{N}$ and no other natural number.

Introducing predicates to our propositions-as-types interpretation leads us to another observation: $\Pi x : A.B(x)$ corresponds to $\forall x.\varphi(x)$. In this case, the formal details of the introduction rules differ somewhat as binders and contexts are handled differently in dependent type theory and first-order logic. However, they still clearly serve the same purpose.

$$\frac{\Gamma, x : A \vdash s : B(x)}{\Gamma \vdash \lambda x.s : \Pi x : A.B(x)} \qquad\qquad \frac{\Gamma \vdash \varphi(x) \quad x \text{ does not occur in } \Gamma}{\Gamma \vdash \forall x.\varphi(x)}$$

$$\frac{f : \Pi x : A.B(x) \quad a : A}{f\ a : B(a)} \qquad\qquad \frac{\forall x.\varphi}{\varphi(t)}$$

Similar to the case of $\varphi \vee \psi$ we are lead to introduce a new type as a correspondent of $\exists x.\varphi(x)$. This is the **dependent sum** $\Sigma x : A.B(x)$ whose members are pairs (a, b) where $a : A$ and $b : B(a)$. Again, the elimination rules differ on the technical details concerning the interaction between binders and contexts.

$$\frac{a : A \quad b : B(a)}{(a, b) : \Sigma x : A.B(x)} \qquad \frac{\varphi(t)}{\exists x.\varphi(x)}$$

$$\frac{s : \Pi x : A.\Pi b : B(x).C \quad t : \Sigma x : A.B(x)}{R_\Sigma\, s\, t : C} \qquad \frac{\Gamma, \varphi(x) \vdash \psi \quad \Gamma \vdash \exists x.\varphi(x) \quad x \text{ does not occur in } \Gamma, \psi}{\Gamma \vdash \psi}$$

The last logical connective one would desire from a predicate logic is equality between terms. For some types, such as $\mathbb{N}$, for which equality between terms is decidable, we can combine the observations we have made until now to simply define a recursive predicate $\mathrm{eq}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N} \to \mathrm{Ty}$ describing equality on the basis of the types 0 and 1:

$$\mathrm{eq}_{\mathbb{N}}\, Z\, Z = 1 \qquad \mathrm{eq}_{\mathbb{N}}(S\, n)\, Z = 0 \qquad \mathrm{eq}_{\mathbb{N}}\, (S\, n)\, (S\, m) = \mathrm{eq}_{\mathbb{N}}\, n\, m$$

However, one sometimes may also want to reason about undecidable equalities, such as those between functions $\mathbb{N} \to \mathbb{N}$. This motivates the definition of **identity types**: For every $A : \mathrm{Ty}$ and $a, b : A$ we define $\mathrm{Id}_A(a, b)$ which has a member if $a = b : A$.

$$\frac{}{\mathrm{refl} : \mathrm{Id}_A(a, a)} \qquad \frac{}{s = s}$$

$$\frac{s : A[a/x] \quad t : \mathrm{Id}_A(a, b)}{R_{\mathrm{Id}}\, s\, t : A[b/x]} \qquad \frac{\varphi(s) \quad s = t}{\varphi(t)}$$

The rules for $\mathrm{Id}_A(a, b)$ may require a bit more elaboration. First, note that the first rule could be restated equivalently as

$$\frac{a = b : A}{\mathrm{refl} : \mathrm{Id}_A(a, b)}$$

because terms with $a = b : A$ are treated as indistinguishable on the meta-level. Second, observe that the second rule is a powerful **rewriting rule** which, for example, allows us to prove that $\mathrm{Id}_A(a, b)$ is an equivalence relation. To illustrate, the proof for symmetry is given below

$$\frac{\dfrac{\dfrac{A : \mathrm{Ty}, a : A, b : A, t : \mathrm{Id}_A(a, b) \vdash \mathrm{refl} : \mathrm{Id}_A(x, a)[a/x]}{A : \mathrm{Ty}, a : A, b : A, t : \mathrm{Id}_A(a, b) \vdash t : \mathrm{Id}_A(a, b)}}{A : \mathrm{Ty}, a : A, b : A, t : \mathrm{Id}_A(a, b) \vdash R_{\mathrm{Id}}\, \mathrm{refl}\, t : \mathrm{Id}_A(x, a)[b/x]}}{\lambda A.\lambda a.\lambda b.\lambda t.R_{\mathrm{Id}}\, \mathrm{refl}\, t : \Pi A : \mathrm{Ty}.\Pi a : A.\Pi b : A.\ \mathrm{Id}_A(a, b) \to \mathrm{Id}_A(b, a)}$$

At this point, we may observe that based on what we have laid out, we are able to *state* a lot of properties but still cannot *prove* anything beyond tautologies of (higher-order) predicate logic. For example, recalling our recursive definition of $\mathrm{eq}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N} \to \mathrm{Ty}$ we cannot yet prove that $\mathrm{eq}_{\mathbb{N}}$ is reflexive ($\Pi n : \mathbb{N}.\mathrm{eq}_{\mathbb{N}}\, n\, n$). Indeed, as $\mathrm{eq}_{\mathbb{N}}$ is recursively defined, we could

reasonably expect to need an inductive argument to prove non-trivial facts about it. Recall the recursor $R_{\mathbb{N}} : A(Z) \to (\Pi n : \mathbb{N}.A(n) \to A(S\,n)) \to \Pi n : \mathbb{N}.A(n)$, when interpreting $A(x) : \mathrm{Ty}$ with parameter $x : \mathbb{N}$ as a predicate, this is exactly the **induction scheme** for $\mathbb{N}$! Indeed, in type theory, induction can be simply regarded as recursive proof construction. That means we can prove the reflexivity of $\mathrm{eq}_{\mathbb{N}}$ via

$$p\,Z = I : \mathrm{eq}_{\mathbb{N}}\,Z\,Z \qquad\qquad p\,(S\,n) = p\,n : \mathrm{eq}_{\mathbb{N}}\,(S\,n)\,(S\,n)$$

note that while this proof looks somewhat trivial, the proof's heavy lifting is done by the computational equations $\mathrm{eq}_{\mathbb{N}}\,Z\,Z = 1 : \mathrm{Ty}$ and $\mathrm{eq}_{\mathbb{N}}\,(S\,n)\,(S\,n) = \mathrm{eq}_{\mathbb{N}}\,n\,n : \mathrm{Ty}$ which are needed to derive the proof's type.

Observe also the curios duality of the relationships between induction and recursion in type theory and set theory: In set theory, induction is provided axiomatically, via the axiom of infinity or the set induction principle, and the existence of recursively defined functions is justified by an inductive proof. In type theory, types come equipped with recursors that allow for the definition of recursive functions and induction can then be conceived of as recursive proof construction.

Foundations of mathematics usually consist of a collection of axioms describing basic mathematical objects, like sets or natural numbers, and a logic used to reason about said objects via the axioms. In this section, we have observed that for powerful enough type theories, this distinction collapses, as typed terms do not only represent computations on syntactic objects but may equally represent proofs about said computations. This observation is summarized by the table below:

Logic	Type theory
Propositions	Types
Predicates	Dependent Types
Proofs	Members of Types
Induction	Recursion
$\top$	1
$\bot$	0
$\varphi \wedge \psi$	$A \times B$
$\varphi \vee \psi$	$A + B$
$\varphi \to \psi$	$A \to B$
$\forall x.\varphi(x)$	$\Pi x : A.B(x)$
$\exists x.\varphi(x)$	$\Sigma x : A.B(x)$
$s = t$	$\mathrm{Id}_A(a, b)$

Another way of making sense of the Curry-Howard correspondence is as an instance of the **Brouwer-Heyting-Kolmogorov interpretation** of intuitionistic logic [24]. It, too, yields a computational interpretation of logic, although on a slightly more general

level. The BHK-interpretation identifies each atomic proposition with a collection of its proofs. Proofs of implications are computable proof-transformations, mapping proofs for the premise to proofs of the consequence. The other connectives are interpreted analogously to the Curry-Howard correspondence as well, such as proofs of conjunctions being pairs of proofs. Overall, this means that the internal logic of a type-theoretic foundation as we have laid it out here is constructive as well.

We remark that the Curry-Howard correspondence should not be understood as the handful of correspondences between dependent types and predicate logic we demonstrate in this section, but rather as their underlying pattern: Constructs and properties can often be found in and moved between logic and type theory, often yielding interesting or useful results. For example, linear logic [13] inspired linear types [11] which have proven valuable for characterizing resource management in programming languages. Conversely, Homotopy Type Theory has given rise to the family of univalent foundations of mathematics [26]. Surprisingly, the correspondence is not restricted to intuitionistic logics, as type theories corresponding to classical logic have been found [20]. Often, problems of two corresponding systems, such as cut-elimination in logics and term-normalization in type theories, can be found to be in correspondence as well.

2.3 Formalizing Dependent Type Theory

In this section, we spell out the formal details of the specific dependent type theory we use in the rest of this report. It takes the form of a derivation system for two kinds of judgments: $\Gamma \vdash s : T$ (under context Γ the term s is of type T) and $\Gamma \vdash s = t : T$ (under context Γ the T-terms s and t are equal). Here, contexts are lists of variable-type pairs $x_0 : A_0, x_1 : A_1, ..., x_n : A_n$ where $x_0 : A_0, ..., x_{i-1} : A_{i-1} \vdash A_i : \mathrm{Ty}$ for $0 \leq i \leq n$.

We begin by giving the rules for equality in the system. We write $[s/x]$ or $[A/x]$ to denote the operation replacing all free occurrences of the variable x with the term s or type A, respectively.

$$\frac{\Gamma \vdash s : T}{\Gamma \vdash s = s : T} \qquad \frac{\Gamma \vdash s = t : T \quad \Gamma[s/x] \vdash a[s/x] = b[s/x] : A[s/x]}{\Gamma[t/x] \vdash a[t/x] = b[t/x] : A[t/x]}$$

$$\frac{\Gamma \vdash s = t : T \quad \Gamma[s/x] \vdash a[s/x] : A[s/x]}{\Gamma[t/x] \vdash a[t/x] : A[t/x]}$$

Note that the symmetry and transitivity of $s = t$ follows from second rule.

For an example of the rules associated with a type, consider those for dependent products

$\Pi x : A.B$:

$$\frac{\Gamma \vdash A : \mathrm{Ty} \quad \Gamma, x : A \vdash B : \mathrm{Ty}}{\Gamma \vdash (\Pi x : A.B) : \mathrm{Ty}} \qquad \frac{\begin{array}{c}\Gamma \vdash A : \mathrm{Ty} \quad \Gamma, x : A \vdash B : \mathrm{Ty} \\ \Gamma \vdash C : \mathrm{Ty} \quad \Gamma, x : C \vdash D : \mathrm{Ty} \\ \Gamma \vdash A = C : \mathrm{Ty} \quad \Gamma, x : A \vdash B = D : \mathrm{Ty}\end{array}}{\Gamma \vdash (\Pi x : A.B) = (\Pi x : C.D) : \mathrm{Ty}}$$

$$\frac{\Gamma \vdash (\Pi x : A.B) : \mathrm{Ty} \quad \Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.s : (\Pi x : A.B)}$$

$$\frac{\Gamma \vdash (\Pi x : A.B) : \mathrm{Ty} \quad \Gamma \vdash s : (\Pi x : A.B) \quad \Gamma \vdash t : A}{\Gamma \vdash s\ t : B[t/x]}$$

$$\frac{\Gamma, x : A \vdash s = t : B}{\Gamma \vdash \lambda x.s = \lambda x.t : (\Pi x : A.B)} \qquad \frac{\Gamma \vdash s = s' : (\Pi x : A.B) \quad \Gamma \vdash t = t' : A}{\Gamma \vdash s\ t = s'\ t' : B[t/x]}$$

$$\frac{\Gamma \vdash \lambda x.s : (\Pi x : A.B) \quad \Gamma \vdash t : A}{\Gamma \vdash s\ t = s[t/x] : B[t/x]} \qquad \frac{\Gamma \vdash s : (\Pi x : A.B) \quad x \notin FV(s)}{\Gamma \vdash \lambda x.s\ x = s : (\Pi x : A.B)}$$

The first two rules state what well-formed dependent product types are and when they are equal. The next two rules give types for terms involving dependent products, namely abstraction and application. The two rules after that give structural equalities for abstraction and application. The last two rules give the computational β-equality and η-equality rules for dependent products.

The above example aptly demonstrates that explicitly spelling out all formal details involves writing down a lot of derivation rules, to the point where the central ideas are obscured. We thus take two measures to find a balance between formal correctness and readability of this chapter: Firstly, we from now on omit the structural and η-equality rules as they all follow a simple pattern and we never make explicit use of them in the remainder of this report. Secondly, we omit the Γ and only indicate additions to the Γ in the recursive cases. With these conventions, the rules for $\Pi x : A.B$ are follows.

$$\frac{A : \mathrm{Ty} \quad x : A \vdash B : \mathrm{Ty}}{(\Pi x : A.B) : \mathrm{Ty}} \qquad \frac{(\Pi x : A.B) : \mathrm{Ty} \quad x : A \vdash t : B}{\lambda x.s : (\Pi x : A.B)}$$

$$\frac{(\Pi x : A.B) : \mathrm{Ty} \quad s : (\Pi x : A.B) \quad t : A}{s\ t : B[t/x]} \qquad \frac{\lambda x.s : (\Pi x : A.B) \quad t : A}{s\ t = s[t/x] : B[t/x]}$$

When defining a formal system, it is often useful to have as little redundancy in its rules and axioms as possible as this eases the study of its meta-theory. In the same vein, we omit redundant rules. For example, function types $A \to B$ can be viewed as an instance of $\Pi x : A.B$ in which B does not refer to $x : A$. Indeed, if B is constant and we write $A \to B$ for $\Pi x : A.B$, the rules above become as below, which are precisely the rules we would

have given for $A \to B$. We thus omit explicit rules for $A \to B$ from the system.

$$\frac{A : \mathrm{Ty} \quad B : \mathrm{Ty}}{A \to B : \mathrm{Ty}} \qquad \frac{A \to B : \mathrm{Ty} \quad x : A \vdash t : B}{\lambda x.s : A \to B}$$

$$\frac{A \to B : \mathrm{Ty} \quad s : A \to B \quad t : A}{s\,t : B} \qquad \frac{\lambda x.s : A \to B \quad t : A}{s\,t = s[t/x] : B}$$

Next, we add the rules for dependent sums $\Sigma x : A.B$ to the system.

$$\frac{A : \mathrm{Ty} \quad x : A \vdash B : \mathrm{Ty}}{(\Sigma x : A.B) : \mathrm{Ty}} \qquad \frac{(\Sigma x : A.B) : \mathrm{Ty} \quad a : A \quad a : A \vdash b : B}{(a, b) : (\Sigma x : A.B)}$$

$$\frac{s : (\Sigma x : A.B)}{\pi_1\, s : A} \qquad \frac{s : (\Sigma x : A.B)}{\pi_2\, s : B[(\pi_1\, s)/x]} \qquad \frac{(\Sigma x : A.B) : \mathrm{Ty} \quad a : A \quad a : A \vdash b : B}{\pi_1(a, b) = a : A}$$

$$\frac{(\Sigma x : A.B) : \mathrm{Ty} \quad a : A \quad a : A \vdash b : B}{\pi_2(a, b) = b : B[a/x]}$$

Again, we note that the type $A \times B$ can be defined as $\Sigma x : A.B$ and we thus do not give explicit rules for $A \times B$.

Furthermore, we need to add the finite types 0 and 1, binary sums $A + B$ and the natural

numbers $\mathbb{N}$.

$$\frac{}{0 : \mathrm{Ty}} \qquad \frac{t : 0 \quad A : \mathrm{Ty}}{R_0\, t : A} \qquad \frac{}{1 : \mathrm{Ty}} \qquad \frac{}{I : 1}$$

$$\frac{x : 1 \vdash A : \mathrm{Ty} \quad s : \Pi x : I.A \quad t : 1}{R_1\, s\, t : A[s/x]} \qquad \frac{R_1\, s\, I : A[I/x]}{R_1\, s\, I = s\, I : A[I/x]} \qquad \frac{A : \mathrm{Ty} \quad B : \mathrm{Ty}}{A + B : \mathrm{Ty}}$$

$$\frac{A + B : \mathrm{Ty} \quad a : A}{L\, a : A + B} \qquad \frac{A + B : \mathrm{Ty} \quad b : B}{R\, b : A + B}$$

$$\frac{x : A + B \vdash C : \mathrm{Ty} \quad s_l : \Pi y : A.C[L\, y/x] \quad s_r : \Pi y : B.C[R\, y/x] \quad t : A + B}{R_+\, s_l\, s_r\, t : C[t/x]}$$

$$\frac{R_+\, s_l\, s_r\, (L\, a) : C[L\, a/x]}{R_+\, s_l\, s_r\, (L\, a) = s_l\, a : C[L\, a/x]} \qquad \frac{R_+\, s_l\, s_r\, (R\, b) : C[R\, b/x]}{R_+\, s_l\, s_r\, (R\, b) = s_r\, b : C[R\, b/x]} \qquad \frac{}{\mathbb{N} : \mathrm{Ty}}$$

$$\frac{}{Z : \mathbb{N}} \qquad \frac{n : \mathbb{N}}{S\, n : \mathbb{N}}$$

$$\frac{x : \mathbb{N} \vdash A : \mathrm{Ty} \quad s : A[Z/x] \quad t : \Pi x : \mathbb{N}.\Pi y : A.\ A[S\, x/x] \quad n : \mathbb{N}}{R_{\mathbb{N}}\, s\, t\, n : A[n/x]}$$

$$\frac{R_{\mathbb{N}}\, s\, t\, Z : A[Z/x]}{R_{\mathbb{N}}\, s\, t\, Z = s : A[Z/x]} \qquad \frac{R_{\mathbb{N}}\, s\, t\, (S\, n) : A[S\, n/x]}{R_{\mathbb{N}}\, s\, t\, (S\, n) = t\, n\, (R_{\mathbb{N}}\, s\, t\, n) : A[S\, n/x]}$$

The type $\mathbb{B} := 1 + 1$ of boolean truth values is sometimes of interest. We take $\mathrm{true} := L\, I$, $\mathrm{false} := R\, I$ and $R_{\mathbb{B}} := \lambda x.\lambda y.\lambda b.R_+\, (\lambda\_.x)\, (\lambda\_.y)\, b$. Note that the notation $\lambda\_.s$ should be read as $\lambda x.s$ for some $x \notin FV(s)$. It simply stresses that the argument is ignored.

The identity types Id_A are the last kind of type we have introduced in the previous sections. There are a few slightly different but essentially equivalent ways of axiomatizing them. We stick to the variant used by Aczel in [2].

$$\frac{A : \mathrm{Ty} \quad a : A \quad b : A}{\mathrm{Id}_A(a, b) : \mathrm{Ty}} \qquad \frac{\mathrm{Id}_A(a, b) : \mathrm{Ty} \quad a = b : A}{\mathrm{refl} : \mathrm{Id}_A(a, b)}$$

$$\frac{\begin{array}{c}\mathrm{Id}_A(a, b) : \mathrm{Ty} \quad x : A \vdash B : \mathrm{Ty} \\ s : B[a/x] \quad t : \mathrm{Id}_A(a, b)\end{array}}{R_{\mathrm{Id}}\, s\, t : B[b/x]} \qquad \frac{R_{\mathrm{Id}}\, s\, \mathrm{refl} : B[b/x]}{R_{\mathrm{Id}}\, s\, \mathrm{refl} = s : B[b/x]}$$

The system also includes two kinds of types not discussed in the previous two sections. The first one is a **universe of small types** U. In dependent type theory, a universe is a

type whose members are types as well. Careful readers may have noticed that with the rules given above, types of the form $A \to \mathrm{Ty}$ which we used in Section 2.1 are not valid anymore. This is the case as Ty is no a member of itself. In Proposition 11, we show that $\mathrm{Ty} : \mathrm{Ty}$ would in fact lead to an inconsistency of the system. To alleviate this, we introduce a new type U of "small types" which contains many types we use (see the rules below) and the existence of which is consistent.

$$\frac{}{U : \mathrm{Ty}} \qquad \frac{}{0 : U} \qquad \frac{}{1 : U} \qquad \frac{}{\mathbb{N} : U} \qquad \frac{A : U \quad x : A \vdash B : U}{(\Pi x : A.B) : U}$$

$$\frac{A : U \quad x : A \vdash B : U}{(\Sigma x : A.B) : U} \qquad \frac{A : U \quad B : U}{A + B : U} \qquad \frac{A : U \quad a : A \quad b : A}{\mathrm{Id}_A(a, b) : U} \qquad \frac{A : U}{A : \mathrm{Ty}}$$

The last rule states that Ty subsumes U, meaning it suffices to provide a member of U to provide a member of Ty. This means that we can recover most functions of type $A \to \mathrm{Ty}$ from Section 2.1 as functions of type $A \to U$. For example, vectors can now be $\mathrm{vec} : U \to \mathbb{N} \to U$.

The second new kind of type we add are **well-founded trees**, called *W-types*. W-types can be considered a generalization of recursive types, such as $\mathbb{N}$. They also play an important role in the construction of the "type of sets" that is the base of Aczel's interpretation.

$$\frac{A : \mathrm{Ty} \quad x : A \vdash B : \mathrm{Ty}}{W(x : A)B : \mathrm{Ty}} \qquad \frac{A : U \quad x : A \vdash B : U}{W(x : A)B : U} \qquad \frac{W(x : A)B : \mathrm{Ty} \quad a : A \quad f : B[a/x] \to W(x : A)B}{\sup(a, f) : W(x : A)B}$$

$$\frac{t : W(x : A)B \quad y : W(x : A)B \vdash C : \mathrm{Ty} \quad s : \Pi a : A.\Pi f : (B[a/x] \to W(x : A)B).\Pi g : (\Pi b : B[a/x].C[f\, b/y]).C[\sup(a, f)/y]}{R_W\, s\, t : C[t/y]}$$

$$\frac{R_W\, s\ \sup(a, f) : C[\sup(a, f)/x]}{R_W\, s\ \sup(a, f) = s\, a\, f\, (\lambda b.R_W\, s\, (f\, b)) : C[\sup(a, f)/x]}$$

We define $\mathrm{Ix} : W(x : A)B \to A$ and $\xi : \Pi w : W(x : A)B.\ \mathrm{Ix}(w) \to W(x : A)B$ via $\mathrm{Ix} := R_W(\lambda a.\lambda f.\lambda g.a)$ and $\xi := R_W(\lambda a.\lambda f.\lambda g.f)$ which project out the first and second component of $\sup(a, f)$ respectively.

Intuitively, W-types should be thought of as labeled trees. Each $\sup(a, f)$ can be seen as a node, a being the node's label and the image of f being the node's successors. For example, given some $A : \mathrm{Ty}$, the A-labeled binary trees is $T(A) := W(A + 1)(R_+\ (\lambda\_.\mathbb{B})\ (\lambda\_.0))$ for which we define the constructors $\mathrm{leaf} : T(A)$ and $\mathrm{node} : A \to T(A) \to T(A) \to T(A)$ given below. An inner node is labeled by $L\, a$ for an "actual label" $a : A$, its successor

function then mapping the two-member type $\mathbb{B}$ to its two successors. A leaf node is labeled with $R\,I$, its successor function being of type $0 \to T(A)$, meaning it has no successors.

$$\text{node} := \lambda a \lambda l \lambda r.\, \sup(L\,a, R_{\mathbb{B}}\,l\,r) \qquad\qquad \text{leaf} := \sup(R\,I, \lambda f.\, R_0\,f)$$

As previously stated, W-types generalize many recursive types, such as $\mathbb{N}$, as they, too, can be made sense of as labeled trees. For example, $\mathbb{N}$ can be thought of as the type of trees of breadth at most 1 and thus be defined via the type $N := W(x : \mathbb{B})(R_{\mathbb{B}}\,0\,1\,x)$ with

$$Z := \sup(\text{true}, \lambda f.\, R_0\,f) \qquad\qquad S := \lambda n.\, \sup(\text{false}, \lambda\_.\, n)$$

However, we cannot actually prove that these constructions are truly unique as our system lacks the principle of functional extensionality: We cannot prove for $f, g : A \to B$ which have $f\,a = g\,a$ for all $a : A$ that $f = g : A \to B$. Thus, we cannot even prove that $\sup(\text{false}, \lambda\_.n) = \sup(\text{false}, R_1\,(\lambda\_.n)) : N$, meaning there is no unique way of obtaining a number's successor. This, in turn, means that we *cannot* derive a term for the recursor $R_N : A[Z/x] \to (\Pi n : N.\, A[n/x] \to A[S\,n/x]) \to \Pi n : N.A[n/x]$ of the natural numbers for N, as it does not provably cover all different ways of obtaining a number's successor. The W-type N above is thus only a very rough approximation of $\mathbb{N}$. Indeed, to be able to define $\mathbb{N}$ with a properly computing recursor via W-types, a very strong, fairly exotic variant of the principle of functional extensionality is required.

In Section 4 we define an extensional notion of equality $a \equiv b$ for another W-type. It is possible to give an analogous extensional equality for N under which the Z and S implementations we gave above would be unique up to $\equiv$. However, all theorems concerning natural numbers would then also need to be weakened to only hold up to $\equiv$. This would not be sufficient for working with injectively represented sets, which play an important role in Section 6.

3 Constructive Zermelo-Fraenkel Set Theory

As CZF is a subsystem of ZF, we work in the language of set theory, i.e. the language of first-order logic with the binary predicates $x \in y$ and $x = y$. The underlying deduction system is some incarnation of intuitionistic first-order logic. We call formulas of the shape $\forall x.x \in y \to \varphi$ and $\exists x.x \in y \wedge \varphi$ instances of **restricted quantification**. We call a formula **restricted** if all quantifiers occurring in it are instances of restricted quantification and shorten these as $\forall x \in y.\varphi$ and $\exists x \in y.\varphi$, respectively. Given a binary formula $\varphi(x, y)$ we define the shorthands $\overrightarrow{\varphi}(a, b) := \forall x \in a.\exists y \in b.\varphi(x, y)$ and $\overleftrightarrow{\varphi}(a, b) := \overrightarrow{\varphi}(a, b) \wedge (\forall y \in b.\exists x \in a.\varphi(x, y))$. We sometimes also write $\overrightarrow{\varphi}(a, -) := \forall x \in a.\exists y.\varphi(x, y)$. The axiomatization of CZF we use in this report is given below. Note that it is fairly "weak," for example not using an if-and-only-if characterization of Pairing and Union, which simplifies our proofs in Section 4 and Section 7.

- **Equality:**
  (a) $\forall xy.\, x = y \leftrightarrow \forall z.(z \in x \leftrightarrow z \in y)$
  (b) $\forall xyz.\, x = y \to x \in z \to y \in z$
  Axiom (a) is usually called the axiom of extensionality. Note that (b) is required as we treat $x = y$ not as the equality of first-order logic but as a binary predicate.
- **Pairing:** $\forall xy \exists z.\, x \in z \wedge y \in z$
- **Union:** $\forall x \exists y. \forall a \in x. \forall b \in a.\, a \in y$
  Note that we can obtain the usual axioms of Pairing and Union by separating on the sets obtained via the two variants given above.
- **Restricted Separation:** $\forall x \exists y \forall z.\, z \in x \wedge \varphi(z) \leftrightarrow z \in y$
  Here we require that $\varphi(x)$ be a restricted formula.
- **Strong collection:** $\forall a. \overrightarrow{\varphi}(a, -) \to \exists b.\, \overleftrightarrow{\varphi}(a, b)$
  If $\varphi(x, y)$ is a functional relation, this is the axiom of replacement from ZF. Note that the difference between strong collection and the usual axiom of collection is the additional backwards condition in $\overleftrightarrow{\varphi}(a, b)$.
- **Subset collection:** $\forall ab \exists c \forall u. \overrightarrow{\varphi}(a, b, u) \to \exists d \in c.\, \overleftrightarrow{\varphi}(a, d, u)$
  Here $\overrightarrow{\varphi}(a, b, u)$ and $\overleftrightarrow{\varphi}(a, d, u)$ are the same as for binary φ except φ may refer to u.
- **Infinity:** $\exists x.(\forall y.\, y \in x \leftrightarrow (y = \emptyset \vee \exists z \in x.\, y = \{z\} \cup z))$
  Here '$y = \emptyset$' is a shorthand for $\forall z \in y.\, \bot$ and '$y = \{z\} \cup z$' for $\forall a.\, a \in y \leftrightarrow a \in z \vee a = z$.
- **Set induction:** $(\forall y.(\forall x \in y. \varphi(x)) \to \varphi(y)) \to \forall x. \varphi(x)$
  Note that this is a constructively viable replacement to the axiom of foundation.

In this report, we use **classes** to streamline definitions and proofs. A class is a collection of sets, characterized by a first-order formula, that is not necessarily a set. As an example, we often refer to the powerset $\mathcal{P}(A)$ of some set A, even though CZF does not guarantee the existence of all powersets. Thus, $B \subseteq \mathcal{P}(A)$, for example, should not be read as an assertion of the existence of $\mathcal{P}(A)$ but rather as stating that B consists of subsets of A.

CZF differs from regular ZF in two aspects: its intuitionistic base and its predicativity. The remainder of this section is concerned with analyzing how CZF embodies these these two aspects, how they influence the choice of axioms for CZF and which kind of set theories one arrives at if these choices are changed. For this, we introduce a few further axioms of set theory which are not part of the above axiomatization of CZF.

- **Restricted excluded middle (REM):** $\varphi \vee \neg\varphi$ where φ is a restricted formula.
- **Law of excluded middle (LEM):** $\varphi \vee \neg\varphi$ for arbitrary formulas.
- **Full Separation:** $\forall x \exists y \forall z.\, z \in x \wedge \varphi(z) \leftrightarrow z \in y$ where we allow any $\varphi(x)$
- **Foundation:** $\forall x.(\exists y \in x) \to \exists y \in x. \forall z \in y.\, z \notin x$
  Informally, this states that any non-empty set has an element with no common ele-

ments with itself.

- **Exponentiation:** $\forall xy\exists z\forall f.\ f \in z \leftrightarrow (\forall a \in x.\exists b \in y.(a,b) \in f) \wedge (\forall abb'.(a,b) \in f \rightarrow (a,b') \in f \rightarrow b = b')$
  More informally, this states that the set of functions $x \rightarrow y$ between every pair of sets x and y exists.
- **Powerset:** $\forall x\exists y\forall z.\ z \in y \leftrightarrow z \subseteq x$

Note that all of these proofs will formally take place in CZF$^-$ which is CZF without the axiom of subset collection.

At first blush, the **intuitionistic base** of CZF simply describes that the underlying logic is intuitionistic, not classical, first-order logic. However, it turns out that by naïvely adding certain set-theoretical axioms to CZF one can make the REM provable which would make it not intuitionistic anymore.

For example, if one were to add the axiom of foundation to CZF, one could prove the restricted excluded middle. This is why the axiom of set induction is used instead to guarantee well-foundedness of the set-theoretic universe.

Proposition 1 (CZF$^-$) The axiom of foundation entails $\varphi \vee \neg\varphi$ for restricted φ

Proof Consider the set $A := \{x \in \{0,1\} \mid x = 1 \vee (x = 0 \wedge \varphi)\}$. As $1 \in A$, we know by the axiom of foundation that there is some $x \in A$ with no common elements with A. If $x = 0$ then φ holds as $0 \in A$. If $x = 1$ then this means $0 \notin A$ and thus $\neg\varphi$. We may thus conclude that $\varphi \vee \neg\varphi$ overall. ∎

Curiously, knowing that $2 = \mathcal{P}(1)$ is also equivalent to the REM.

Proposition 2 (CZF$^-$) The restricted excluded middle is equivalent to $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

Proof The $\longleftarrow$-direction follows from the proof of Proposition 8. For any restricted φ consider $I := \{x \in \{\emptyset\} \mid \varphi\}$ which exists by bounded separation. As $I \subseteq \{\emptyset\}$ we know $I \in \{\emptyset, \{\emptyset\}\}$ and thus $\emptyset \in I \vee \emptyset \notin I$, yielding $\varphi \vee \neg\varphi$ because clearly $\emptyset \in I \leftrightarrow \varphi$. ∎

In Section 6.1 we show in Proposition 26 that similarly, the axiom of choice entails the REM in CZF. Note also that under full separation, all of these proofs can be extended to show the full LEM.

Proposition 3 (CZF$^-$) Under full separation, REM entails LEM.

Proof We know by Proposition 2 that REM entails $\mathcal{P}(1) = 2$. Under full separation, we may obtain $I := \{x \in \{\emptyset\} \mid \varphi\}$ for arbitrary φ and then carry out the same argument as in Proposition 2. ∎

Note that in [21] it is shown that indeed CZF $\nvdash$ REM.

The second difference between CZF and ZF is its **predicativity**. The notion of (im)predicativity can be viewed as a response to Russel's paradox. A definition is deemed to be impredicative if it refers to a totality of objects, including the one being defined. This is captured by Russel's **vicious circle principle**: "Whatever contains an apparent variable must not be a possible value of that variable"[25]. This motivates two axiomatic differences between CZF and ZF: the restriction of separation and the substitution of the axiom of subset collection instead of the powerset axiom. The reason for the restriction of separation is quite apparent: A set obtained via unrestricted separation is defined in terms of all sets, including itself, making its definition impredicative. The case of the powerset axiom is more subtle. Even with restricted separation, one may use it to make definitions such as $A := \{x \in B \mid \forall C \in \mathcal{P}(B).\varphi(x, C)\}$ where $\varphi(x, C)$ is a restricted formula. But then, A is defined in terms of $\mathcal{P}(B)$, a totality of objects (subsets of B), including itself. To alleviate this, constructive set theories replace powerset with weaker axioms, such as Myhill's exponentiation axiom [19] or the subset collection axiom of CZF.

We examine the relationship of the three axioms that, given some sets, allow for the generation of "bigger sets": Exponentiation, subset collection and the powerset axiom. For this, it will be useful to first give a different characterization of the axiom of subset collection. For $R \subseteq A \times B$ we write $R : A \lhd B$ when $\forall a \in A.\exists b \in B.(a, b) \in R$ and further write $R : A \bowtie B$ when additionally $\forall b \in B.\exists a \in A.(a, b) \in R$. We call $C \subseteq \mathcal{P}(B)$ **A-full** if for any $R : A \lhd B$ there is a $D \in C$ with $R : A \bowtie D$.

Proposition 4 (CZF$^-$) Subset collection is equivalent to $\forall AB.\exists C \subseteq \mathcal{P}(B).\ C$ is A-full.

Proof For the $\rightarrow$-direction, observe that when taking $\varphi(x, y, u) := (x, y) \in u$, subset collection is $\forall AB.\exists C.\forall R.\ R : A \lhd B \rightarrow \exists D \in C.R : A \bowtie D$. One can then obtain a $D' \subseteq D$ with $D' \subseteq \mathcal{P}(B)$ via restricted separation.

Now suppose C was A-full. Now any set U and formula $\varphi(x, y, U)$ for which we know $\forall a \in A.\exists b \in B.\varphi(x, y, U)$ allow us to obtain a relation $R \subseteq A \times B$ by applying strong replacement on A with $\psi(x, r) := \exists y \in B.\ \varphi(x, y, U) \wedge r = (x, y)$. Clearly, $R : A \lhd B$ meaning there is a $D \in C$ with $R : A \bowtie D$. But as $\forall xy.(x, y) \in R \rightarrow \varphi(x, y, u)$ that means $\overleftrightarrow{\varphi}(A, D, U)$ as desired. ∎

We can now prove that the powerset entails subset collection, which in turn entails exponentiation, thus ordering these principles by their "strength".

Corollary 5 (CZF$^-$) Powerset entails subset collection.

Proof This follows from the observation that $\mathcal{P}(B)$ is A-full for any A. ∎

Proposition 6 (CZF$^-$) Subset collection entails exponentiation.

Proof Let $C \subseteq \mathcal{P}(A \times B)$ be A-full. We show $A \to B \subseteq C$ meaning we can obtain $A \to B$ via restricted separation. Pick some $f : A \to B$ then we can obtain via replacement $f' : A \to A \times B$ with $f'(a) = (a, f(b))$. As f is a function, $f' : A \rtimes A \times B$ meaning there is some $D \in C$ with $f' : A \bowtie A \times B$. Now simply observe that $(a, b) \in D$ iff $b = f(a)$ and thus $D = f$. ∎

Interestingly, this hierarchy collapses under the REM. This sort of phenomenon, in which principles are classically equivalent but behave differently in an intuitionistic setting, can also be observed for set-induction and foundation.

Proposition 7 (CZF$^-$) Powerset is equivalent to exponentiation and $\mathcal{P}(\{\emptyset\})$ being a set.

Proof The $\to$-direction is clear. For the other direction, let 2 be the powerset of $\{\emptyset\}$. Now consider $P := \{\{a \in A \mid \emptyset \in f(a)\} \mid f : A \to 2\}$ which exists by replacement and restricted separation. It is clear that $P \subseteq \mathcal{P}(A)$. Now for any $B \subseteq A$ we define $f(a) = \{x \in \{\emptyset\} \mid a \in B\}$ via replacement and restricted separation. As $f : A \to 2$ with $B = \{a \in A \mid \emptyset \in f(a)\}$ thus $B \in P$, meaning $\mathcal{P}(A) \subseteq P$ overall. ∎

Proposition 8 (CZF$^-$) Under the restricted excluded middle, exponentiation entails powerset.

Proof By Proposition 7 it suffices to show that $\{\emptyset\}$ has a powerset. We can obtain $P := \{\emptyset, \{\emptyset\}\}$ by pairing and restricted separation. It is clear that $P \subseteq \mathcal{P}(\{\emptyset\})$. For $\mathcal{P}(\{\emptyset\}) \subseteq P$, pick some $A \subseteq \{\emptyset\}$, then $\emptyset \in A$ or $\emptyset \notin A$ by REM which means $A = \{\emptyset\}$ or $A = \emptyset$ and thus $A \in P$ in either case. ∎

Observe that Proposition 2 demonstrates why the proof of Proposition 7 would not work by simply taking $2 := \{\emptyset, \{\emptyset\}\}$. Without REM, we can only prove that $f(a) = \{x \in \{\emptyset\} \mid a \in B\} \subseteq \{\emptyset\}$ and thus need to assume that $2 = \mathcal{P}(\{\emptyset\})$ to deduce that $f : A \to 2$.

This means the relationship between CZF and ZF can be spelled out as follows. Note especially, that (ii) states exactly that the intuitionistic base and predicativity are the only differences between CZF and ZF.

Theorem 9 The following axiomatic systems are equivalent:

(i) CZF over full classical logic

(ii) CZF with restricted excluded middle and full seperation

(iii) ZF

Proof The equivalence of (i) and (ii) follows from Propositions 2 and 3. It is also clear that (iii) subsumes (i). For (i) to (iii), observer that under the LEM, full separation is obtained via Propositions 2 and 3, the existence of powersets follows from Proposition 8 and set induction is classically equivalent to the axiom of foundation. ∎

4 Interpreting CZF

Aczel [1] gives an interpretation of CZF into the type theory from Section 2.3. It consists of a type $V : \mathrm{Ty}$ of sets and binary predicates $\equiv : V \to V \to U$ and $\in : V \to V \to U$ which capture the notions of $=$ and $\in$ from CZF as small types. Using the ideas from Section 2.2 we can use these to translate set-theoretic formulas φ into types $|\varphi| : \mathrm{Ty}$. We have demonstrated in Section 2.2 that our type theory corresponds to intuitionistic predicate logic. It thus suffices to show that each axiom φ of CZF is satisfied by the interpretation to show the interpretation correct overall. By the propositions-as-types interpretation, this can be achieved by finding terms $p : |\varphi|$ for each axiom φ.

The **type V : Ty of sets** is defined as a W-type via $V := W(A : U)A$. That means each $v : V$ is of the form $\sup(A, f)$ where $A : U$ and $f : A \to V$. The idea behind this type is that, in the presence of set-induction, each set can be thought of as a well-founded tree, with its elements as its direct successors. Taking the tree's branching to be on arbitrary $A : U$ yields "sufficient freedom" to express all constructions of CZF. For example, that the empty set is represented by $\sup(0, \lambda f.R_0\, f)$ as the image of $\lambda f.R_0\, f$ is empty. Given two sets $v := \sup(A, f)$ and $u := \sup(B, g)$ we can obtain their union as $v \cup u := \sup(A+B, \lambda s.R_+\, f\, g\, s)$ as clearly anything in the image of $\lambda s.R_+\, f\, g\, s$ stems from either the image of f or the image of g.

To improve readability, we use different notation for members of V compared to general W-types. Instead of $\sup(A, f)$ we adopt Aczel's notation and write $\{f\, a \mid a : A\}$. If f is a λ-expression, we omit the λ to be closer to the set comprehension notation of set theory. For example, we now write $\emptyset$ as $\{R_0\, f \mid f : 0\}$. Note that $f : 0$ on the right-hand side indicates that this is a V-construction in type theory instead of a plain set construction in CZF. To further avoid confusion, we denote all members of V by lowercase Greek letters. As this makes the element projection $\xi : \Pi\alpha : V.\ \mathrm{Ix}(\alpha) \to V$ hard to distinguish from members of V, we denote it by π_V instead.

Recall the remark about proving equalities between members of W-types in Section 2.3. Similarly, taking $\alpha \equiv \beta := \mathrm{Id}_V(\alpha, \beta)$ will not do as we would, for example, not be able to prove that $\{\gamma \mid i : 1\} \equiv \{R_1\, \gamma\, i \mid i : 1\}$ because our system lacks functional extensionality. Instead we define $\alpha \equiv \beta$ per recursion on its first argument as below

$$\{f\, a \mid a : A\} \equiv \{g\, b \mid b : B\} := (\Pi a : A.\Sigma b : B.\ f\, a \equiv g\, b) \times (\Pi b : B.\Sigma a : A.\ f\, a \equiv g\, b)$$

It is easy to see that with this equivalence we can prove $\{u \mid i : 1\} \equiv \{R_1\, u\, i \mid i : 1\}$. At this point, we note that $u \equiv v$ forms an equivalence relation. We then define **membership** in terms of $u \equiv v$, again to make up for the lack of functional extensionality. Recall that in the setting of $\alpha : V$, $\mathrm{Ix}(\alpha)$ is the "branching type" of α and that $\pi_V\, \alpha\, a$ for $a : \mathrm{Ix}(\alpha)$ is the a-th child, and thus element, of α. The definition can thus be read as $\beta \in \alpha$ meaning that α has a child which is extensionally equal to β. Note that while we use the same symbol for

$\in$ in the set-theoretic and type-theoretic setting, it will always be clear from the context which one is meant at any given instance.

$$\beta \in \alpha := \Sigma a : \mathrm{Ix}(\alpha).\ \beta \equiv \pi_V\ \alpha\ a$$

Together, these two definitions allow for the familiar characterization of membership and equality.

$$\alpha \equiv \beta \leftrightarrow (\forall \gamma \in \alpha.\gamma \in \beta) \wedge (\forall \gamma \in \beta.\gamma \in \alpha)$$

Having defined the predicates $\equiv$ and $\in$ we can now give the **translation** $|\varphi| : \mathbf{Ty}$ for ZF formulas. Note that we give separate translations for restricted and unrestricted quantifications. Importantly, this means that for any *restricted* φ we even have $|\varphi| : U$.

$$|\bot| := 0 \qquad |x \in y| := x \in y \qquad |x = y| := x \equiv y \qquad |\varphi \wedge \psi| := |\varphi| \times |\psi|$$

$$|\varphi \vee \psi| := |\varphi| + |\psi| \qquad |\varphi \to \psi| := |\varphi| \to |\psi| \qquad |\forall x \in v.\varphi| := \Pi a : \mathrm{Ix}(x).\ |\varphi[\pi_V\ x\ a/x]|$$

$$|\exists x \in v.\varphi| := \Sigma a : \mathrm{Ix}(x).\ |\varphi[\pi_V\ x\ a/x]| \qquad |\forall x.\varphi| := \Pi x : V.\ |\varphi| \qquad |\exists x.\varphi| := \Sigma x : V.\ |\varphi|$$

From now on, we often give proofs in type theory, which we indicate with (TT). While these proofs are given as normal prose proofs, they should be understood as describing the construction of a term of the appropriate type. This is very similar to how set-theoretic proofs are usually understood to provide enough information to give explicit first-order derivations based on the axiomatization being used. However, there are a few different "levels" of proof that all fall under the umbrella of a proof in type theory in this work.

- **A meta-level proof about type theory:** These proofs explicitly reason about the existence of terms, such as Proposition 11. Formally, they can be seen as taking place in a constructive meta-system outside of type theory, giving a prose proof corresponding to the desired terms, possibly making use of additional assumptions about the type theory from Section 2.3.
- **A set-theoretic proof in type theory:** These are proofs of set-theoretic, possibly prosaic statements φ within type theory. Formally, this is a prose proof corresponding to a term of type $|\varphi|$. A set theoretic statement can be recognized by being stated in terms of $\equiv$ and $\in$ or referring to set-theoretic statements $\psi(u)$. Examples of such are Proposition 10 and Theorem 12.
- **A type-theoretic proof in type theory:** Rarely, we give proofs of type-theoretic statements which do not refer to V. Formally, these are prose proofs corresponding to a term of the propositions-as-type interpretation of the statement. Examples of this kind of proof are Proposition 35 and Proposition 36.

At this point, it is helpful to recall the three different notions of equality that we have in type theory. First of all, there is **judgmental equality** $a = b : A$ which is one of the two

kinds of judgments of the derivation system used to define our type theory in Section 2.3. In a sense, it should be considered to be *outside* of the type theory, as we cannot explicitly reason about it via the propositions-as-types interpretation. The second kind of equality is **intensional equality** $\mathrm{Id}_A(a,b)$ which is the general propositions-as-types interpretation of "proper equality" between members of a type. While we know that whenever $a = b : A$ we also have $\mathrm{Id}_A(a,b)$, it is important to note that the converse is not the case in our system. This means that it is "less strict" than the judgmental equality. Furthermore, when we write $a = b$ (instead of $a = b : A$) in type-theoretic statements or proofs, this should be understood as a shorthand for $\mathrm{Id}_A(a,b)$. Lastly, we have the **extensional equality** $\alpha \equiv \beta$ for members of V. Again, we know that $\mathrm{Id}_V(\alpha,\beta)$ entails $\alpha \equiv \beta$ but not the converse, meaning extensional equality is the least strict of all three notions of equality. This is because it does not scrutinize the representation of sets but only their elements (up to $\equiv$).

It is useful to prove that $\alpha \equiv \beta$ acts as first-order equality for formulas $|\varphi(\alpha)|$.

Proposition 10 (TT) If $\alpha \equiv \beta$ then $\varphi(\alpha)$ entails $\varphi(\upsilon)$.

Proof Per induction on φ. We only cover a few illustrative cases.

$\varphi = (\alpha = x)$: Then $x \equiv \alpha \equiv \beta$ entails $\beta \equiv x$ as $\equiv$ is an equivalence relation.

$\varphi = (\alpha \in x)$: Then $\alpha \in x$ means there is an $a : \mathrm{Ix}(x)$ such that $\pi_V\, x\, a \equiv \alpha$. Then $\pi_V\, x\, a \equiv \beta$ as well by transitivity of $\equiv$ and thus $\beta \in x$.

$\varphi = (\exists x \in \alpha.\psi(\alpha, x))$: Then there is $a : \mathrm{Ix}(\alpha)$ with $x \equiv \pi_V\, \alpha\, a$ and $\psi(\alpha, x)$. As $\alpha \equiv \beta$ there is some $b : \mathrm{Ix}(\beta)$ with $x \equiv \pi_V\, \beta\, b$ meaning $x \in \beta$. Per IH, $\alpha \equiv \beta$ yields $\psi(\beta, x)$. ∎

We write $\tau : \Pi\alpha : V.\Pi\beta : V.\alpha \equiv \beta \to |\varphi(\alpha)| \to |\varphi(\beta)|$ for the transfer of proofs along $\alpha \equiv \beta$ arising from the proof below. For $t : |\varphi(\alpha)|$ we simply write $\tau\, t : |\varphi(\beta)|$ if $\alpha \equiv \beta$ is clear from the context.

Before we prove that this interpretation satisfies the axioms of CZF we first demonstrate why extreme care was required when giving the rules for the universe U. With the rules as we have given them, we can only show that $V : \mathrm{Ty}$ and *not* that $V : U$ as it is *not* the case that $U : U$. Indeed, if $V : U$ was the case one could derive a term $t : 0$ which would mean the type theory we defined was inconsistent. This result is due to Girard [12].

Proposition 11 (TT) If $V : U$ then there exists a term $t : 0$.

Proof If $V : U$ then $A := \Sigma\beta : V.\ (\beta \in \beta \to 0) : U$ as well. Now consider $\alpha := \sup(A, \pi_1)$: Clearly $\alpha \in \alpha \to 0$ as $\alpha \in \alpha$ means there is some $a : \mathrm{Ix}(\alpha)$ such that $\alpha \equiv \beta$ for $\beta := \pi_V\, \alpha\, a$. But then $\beta \in \beta \to 0$ and $\beta \equiv \alpha$, but by $\beta \equiv \alpha$ and $\alpha \in \alpha$ we can conclude $\beta \in \beta$ and thus 0. But if $\alpha \in \alpha \to 0$ then clearly $\alpha \in \alpha$ per construction of α, meaning 0 can be obtained from $\alpha \in \alpha \to 0$. ∎

Note that essentially the same proof shows that Ty : Ty would be lead to an inconsistency, as this would allow us to define $V' := W(A : \mathrm{Ty})A$ for which the same proof strategy would apply.

We now show that the axioms of CZF are satisfied by the interpretation. This is sufficient to prove that the interpretation models CZF as we have already observed in Section 2.2 that the reasoning facilities within our type theory correspond to intuitionistic predicate logic.

Theorem 12 (TT) All axioms of CZF hold.

Proof

- **Equality:** $\forall xy.\, x = y \leftrightarrow \forall.(z \in x \leftrightarrow z \in y)$ and $\forall xyz.x = y \to x \in z \to y \in z$
  Both follow directly from Proposition 10.
- **Pairing:** $\forall xy.\exists z.x \in z \wedge y \in z$
  Take $z := \{R_{\mathbb{B}}\, x\, y\, b \mid b : \mathbb{B}\}$ then $\pi_V\, z\, \mathrm{true} \equiv x$ and $\pi_V\, z\, \mathrm{false} \equiv y$ meaning $x, y \in z$.
- **Union:** $\forall x \exists y \forall z \in x.\forall z' \in z.\, z' \in y$
  Observe that $z' \in z \in x$ means there is an $a : \mathrm{Ix}(x)$ and a $b : \mathrm{Ix}(\pi_V\, x\, a)$ such that $z \equiv \pi_V\, x\, a$ and $z' \equiv \pi_V\, (\pi_V\, x\, a)\, b$. We may thus simply take $y := \{\pi_V\, (\pi_V\, x\, (\pi_1\, p))(\pi_2\, p) \mid p : \Sigma a : \mathrm{Ix}(x).\, \mathrm{Ix}(\pi_V\, x\, a)\}$.
- **Restricted Separation:** $\forall x \exists y \forall z.(z \in x \wedge \varphi(z)) \leftrightarrow z \in y$
  As φ is restricted, $|\varphi(z)| : U$. Thus take $y := \{\pi_V\, x\, (\pi_1\, p) \mid p : \Sigma a : \mathrm{Ix}(x).|\varphi(\pi_V\, x\, a)|\}$. First, suppose $\pi_V\, x\, a \equiv z$ for some $a : \mathrm{Ix}(x)$ and $t : |\varphi(z)|$ then $(a, \tau\, t) : \Sigma a : \mathrm{Ix}(x).|\varphi(\pi_V\, x\, a)|$ and $\pi_V\, y\, (a, t) = \pi_V\, x\, a \equiv z$ meaning $z \in y$. Conversely, suppose $z \equiv \pi_V\, y\, t$ for some $t : \Sigma a : \mathrm{Ix}(x).|\varphi(\pi_V\, x\, a)|$, then $\pi_V\, y\, t = \pi_V\, x\, (\pi_1\, t)$ meaning $z \in x$ and $\tau\, (\pi_2\, t) : |\varphi(z)|$.
- **Strong collection:** $\forall a.\overrightarrow{\varphi}(a, -) \to \exists b.\, \overleftrightarrow{\varphi}(a, b)$
  We may assume a term $f : |\forall x \in a.\exists y.\, \varphi(x, y)| = \Pi x : \mathrm{Ix}(a).\Sigma y : V.|\varphi(\pi_V\, a\, x, y)|$. Then we define $b := \{\pi_1\, (f\, x) \mid x : \mathrm{Ix}(a)\}$. It is easy to see that for $x : \mathrm{Ix}(a)$ we have $\varphi(\pi_V\, a\, x, \pi_V\, b\, x)$ and thus $\overleftrightarrow{\varphi}(a, b)$.
- **Subset collection:** $\forall ab \exists c \forall u.\overrightarrow{\varphi}(a, b, u) \to \exists d \in c.\, \overleftrightarrow{\varphi}(a, d, u)$
  Observe that for any $u : V$ such that $\overrightarrow{\varphi}(a, b, u) = \forall x \in a \exists y \in b.\, \varphi(x, y, u)$ holds, we may assume a term $g : \Pi x : \mathrm{Ix}(a).\Sigma y : \mathrm{Ix}(b).\varphi(\pi_V\, a\, x, \pi_V\, b\, y, u)$. We may also regard g as an $f : \mathrm{Ix}(a) \to \mathrm{Ix}(b)$ via $f := \lambda x.\pi_1\, (g\, x)$. Then, as $\varphi(\pi_V\, a\, x, \pi_V\, b\, (f\, x), u)$ for any $x : \mathrm{Ix}(a)$, we know $\overleftrightarrow{\varphi}(a, d_f, u)$ where $d_f := \{\pi_V\, b\, (f\, x) \mid x : \mathrm{Ix}(a)\}$. By this reasoning, we then simply may take $c := \{d_f \mid f : \mathrm{Ix}(a) \to \mathrm{Ix}(b)\}$.
- **Infinity:** $\exists x.(\forall y.\, y \in x \leftrightarrow (y = \emptyset \vee \exists z.\, y = z \cup \{z\}))$
  We take $\emptyset := \{R_0\, f \mid f : 0\}$ and $\{\alpha\} := \{\alpha \mid i : 1\}$ and observe that these satisfy the usual properties. Now we can define $\widehat{\ } : \mathbb{N} \to V$ by recursion via

$$\widehat{0} := \emptyset \qquad \widehat{S\, n} := \widehat{n} \cup \{\widehat{n}\}$$

Then we take $x := \{\widehat{n} \mid n : \mathbb{N}\}$. First, pick some $y \equiv \pi_V\, x\, n = \widehat{n}$: If $n = 0$ then $x \equiv \widehat{0} = \emptyset$. If $n = S\, n'$ then we deduce that $x \equiv \widehat{S\, n'} = \widehat{n'} \cup \{\widehat{n'}\}$ with $\widehat{n'} \in x$. Conversely, if $y \equiv \emptyset$ then clearly $y \equiv \widehat{0} = \pi_V\, x\, 0$. If some $z \equiv \widehat{n}$ and $y \equiv z \cup \{z\}$ then $z \equiv \widehat{n} \cup \{\widehat{n}\} = \widehat{S\, n} = \pi_V\, x\, (S\, n)$.

- **Set induction:** $(\forall y.(\forall x \in y.\varphi(x)) \to \varphi(y)) \to \forall x.\varphi(x)$
  Consider the typing rule for recursion on V:

$$\frac{\begin{array}{c} t : V \quad y : V \vdash C : \mathrm{Ty} \\ s : \Pi A : U.\Pi f : A \to V.(\Pi a : A.C[f\, a/y]) \to C[\sup(A, f)/y] \end{array}}{R_W\, s\, t : C[t/y]}$$

  When considering the special case of $C := |\varphi(y)|$ for some set-theoretic formula φ, the type of the term s can be read as

$$\forall A : U.\forall f : A \to V.(\forall x \in \{f\, a \mid a : A\}.\varphi(x)) \to \varphi(\{f\, a \mid a : A\})$$

  which is just a slightly more complicated way of stating $\forall y.(\forall x \in y.\varphi(x)) \to \varphi(x)$, the premise of set-induction. Thus, specializing recursion on V to a predicate $|\varphi(y)|$ yields set-induction on members of V. ∎

5 Interpreting Inductive Definitions

An inductive definition describes the smallest collection of objects closed under certain operations. For example, the collection of natural numbers is the smallest collection which contains 0 and is closed under taking successors. In ZF a set satisfying these two conditions is called inductive and the ZF variant of the axiom of infinity only asserts the existence of *some* inductive set I. The natural numbers can then be obtained as

$$\omega := \{n \in I \mid \forall J.\ J \text{ inductive } \to n \in J\}$$

Observe that this is an **impredicative definition** as the separating formula quantifies over all sets J. As CZF only allows for restricted separation, this method of obtaining the natural numbers can not be carried out there. Instead, the axiom of infinity in CZF is the stronger statement $\exists x.(\forall y.\ y \in x \leftrightarrow (y = \emptyset \vee \exists z \in x.\ y = \{z\} \cup z))$. This observation extends to many other inductive definitions: While we obtain the inductively defined sets in ZF by impredicatively intersecting over all sets satisfying the closure condition, the restricted separation of CZF prevents us from doing the same there.

It would be wrong to conclude from this observation that inductive definitions are inherently unconstructive. Indeed, most types of dependent type theory are defined via closure conditions and are bounded from above by eliminators. The W-types were intended specifically to allow the definition of arbitrary inductive types. In this section, we thus aim to transfer the power of inductive definitions granted to dependent type theory by W-types to our CZF interpretation by way of the regular extension axiom.

5.1 The Regular Extension Axiom

Definition 13 A class A is **regular** if it is

- **transitive**, meaning $a \in A$ entails $a \subseteq A$
- **closed under relational collection**, meaning if $a \in A$ and $R \subseteq a \times A$ is such that $\forall x \in a.\exists y.\ (x, y) \in R$ then there has to be a $b \in A$ with $R : a \bowtie b$.

Definition 14 The **regular extension axiom (REA)** states that $\forall x \exists y.\ x \subseteq y \wedge y$ regular.

We demonstrate that CZF + REA shows that a broad range of inductively defined classes are sets in Section 5.2. Rathjen [22] showed that CZF + REA has the same proof-theoretic strength as the subsystem of second-order arithmetic with Δ^1_2-comprehension and bar induction.

We close this section by showing that our type-theoretic interpretation satisfies REA. For this, we start with an important result.

Lemma 15 (CZF) Any set a is extended by a transitive set b.

Proof We prove this claim via set induction. Suppose each $x \in a$ was extended by some transitive set. Then we can collect them into a set t via strong collection. Now consider $b := a \cup \bigcup t$. Clearly, $a \subseteq b$. Furthermore, b is transitive. Consider some $x \in b$: If $x \in a$ then there is a $x \subseteq b_x \in t$ and thus $x \subseteq b_x \subseteq b$. If $x \in y \in t$ then $x \subseteq y \subseteq b$ as y is transitive per collection of t. ∎

Using this fact, we can show that the interpretation satisfies REA.

Theorem 16 (TT) Any set α is extended by a regular set $\hat{\alpha}$.

Proof By Lemma 15 it suffices to show REA for transitive sets. Thus pick some transitive α. We take $A := \mathrm{Ix}(\alpha)$ and $B(a) := \mathrm{Ix}(\pi_V\, \alpha\, a)$ for $a : A$. Now consider some $\beta_1 \in \alpha$ then $\beta_1 \equiv \{f_1\, b \mid b : B(a_1)\}$ for some $a_1 : A$ and $f_1 : B(a_1) \to V$. Furthermore consider some $\beta_2 \in \beta_1$, as α is transitive, $\beta_2 \in \alpha$ meaning $\beta_2 \equiv \{f_2\, b \mid b : B(a_2)\}$ for $a_2 : A$ and $f_2 : B(a_2) \to V$ as well. This can be continued until the empty set is reached. Indeed, we can define a function shape $: \Pi\beta : V.\ \beta \in \alpha \to W(a : A)B(a)$ per V-recursion which assigns to each $\beta \in \alpha$ its thusly derived α-shape (the explicit definition of shape involves technical computations involving the proof of transitivity of u and the definition of $\equiv$ which is why we opt to not write it out for sake of space). In turn we can define a function set $: W(a : A)B(a) \to V$ which recursively constructs from each v-shape a set as follows

$$\mathrm{set}(\mathrm{sup}(a, f : B(a) \to W(a : A)B(a))) := \{\mathrm{set}(f\, b) \mid b : B(a)\} : V$$

A simple set-induction shows that for $\beta \in \alpha$ we have $\mathrm{set}(\mathrm{shape}(\beta)) \equiv \beta$. However, it need not be the case that $\mathrm{set}(t) \in \alpha$ for arbitrary $t : W(a : A)B(a)$. We now show that

$\hat{\alpha} := \{\mathrm{set}(t) \mid t : W(a : A)B(a)\}$, i.e. the set containing the sets of all possible shapes from $W(a : A)B(a)$ is the desired regular extension of α. For this, we need to prove three claims.

- $\alpha \subseteq \hat{\alpha}$**:** For this, simply observe that $\alpha \ni \beta \equiv \mathrm{set}(\mathrm{shape}(\beta)) \in \hat{\alpha}$.
- $\hat{\alpha}$ **is transitive:** We know $\hat{\alpha} \ni \beta \equiv \mathrm{set}(t)$ for some $t = \sup(a, f) : W(a : B)B(a)$ and thus $\beta \equiv \mathrm{set}(\sup(a, f)) = \{set(f\ b) \mid b : B(a)\}$. Then $\beta \ni \gamma \equiv \mathrm{set}(f\ b)$ for some $b : B(a)$ meaning $\gamma \in \hat{\alpha}$.
- $\hat{\alpha}$ **is closed under relational collection:** Pick $\mathrm{set}(\sup(a, f)) \equiv \beta \in \hat{\alpha}$ and $R : \beta \ltimes \hat{\alpha}$. By the propositions-as-types interpretation, the proof of $R : \beta \ltimes \hat{\alpha}$ gives rise to a function $g : B(a) \to W(a' : A)B(a')$ such that $(\pi_V\ \beta\ b, \mathrm{set}(g\ b)) \in R$ for $b : B(a)$. Thus the set $\gamma := \mathrm{set}(\sup(a, g)) \in \hat{\alpha}$ is a relational collection of β. ∎

5.2 Inductive Definitions in CZF

To show that CZF + REA admits inductive definitions, we first need to formalize what inductive definitions *are*.

Definition 17 Let Φ be a class, a class X is **Φ-closed** if $A \subseteq X$ implies $a \in X$ for every $(a, A) \in \Phi$. We write $I(\Phi)$ for the **smallest Φ-closed class**.

The intuition behind this definition is that a class Φ represents the closure conditions of an inductive definition. Thus $(a, A) \in \Phi$ signifies that a is constructed from elements of A. For example, the class Φ_ω below is the class representing the inductive definition of the natural numbers.

$$\Phi_\omega := \{(\emptyset, \emptyset)\} \cup \{(a \cup \{a\}, \{a\}) \mid a \text{ a set}\}$$

The class $I(\Phi)$ is thus **inductively defined** by Φ and the elements of $I(\Phi)$ are said to be **inductively generated** by Φ. Now, clearly, not all $I(\Phi)$ should be sets. Consider, for example, the class of all sets V which can be inductively defined by Φ_V below.

$$\Phi_V := \{(a, \emptyset) \mid a \text{ a set}\}$$

This leads us to define a more restricted notion of inductive definitions we consider a "reasonable" inductive definitions.

Definition 18 An inductive definition Φ is **bounded** if

(a) For any set A, $\Phi(A) := \{a \mid (a, A) \in \Phi\}$ is a set as well.

(b) There is a set B such that if $(a, A) \in \Phi$ there is a $b \in B$ and a surjection $f : b \to A$. We call B a **bound** of Φ.

Condition (a) rules out inductive definitions that "grow too fast". For example, it is easy to see that Φ_V violates (a) and thus is not bounded. Condition (b) is somewhat more technical but turns out to be closely linked to the relational collection closedness of regular sets. In Theorem 23, we show that under REA, every bounded inductive definition defines a set, validating this a good notion of "valid" inductive definitions.

We proceed by giving a few examples of interesting bounded inductive definitions.

Definition 19 For classes A and $R \subseteq A \times A$ where $R_a = \{a' \mid (a', a) \in R\}$ is a set for each $a \in A$, we define the **well-founded part of** R Wf_R inductively via the class

$$\Phi_{\mathrm{Wf}} := \{(a, R_a) \mid a \in A\}$$

If A and R are sets then Φ_{Wf} is bounded by $\{R_a \mid a \in A\}$.

Definition 20 For a class A, we define the **hereditary image** $HA(A)$ inductively via

$$\Phi_{HA(A)} := \{(\mathrm{im}(f), b) \mid a \in A, f : a \to b\}$$

If A is a set clearly A is a bound of $\Phi_{HA(A)}$.

Notably, $HA(\omega)$ is the class of heredetarily finite sets and $HA(\omega + 1)$ the class of heredetarily countable sets.

Definition 21 For a class A and sets B_a for each $a \in A$, we can define the W**-set** $W_{a \in A} B_a$ inductively via

$$\Phi_W := \{((a, f), b) \mid a \in A, f : B_a \to b\}$$

If A is a set then $\bigcup_{a \in A} B_a$ is a bound of Φ_W.

Observe that, although we call these classes *W-sets*, they need not be sets in CZF in the absence of REA. However, we chose to still use this terminology to parallel the W-types of type theory.

To prove that all bounded inductive definitions form sets under REA, we need to consider the one-step extension operation $\Gamma(x)$.

Lemma 22 (CZF) Let Φ be bounded and write $\Gamma(x) := \{a \mid (a, A) \in \Phi, A \subseteq x\}$.

(i) $\Gamma(x)$ is a set if x is

(ii) There is a class function mapping each set a to a set Γ^a with $\Gamma^a = \Gamma(\bigcup\{\Gamma^b \mid b \in a\})$

(iii) $I(\Phi) = \bigcup\{\Gamma^a \mid a \text{ a set}\}$

Proof (i) If B bounds Φ we know that for each $a \in \Gamma(x)$ there is a $b \in B$ and some $f : b \to x$ such that $a \in \Phi(\mathrm{im}(f))$. Thus $\Gamma(x) := \bigcup_{b \in B} \bigcup\{\Phi(\mathrm{im}(f)) \mid f : b \to x\}$. The $\{\Phi(\mathrm{im}(f)) \mid f : b \to x\}$ can be obtained via replacement on $x \to b$ as each $\Phi(\mathrm{im}(f))$ is a set, making $\Gamma(x)$ a set.

(ii) Consider the class $I(\Psi)$ for the inductive definition

$$\Psi := \{((x, \Gamma(\bigcup y)), R) \mid R : x \bowtie y\}$$

We show that for each set a there is a unique Γ^a such that $(a, \Gamma^a) \in I(\Psi)$ per set induction and that this Γ^a has the desired property. Suppose each $b \in a$ had a unique $(b, \Gamma^b) \in I(\Psi)$ and that $\Gamma^b = \Gamma(\bigcup\{\Gamma^c \mid c \in b\})$. For any $(a, z) \in I(\Psi)$ we know that $y = \Gamma(\bigcup y)$ for a y such that

$$\forall b \in a \exists x \in y.\ (b, x) \in I(\Psi) \wedge \forall x \in y \exists b \in a.\ (b, x) \in I(\Psi)$$

but as each $(b, \Gamma^b) \in I(\Psi)$ is unique that means $y = \{\Gamma^b \mid b \in a\}$ and thus that Γ^a is unique and $\Gamma^a = \Gamma(\bigcup\{\Gamma^b \mid b \in a\})$ as desired.

(iii)

- $\bigcup\{\Gamma^a \mid a \text{ a set}\} \subseteq I(\Phi)$: Per set induction on a. If $\Gamma^b \subseteq I(\Phi)$ for $b \in a$ then $\bigcup\{\Gamma^b \mid b \in a\} \subseteq I(\Phi)$ and thus $\Gamma^a = \Gamma(\bigcup\{\Gamma^b \mid b \in a\}) \subseteq I(\Phi)$ as $I(\Phi)$ is Φ-closed.
- $I(\Phi) \subseteq \bigcup\{\Gamma^a \mid a \text{ a set}\}$: It suffices to show that $\bigcup\{\Gamma^a \mid a \text{ a set}\}$ is Φ-closed. If $x \subseteq \bigcup\{\Gamma^a \mid a \text{ a set}\}$ then for each $y \in x$ there is a set a such that $y \in \Gamma^a$. These may be collected into a set b. Then $x \subseteq \bigcup\{\Gamma^a \mid a \in b\}$ and thus $\Gamma(x) \subseteq \Gamma^b \subseteq \bigcup\{\Gamma^a \mid a \text{ a set}\}$. ∎

Theorem 23 (CZF + REA) If Φ is bounded, $I(\Phi)$ is a set.

Proof By REA we may assume the bound B of Φ to be a regular set. We now claim $I := \bigcup\{\Gamma^b \mid b \in B\} = I(\Phi)$. By Lemma 22 (iii) we know $I \subseteq I(\Phi)$. For $I(\Phi) \subseteq I$ it again suffices to show that I is Φ-closed. For $x \in \Gamma(I)$ we know $(x, X) \in \Phi$ for $X \subseteq I$ with surjection $f : b \to X$ for some $b \in B$. As this means that $\forall y \in b \exists z \in B.\ f(y) \in \Gamma^z$, regularity of B yields a $c \in B$ with $\forall y \in b \exists z \in c. f(y) \in \Gamma^z$. Then $x \in \Gamma(X) \subseteq \Gamma^c \subseteq I$. ∎

Corollary 24 (CZF + REA)

(i) For any set $R \subseteq A \times A$, Wf_R is a set.

(ii) For any set A, $HA(A)$ is a set.

(iii) For any set A and family of sets $(B_a)_{a \in A}$, $W_{a \in A} B_a$ is a set.

6 Interpreting Choice

6.1 Choice in CZF

This section is concerned with the interpretation of choice principles and related axioms. We begin by introducing each of these principles and exploring some of their consequences.

First, recall the axiom of choice.

Definition 25 The **axiom of choice (AC)** states that for every family of sets $(B_a)_{a\in A}$ for some set A, the set

$$\Pi a \in A.B_a := \left\{ f \in A \to \bigcup_{a\in A} B_a \mid \forall a \in A.\, f(a) \in B_a \right\}$$

is non-empty if all of the B_a are.

Observe that this presentation, which is somewhat closer to type theory, is equivalent to the more common formulations of the AC. Note that the set $\Pi a \in A.B_a$ can always be obtained via restricted separation on the exponential $A \to \bigcup\{B_a \mid a \in A\}$.

There are two ways of formalizing a family $(B_a)_{a\in A}$ of sets. First of all, we may simply consider a function B with $\mathrm{dom}(B) = A$, each B_a being $B(a)$. Alternatively, such a family may be given by formula $\varphi(x, y)$ with $\overrightarrow{\varphi}(A, -)$ which is functional on A, each B_a being the unique set with $\varphi(a, B_a)$. By the axiom of strong collection, we may easily convert one representation into the other, which is why we use the two representations interchangeably from now on.

The following result is usually credited to Diaconescu [9]. It can be viewed as evidence that in set theory, the full axiom of choice is not constructively acceptable.

Proposition 26 (CZF) The axiom of choice entails the restricted excluded middle.

Proof Pick some restricted formula φ and consider the sets $A := \{x \in 2 \mid (x = 0) \vee \varphi\}$ and $B := \{x \in 2 \mid (x = 1) \vee \varphi\}$ where $2 := \{0, 1\}$. Now define $C := \{A, B\}$ and consider the family $(x)_{x\in C}$, clearly each $x \in C$ is non-empty and there thus is a function $f \in \Pi x \in C.x$ by the axiom of choice. As there are only four possible variants of $\{f(A), f(B)\}$ per construction of A and B, we may make the following case-distinction:

- $f(A) = f(B)$: Then $f(A) = 1$, meaning $1 \in A$, or $f(B) = 0$, meaning $0 \in B$, and thus φ holds in either way.
- $f(A) \neq f(B)$: For this to be possible, we need to have $A \neq B$ as otherwise $f(A) = f(B)$ holds trivially. That means $1 \notin A$ and $0 \notin B$. But then $\neg\varphi$ holds.

As either case yields a decision on φ, we may conclude $\varphi \vee \neg\varphi$ overall. ∎

Corollary 27 CZF + Full Separation + AC is equivalent to ZFC.

The next two principles we consider are the axiom of dependent choice and the axiom of relativized dependent choice.

Definition 28

- The **axiom of dependent choice (DC)** states that for any set A and formula $\varphi(x, y)$ such that $\overrightarrow{\varphi}(A, A)$ there exists, for any $a \in A$, a sequence $f : \mathbb{N} \to A$ with $f(0) = a$ and for any $n \in \mathbb{N}$, $\varphi(f(n), f(n+1))$.
- The **axiom of relativized dependent choice (rDC)** states that for any formulas $\theta(x)$ and $\varphi(x, y)$ such that $\forall x.\theta(x) \to \exists y.\theta(y) \wedge \varphi(x, y)$ there exists, for any $\theta(x)$, a function f with $\mathrm{dom}(f) = \mathbb{N}$, $f(0) = x$ and for any $n \in \mathbb{N}$, $\theta(f(n))$ and $\varphi(f(n), f(n+1))$.

The axiom of dependent choice is a choice-fragment, meaning it is a consequence of the full axiom of choice. Similarly, the axiom of relativized choice entails the plain axiom of dependent choice. Aczel [4] has shown that rDC is equivalent to DC together with an additional principle called the relation reflection scheme (RRS).

Proposition 29 (CZF)

(i) AC entails DC

(ii) rDC entails DC.

Proof

(i) For each $a \in A$, we can obtain a non-empty $B_a \subseteq \{b \in A \mid \varphi(a, b)\}$ via strong collection. AC then yields a function $f : \Pi a \in A.B_a$. For some $a \in A$, the sequence $g : \mathbb{N} \to A$ may then be defined recursively via $g(0) := a$ and $g(n+1) := f(g(n))$.

(ii) To obtain DC from rDC, simply take $\theta(x) := x \in A$. ∎

For the next axiom, we require an additional notion.

Definition 30

- A set B is a **base** if the axiom of choice holds for all B-indexed families.
- The **presentation axiom (PAx)** states that for every set A there exists a base B and a surjection $f : B \to A$. The function f is called a **presentation** of A.

Interestingly, PAx provides sufficient proving strength to deduce subset collection from exponentiation, but not the powerset axiom.

Proposition 31 (CZF$^-$) Exponentiation + PAx entails subset collection.

Proof Pick sets X, Y, by PAx, there is a presentation $f : B \to X$. We claim that $F := \{\mathrm{im}(g) \mid g : B \to Y\} \subseteq \mathcal{P}(Y)$ is X-full. Pick some $R : X \ltimes Y$, because B is a base there thus is a $g \in \Pi b \in B.\{y \in Y \mid (f(b), y) \in R\}$ and clearly $R : X \bowtie \mathrm{im}(g)$. ∎

The last two axioms we consider are a strengthening of PAx and a weakening of the AC. For this, we first introduce an important class of sets.

Definition 32 A class X is **$\Pi\Sigma WI$-closed** if it contains

- ω and each $n \in \omega$
- For any $A \in X$ and family $B : A \to X$ the set $\Pi a \in A.B_a$
- For any $A \in X$ and family $B : A \to X$ the set $\Sigma a \in A.B_a := \{(a, b) \mid a \in A, b \in B_a\}$
- For any $A \in X$ and family $B : A \to X$ the class $Wa \in A.B_a$ if it is a set
- For any $A \in X$ and $a, b \in A$ the set $\mathrm{Id}_A(a, b) := \{z \in \{\emptyset\} \mid a = b\}$

The class of **$\Pi\Sigma WI$-sets** is the smallest $\Pi\Sigma WI$-closed class.

This definition can be explicitly formalized as an inductive, although not bounded, class $\Phi_{\Pi\Sigma WI}$. The clause for W-sets is somewhat intricate: Without REA, it need not be the case that all $Wa \in A.B_a$ are sets. In this case, $\Pi\Sigma WI$-closedness is only concerned with those which can be proven to be sets. In later parts of this work, we also use analogous classes, such as the $\Pi\Sigma W$-sets, which are defined in the obvious way.

Based on this, we can define the two remaining choice principles we consider in this report.

Definition 33

- The **$\Pi\Sigma WI$-AC** states that every $\Pi\Sigma WI$-set is a base.
- The **$\Pi\Sigma WI$-PAx** states that every $\Pi\Sigma WI$-set is a base and every set A has a presentation $f : B \to A$ where B is a $\Pi\Sigma WI$-set.

We show in Theorem 45 and Lemma 48 that our set interpretation satisfies $\Pi\Sigma WI$-AC and $\Pi\Sigma WI$-PAx, respectively, when the type theory is extended by additional axioms. In Section 7 we show how to build an inner model satisfying, among other axioms, $\Pi\Sigma WI$-PAx.

Proposition 34 (CZF + $\Pi\Sigma WI$-PAx) A set B is a base iff it is in bijection with a $\Pi\Sigma WI$-set.

Proof As every $\Pi\Sigma WI$-set is a base and any set in bijection with a base clearly is a base itself, the backwards direction is clear. Now let B be an arbitrary base. By $\Pi\Sigma WI$-PAx there is a surjection $f : C \to B$ for C as $\Pi\Sigma WI$-set. As B is a base, we can obtain a injection $g : \Pi b \in B.\{c \in C \mid f(c) = b\} (\subseteq B \to C)$ with $f(g(b)) = b$. Then g is a bijection $B \equiv \{c \in C \mid g(f(c)) = c\}$. Now observe that $\{c \in C \mid g(f(c)) = c\} \equiv \Sigma c \in C.\mathrm{Id}(g(f(c)), c)$ which is a $\Pi\Sigma WI$-set as C is, meaning B is in bijection with a $\Pi\Sigma WI$-set. ∎

Observe that this proof already works for ΣI-PAx as neither Π-sets nor W-sets were used in the construction of the bijective set.

6.2 Choice in Type Theory

In Proposition 26 we showed that in set theory, the axiom of choice entails variants of the law of excluded middle and thus is not acceptable constructively. In this section, we examine the axiom of choice in the type theory defined in Section 2.3.

Maybe somewhat surprisingly, a type-theoretical variant of the axiom of choice is provable in our type theory. Similar to its set-theoretical counterpart, it is stated in terms of a $A : \mathrm{Ty}$ and an indexed family $x : A \vdash B(x) : \mathrm{Ty}$. We chose to state it in terms of an additional predicate $x : A, y : B(x) \vdash P(x, y) : \mathrm{Ty}$ which is often handy when using the axiom of choice in later proofs.

Proposition 35 (TT) Whenever for any $a : A$ there exists a $b : B(a)$ with $P(a, b)$ then there is a function $f : \Pi a : A.\ B(a)$ with $P(a, f\ a)$ for all $a : A$.

Proof By the propositions-as-types interpretation, $\forall a : A. \exists b : B.\ P(a, b)$ is a function $g : \Pi a : A. \Sigma b : B.\ P(a, b)$. The desired function can be defined as $f := \lambda a. \pi_1(g\ a)$. ∎

Observe that we have already made implicit use of the principle underlying the proof in Theorem 12 and Theorem 16.

Similarly, the axiom of dependent choice can also be proven.

Proposition 36 (TT) Whenever for any $a : A$ there is an $a' : A$ such that $P(a, a')$ then for any $a : A$ there is a function $f : \mathbb{N} \to A$ such that $f\ 0 = a$ and $P(f\ n, f\ (S\ n))$ for any $n : \mathbb{N}$.

Proof By Proposition 35 we obtain a $g : A \to A$ with $P(a, g(a))$ for all $a : A$. For any fixed $a : A$ we may thus define the desired function via recursion as

$$f\ 0 := a \qquad\qquad f\ (S\ n) := g\ (f\ n)$$

∎

We remark that the provability of the axiom of choice depends on the structure of the type universes of the type theory under consideration. For example, the Calculus of Constructions [7] cannot prove the AC as its universe structure does not allow values of predicative types, such as $\mathbb{N}$ or pairs, to be projected out of its impredicative universe of propositions.

6.3 Interpreting DC

In this section, we show how to use the type-theoretic DC from Proposition 36 to prove that our interpretation V satisfies DC as well. While the proof itself is rather simple, we use it as an opportunity to introduce the various notions and techniques for proving choice-interpretation which we also use in Section 6.4 to show that V satisfies $\Pi\Sigma WI$-AC.

So far, we only ever reasoned about sets up to extensional equality. However, when considering functions between sets, it is often important to know specific details of their representation within V.

Definition 37 A set $\{f\ a \mid a : A\}$ is **injectively represented** if for any $a, b : A$ we have $a = b$ whenever $f\ a \equiv f\ b$.

Canonical examples of injectively represented sets are the natural numbers of our interpretation.

Proposition 38 (TT) The set ω and each $\widehat{n}$ for $n : \mathbb{N}$ are injectively represented.

Proof For $\omega = \sup(\mathbb{N}, \lambda n.\widehat{n})$, simply observe that $\widehat{n} \equiv \widehat{m}$ means $k < n$ iff $k < m$ for $k : \mathbb{N}$ and thus that $m = n$. The injective representation for the $\widehat{n}$ is proven per induction on $n : \mathbb{N}$. If $n = 0$ then $\widehat{0}$ has no elements and is thus trivially injectively represented. For an $n+1$ we know that $\widehat{n+1} = \widehat{n} \cup \{\widehat{n}\} = \sup(\mathrm{Ix}(\widehat{n}) + 1, R_+(\pi_V\ \widehat{n})\ (\lambda\_.\widehat{n}))$ and thus is injectively represented as $\widehat{n}$ is such per induction hypothesis and $\widehat{n} \notin \widehat{n}$. ∎

The importance of injective representations is that they allow us to lift type-theoretic functions to interpretations of set-theoretic functions in V.

Lemma 39 (TT) Let $\alpha : V$ be injectively represented, then for any $\beta : V$ and function $f : \mathrm{Ix}(\beta) \to \mathrm{Ix}(\alpha)$ there exists an $F : V$ which is a set-theoretic function $F : \beta \to \alpha$ with $F(\pi_V\ \beta\ a) = \pi_V\ \alpha\ (f\ a)$ for any $a : \mathrm{Ix}(\beta)$.

Proof Observe that $\langle \gamma, \delta \rangle := \{\gamma, \{\gamma, \delta\}\} : V$ for $\gamma, \delta : V$ forms set-theoretic tuples using the interpretation of the Pairing axiom from Theorem 12. We then define $F := \{\langle \pi_V\ \beta\ a, \pi_V\ \alpha\ (f\ a)\rangle \mid a : \mathrm{Ix}(\alpha)\}$. It is easy to see that F is a set of pairs. Now, observe that for $\langle x, y\rangle, \langle x', y'\rangle \in F$ with $x \equiv x'$ we know by injective representation of β that there is a unique $a : \mathrm{Ix}(\beta)$ with $\pi_V\ \beta\ a \equiv x \equiv x'$ and thus that $y \equiv \pi_V\ \alpha\ (f\ a) \equiv y'$ by definition of F, meaning F is a functional relation. Lastly, it is clear that $F : \beta \to \alpha$ and that $F(\pi_V\ \beta\ a) = \pi_V\ \alpha\ (f\ a)$ per construction of F. ∎

Observe that the injective representation of α is crucial for the functionality of F. Indeed, if there were $a \neq b$ with $\pi_V\ \alpha\ a \equiv \pi_V\ \alpha\ b$ then it could be possible that $F(\pi_V\ \alpha\ a) \equiv \pi_V\ \beta\ (f\ a) \not\equiv \pi_V\ \beta\ (f\ b) \equiv F(\pi_V\ \alpha\ b)$, which would make F a non-functional relation.

With this, we can prove that the interpretation satisfies DC.

Theorem 40 (TT) For any set $\alpha : V$ and any formula $\varphi(x, y)$ such that for all $\beta \in \alpha$ there is a $\gamma \in \alpha$ such that $\varphi(\beta, \gamma)$ then for any $\beta \in \alpha$ there is a set-theoretic function $F \in \omega \to \alpha$ with $F(\hat{0}) \equiv \beta$ and $\varphi(F(\widehat{n}), F(\widehat{n+1}))$ for any $\widehat{n} \in \omega$.

Proof As $\beta \in \alpha$ there is some $a : \mathrm{Ix}(\alpha)$ with $\beta \equiv \pi_V\ \alpha\ a$. Then the theorem's premise together with the type-theoretic DC yields a type-theoretic function $f : \mathbb{N} \to \mathrm{Ix}(\alpha)$ with $f\ 0 = a$ and $\varphi(\pi_V\ \alpha\ (f\ n), \pi_V\ \alpha\ (f\ (S\ n)))$ for all $n : \mathbb{N}$. Then the desired set-theoretic function $F : \omega \to \alpha$ can be obtained via Lemma 39 as ω is injectively represented by Proposition 38 ∎

6.4 Interpreting ΠΣWI-AC

We begin by reducing the claim of this section somewhat.

Lemma 41 (CZF) There is a class-level function $i_A(a,b)$ mapping ΠΣW-sets A and elements $a, b \in A$ to a ΠΣW-set in bijection with $\mathrm{Id}_A(a,b)$.

Proof We prove this per induction on the class of ΠΣW-sets.

- For elements of ω we define per recursion

  $$i(0,0) := \{\emptyset\} \qquad i(0,m+1) := \emptyset \qquad i(n+1,0) := \emptyset \qquad i(n+1,m+1) := i(n,m)$$

  It is easy to see that for any $n, m \in \omega$ we have $i(n,m) = \mathrm{Id}_\omega(n,m)$. For any $n \in \omega$ and $m, m' \in n$ we can take $i_n(m,m') := i_\omega(m,m')$ as $n \subset \omega$.
- Let A and each B_a for $a \in A$ be ΠΣW-sets for which i has already been defined, then we can take $i_{\Pi a \in A.B_a}(f,g) := \Pi a \in A.\ i_{B_a}(f(a),g(a))$. Then $\exists x \in i_{\Pi a \in A.B_a}(f,g)$ iff $\forall x \in A. f(a) = g(a)$ iff $f = g$. Furthermore, $i_{\Pi a \in A.B_a}(f,g)$ has at most one element as all of the $i_{B_a}(f(a),g(a))$ have at most one element per induction hypothesis.
- Let A and each B_a for $a \in A$ be ΠΣW-sets for which i has already been defined, then we can take $i_{\Sigma a \in A.B_a}((a,b),(a',b')) := \Sigma x \in i_A(a,a').\ \Pi x \in i_A(a,a').i_{B_a}(b,b')$. Observe that in this definition, if $a \neq a'$, it may be the case that $b' \notin B_a$ and $i_{B_a}(b,b')$ is thus not defined. However, in this case $\Pi x \in i_A(a,a').i_{B_a}(b,b') = \emptyset$, making $i_{\Sigma a \in A.B_a}$ well-defined overall. Again, observe that $i_\Sigma((a,b),(a',b'))$ is inhabited iff $a = a$ and $b = b'$. By the inductive hypothesis, it can have at most one element, similarly to the previous case.
- Let A be a ΠΣW-sets for which i has already been defined, then we define $i_{Wa \in A.B_a}$ per induction as follows

  $$i_{Wa \in A.B_a}((a,f),(a',g)) := \Sigma x \in i_A(a,a').\Pi x \in i_A(a,a').\Pi b \in B_a.\ i_{Wa \in A.B_a}(f(b),g(b))$$

  this definition is a combination of the ideas behind the definitions of i for Π- and Σ-sets. Thus, an inductive proof combining both arguments shows that indeed $i_{Wa \in A.B_a}((a,f),(a',g))$ is in bijection with $\mathrm{Id}_{Wa \in A.B_a}((a,f),(a',g))$. ∎

Corollary 42 (CZF)

(i) Every ΠΣWI-set is in bijection with a ΠΣW-set

(ii) ΠΣWI-AC is equivalent to ΠΣW-AC.

(iii) ΠΣWI-PAx is equivalent to ΠΣW-PAx

Proof

(i) If A is a $\Pi\Sigma WI$-set, one can obtain a $\Pi\Sigma W$-set B in bijection with it by simply replacing each instance of $\mathrm{Id}_C(c, c')$ in its construction process with $i_C(c, c')$.

(ii) This follows as any set in bijection with a base is a base itself.

(iii) The desired surjection can be obtained by composing with the bijection. ∎

Next, we prove that every injectively represented set is a base. This means it suffices to show that all $\Pi\Sigma W$-sets can be injectively represented to conclude $\Pi\Sigma W$-AC.

Lemma 43 (TT) Every injectively represented set is a base.

Proof Let $\alpha : V$ be injectively representend and let $F : V$ be a function with $\mathrm{dom}(F) \equiv \alpha$ such that $\forall \beta \in \alpha.\exists \gamma \in F(\beta)$. By a similar argument as Proposition 35 we can obtain a function $f : \mathrm{Ix}(\alpha) \to V$ from the proof of that formula, such that for all $a : \mathrm{Ix}(\alpha)$ we have $f\, a \in F(\pi_V\, \alpha\, a)$. Then, taking $\gamma := \sup(\mathrm{Ix}(\alpha), f)$, we can lift $\lambda a.a : \mathrm{Ix}(\alpha) \to \mathrm{Ix}(\gamma)$ via Lemma 39 to obtain set-theoretic function $G \in \alpha \to \gamma$ which also is a choice function $G : \Pi\beta \in \alpha.F(\beta)$. ∎

Before we can prove that V satisfies $\Pi\Sigma W$-AC, we need to add an additional *type-theoretic* axiom. Recall from Section 2.3 that our type theory lacks functional extensionality. However, it is required to prove Theorem 45.

Definition 44 The axiom of U **functional extensionality (UFE)** posits a term of type

$$\Pi A : U.\Pi B : A \to U.\Pi f : (\Pi A.B).\Pi g : (\Pi A.B).(\Pi a : A.\mathrm{Id}_{B_a}(f\, a, g\, a)) \to \mathrm{Id}_{\Pi A.B}(f, g)$$

Theorem 45 (TT + UFE) The $\Pi\Sigma WI$-AC holds.

Proof By Corollary 42 it suffices to show $\Pi\Sigma W$-AC. For this, we prove that the class of injectively representable sets is $\Pi\Sigma W$-closed. As the $\Pi\Sigma W$-sets are the smallest $\Pi\Sigma W$-closed class, this means the $\Pi\Sigma W$-sets are injectively representable and by Lemma 43 thus bases, proving our claim.

- We have shown that ω and its elements are injectively representable in Proposition 38.
- Let $A : V$ be injectively represented and $B : \mathrm{Ix}(A) \to V$ be a family of injectively represented sets. Then we claim $\hat{\Pi}\, B := \{\mathrm{lift}\, g \mid g : \Pi a : \mathrm{Ix}(A).\, \mathrm{Ix}(B\, a)\}$ is an injective representation of $\Pi A.B$ where $\mathrm{lift}\, g := \{\langle \pi_V\, A\, a, \pi_V\, (B\, a)\, (g\, a)\rangle \mid a : A\}$ lifts a dependent function between indexes of injectively represented sets into a function of $\Pi A.B$ similar to Lemma 39. As for any $G : V$ the proof $G \in \Pi A.B$ induces a dependent function $g : \Pi a : \mathrm{Ix}(a).\, \mathrm{Ix}(B\, a)$ by Proposition 35, $\hat{\Pi}\, B$ does indeed contain all elements of $\Pi A.B$. That all elements of $\hat{\Pi}\, B$ are in $\Pi A.B$ is clear. For the injective representation, pick $\mathrm{lift}(g) \equiv \mathrm{lift}(g') \in \hat{\Pi}\, B$, then it is easy to see that this means that for all $a : \mathrm{Ix}(A)$, $\pi_V\, (B\, a)\, (g\, a) \equiv \pi_V\, (B\, a)\, (g'\, a)$ and by the injective representation of $B\, a$ that $g\, a = g'\, a$, yielding $g = g'$ by UFE.

- Let $A : V$ be injectively represented and $B : \mathrm{Ix}(A) \to V$ be a family of injectively represented sets. We claim that $\hat{\Sigma}\, B := \{\langle \pi_V\, A\, a, \pi_V\, (B\, a)\, b\rangle \mid (a, b) : \Sigma a : \mathrm{Ix}(A).\mathrm{Ix}(B\, a)\}$ is an injective representation of $\Sigma A.B$. It is easy to see that $\hat{\Sigma}\, B \equiv \Sigma A.B$. For the injectivity of the representation, pick $\langle x, y\rangle \equiv \langle x', y'\rangle \in \hat{\Sigma} B$, meaning $x \equiv x'$ and $y \equiv y'$. By the injective representation of A, we know that there is a unique $a : \mathrm{Ix}(A)$ with $\pi_V\, A\, a = x \equiv x'$ and thus that $y \equiv y' \in B\, a$. By the injective representation of $B\, a$, this means that there is a unique $b : \mathrm{Ix}(B\, a)$ such that $\pi_V\, (B\, a)\, b = y \equiv y'$. Then $(a, b) : \Sigma a : A.B\, a$ is unique such that $\pi_V\, (\hat{\Sigma}\, B)\, (a, b) = \langle x, y\rangle \equiv \langle x', y'\rangle$.
- Let $A : V$ be injectively represented and $B : \mathrm{Ix}(A) \to V$ be a family of injectively represented sets. We claim that $\hat{W}\, B := \{\mathrm{set}\, w \mid w : Wa : \mathrm{Ix}(A).\mathrm{Ix}(B\, a)\}$ is an injective representation of $WA.B$ where $\mathrm{set}(\mathrm{sup}(a, f)) := \langle \pi_V\, A\, a, \{\langle \pi_V\, (B\, a)\, b, \mathrm{set}(f\, b)\rangle \mid b : \mathrm{Ix}(B\, a)\}\rangle$. Observe that injective representation of the $B\, a$ is required for this to be well-defined. Two simple inductive arguments show that $\hat{W}\, B \equiv WA.B$. The injectivity of the representation is proven per induction on the members of $Wa : \mathrm{Ix}(A).\mathrm{Ix}(B\, a)$: Suppose $\mathrm{set}(\mathrm{sup}(a', f)) \equiv \mathrm{set}(\mathrm{sup}(b, g)) \in \hat{W}\, B$ and we already knew that $\mathrm{set}(f\, b)$ for each $b : B\, a$ was represented injectively. Then we know that $\pi_V\, A\, a \equiv \pi_V\, A\, a'$ and thus that $a = a'$. Then $\{\langle \pi_V\, (B\, a)\, b, \mathrm{set}(f\, b)\rangle \mid b : \mathrm{Ix}(B\, a)\} \equiv \{\langle \pi_V\, (B\, a)\, b, \mathrm{set}(g\, b)\rangle \mid b : \mathrm{Ix}(B\, a)\}$ means that $\mathrm{set}(f\, b) \equiv \mathrm{set}(g\, b)$ for each $b : B$ and per IH thus that $f\, b = g\, b$, yielding $f = g$ by UFE. Then $\mathrm{sup}(a, f) = \mathrm{sup}(a', g)$ overall. ∎

6.5 Interpreting $\Pi\Sigma WI$-PAx

Aczel gives two different proofs for this in [2] and [3]. In this section, we cover the proof from [2]. The proof requires two additional axioms.

Definition 46 For every predicate $P : U \to \mathrm{Ty}$, the axiom of **U-closedness (UC)** posits an induction scheme

$$
\begin{aligned}
&P\, 0 \to P\, 1 \to P\, \mathbb{N} \to \\
&(\Pi A : U.\Pi B : U.\ P\, A \to P\, B \to P(A + B)) \to \\
&(\Pi A : U.\Pi a : A.\Pi b :\ A.\ P\, A \to \mathrm{Id}_A(a, b)) \to \\
&(\Pi A : U.\Pi B : A \to U.\ P\, A \to (\Pi a : A.\ P\, (B\, a)) \to P(\Pi a : A.B\, a)) \to \\
&(\Pi A : U.\Pi B : A \to U.\ P\, A \to (\Pi a : A.\ P\, (B\, a)) \to P(\Sigma a : A.B\, a)) \to \\
&(\Pi A : U.\Pi B : A \to U.\ P\, A \to (\Pi a : A.\ P\, (B\, a)) \to P(Wa : A.B\, a)) \to \\
&\Pi A : U.\ P\, A
\end{aligned}
$$

Intuitively, the axiom of U-closedness states that types formed via the rules we have given in Section 2.3 are the *only* members of U. This means U is closed off from future extensions

which could add additional kinds of types. Such an axiom is highly untypical in type theory where it is common to leave the exact internal structure of a universe such as U unspecified. A motivating example for this can be found in Aczel's own work: In [2], he gives the proof of the interpretation $\Pi\Sigma I$-PAx using UC for the first time. However, the type theory he considers in that paper does not have W-types. In [3], he adds W-types to interpret the REA, which forces him to adapt his proof to $\Pi\Sigma WI$-PAx and, critically, *modify* UC to account for W-types. This demonstrates that UC is not very canonical and should thus be avoided. Indeed, in [3], Aczel gives a different way of obtaining a model for CZF + $\Pi\Sigma WI$-PAx which does not make use of UC. We have nonetheless opted to also give the first proof in terms of UC as knowing that proof makes the somewhat more complicated proof in Section 7 easier to understand.

The second axiom required is the principle of uniqueness of identity proofs.

Definition 47 The principle of **U-restricted uniqueness of identity proofs (UUIP)** posits a term

$$\mathrm{UUIP} : \Pi A : U.\Pi a : A.\Pi b : B.\Pi p : \mathrm{Id}_A(a,b).\Pi q : \mathrm{Id}_A(a,b).\ p = q$$

Note that this principle is contradicts univalent extensions of the type theory, such as [26], which crucially rely on the existence of different proofs of the same identity statement.

Lemma 48 (TT + UE + UC + UUIP) For any type $A : U$ there exists a $\Pi\Sigma WI$-set α which is injectively represented with $\mathrm{Ix}(\alpha) = A$.

Proof We prove the claim per induction on $A : U$ via UC.

- $A = 0, A = 1, A = \mathbb{N}$**:** For these, pick $\widehat{0}, \widehat{1} \equiv \{\widehat{0} \mid x : 1\}$ and ω.
- $A = B + C$**:** Per IH, there are suitable sets $\beta, \gamma : V$ with $\mathrm{Ix}(\beta) = B$ and $\mathrm{Ix}(\gamma) = C$. Then take $\alpha = \{R_+\ (\lambda b.\langle\widehat{0}, \pi_V\ \beta\ b\rangle)\ (\lambda c.\langle\widehat{1}, \pi_V\ \gamma\ c\rangle)\ s \mid s : A+B\}$ which is injectively presented as α and β are. It is a $\Pi\Sigma WI$-set as $\alpha \equiv \Sigma\widehat{2}.F$ with $F := \{(\widehat{0}, \beta), (\widehat{1}, \gamma)\}$.
- $A = \mathbf{Id}_B(b, b')$**:** Let $\mathrm{Ix}(\beta) = B$ be the set for B obtained via IH. Now pick the set $\alpha := \{\widehat{0} \mid x : \mathrm{Id}_A(b, b')\}$ by the injective representation of β we obtain $\alpha \equiv \mathrm{Id}_\beta(\pi_V\ \beta\ b, \pi_V\ \beta\ b')$. For the injective representation of α, observe that by UUIP, $\mathrm{Id}_B(b, b')$ has at most one inhabitant.
- $A = \Pi B.C, A = \Sigma B.C, A = WA.B$**:** Observe that the IH together with the AC yield a family $F : A \to V$ representing with $\mathrm{Ix}(F\ a) = C\ a$ for $a : A$. Then choose $\hat{\Pi}\ F, \hat{\Sigma}\ F$ and $\hat{W}\ F$ from Theorem 45. ∎

Corollary 49 (TT + UE + UC + UUIP) The $\Pi\Sigma WI$-PAx holds.

Proof By Theorem 45 all $\Pi\Sigma WI$-sets are bases. For a set $\beta = \{f\ a \mid a : A\}$, we obtain an injectively presented $\Pi\Sigma WI$-set α with $\mathrm{Ix}(u) = A$ via Lemma 48. Then $f : A \to V$ can be lifted to an $F \in \alpha \to \beta$ via Lemma 39. Clearly $\beta \equiv \mathrm{im}(F)$. ∎

Observe that the UUIP was required for the case of $\mathrm{Id}_B(b, b')$ to show that the representation of $\mathrm{Id}_\beta(\pi_V\ \beta\, b, \pi_V\ \beta\, b')$ is injective. For Theorem 45 we circumvent this problem by reducing $\Pi\Sigma WI$ to $\Pi\Sigma W$ via Corollary 42, thus not being required to give a direct representation of Id-sets via the Id-type. However, for Lemma 48, it is strictly required that $\mathrm{Ix}(v) = \mathrm{Id}_B(b, b')$ meaning the use of the UUIP cannot be avoided.

7 Internalizing Aczel's construction

In [2], Aczel proves $\Pi\Sigma I$-PAx using the axiom of U-closedness as demonstrated in Section 6.5. When extending his type theory with W-types for [3], he recognizes the restrictiveness of U-closedness and gives an alternative method of obtaining a model of CZF + $\Pi\Sigma WI$-PAx: Instead of interpreting it into type theory like the previous axioms, he builds an inner model of CZF + DC + REA + $\Pi\Sigma WI$-PAx over CZF + DC + REA + $\Pi\Sigma WI$-AC. As we illustrate in this section, this inner model should be viewed as internalizing Aczel's type-theoretic construction into set theory. Indeed, all constructions employed in the proofs of this section are extremely similar to those in the type-theoretical interpretation.

Definition 50 We say a class M **satisfies** a formula φ, written $M \vDash \varphi$, if φ holds when all of its unrestricted quantifications are restricted to M. We call a class M an **inner model** of CZF if it satisfies all axioms of CZF.

Note that this notion of an inner model is much weaker than that commonly employed in the study of ZFC as it also considers every set-model of CZF an inner model.

To chose M, we first need to rephrase the proof from Section 6.5: Observe that the definition $V := WA : U.A$ could be rephrased as $V := H(U)$ from Definition 20, that is, as the *type* of U-images. Knowing each $\alpha : V$ to be a U-image, the proof of Section 6.5 uses the internal structure given to U by U-closedness to observe that each $A : U$ can be injectively represented as a $\Pi\Sigma WI$-set and the notion of all $\alpha : V$ being U-images can be internalized as all $\alpha : V$ being $\Pi\Sigma WI$-images. For the internal model, we thus directly chose $M = H(\Pi\Sigma WI)$ which then clearly yields $M \vDash \Pi\Sigma WI$-PAx.

Proposition 51 (CZF + REA)

(i) If $a, b \in M$ then $\{a, b\} \in M$ and $(a, b) \in M$

(ii) If $B \in \Pi\Sigma WI$ and $f : B \to M$ then $f \in M$

(iii) If $A \in \Pi\Sigma WI$ then $A \in M$

Proof

(i) $\{a, b\}$ is the image of $\{(0, a), (1, b)\} : 2 \to M$ meaning $\{a, b\} \in M$. Then clearly also $(a, b) = \{a, \{a, b\}\} \in M$.

(ii) Clearly, $f = \mathrm{im}(g)$ with $g(b) = (b, f(b)) : B \to M$ as $(b, f(b)) \in M$ by (i).

(iii) To show that $A \in M$, it suffices to show that each $x \in M$ for each $x \in A$ as A then is the image of the identity function $1 : A \to M$ and thus $A \in M$ itself. We do this per induction on the construction rules used for A.

- $A \in \omega$: We prove $A \in M$ per strong induction on $A \in \omega$: As $A = \{B \in \omega \mid B \leq A\}$ we know per IH that $B \in M$ for each $B \in A$. Then A is the image of the identity function $1(x) = x : A \to M$ and thus $A \in M$.
- $A = \omega$: The previous case shows that $\omega \subseteq M$.
- $A = \Sigma B.C$: We know $A \subseteq M$ and each $B_a \subseteq M$ for $a \in A$. By (i) we thus know that $(b, c) \in M$ for any $b \in B$ and $c \in C_b$.
- $A = \Pi B.C$: We know $B \subseteq M$ and each $C_b \subseteq M$ for $b \in B$. Then an $f : \Pi B.C$ is $f : B \to M$ and thus $f \in M$ by (ii).
- $A = WB.C$: We know $B \subseteq M$ and each $C_b \subseteq M$ for $b \in B$. We prove this per induction on (b, f): If each $f(c) \in M$ for $c \in C_b$ then $f : C_b \to WB.C$ is $f : C_b \to M$, meaning $f \in M$ by (ii) and $(b, f) \in M$ by (i).
- $A = \mathbf{Id}_B(b, b')$: We have shown $0 \in M$ in the first case. ∎

Theorem 52 (CZF + REA + ΠΣWI-AC) $M \vDash \Pi\Sigma WI$-AC and $M \vDash \Pi\Sigma WI$-PAx

Proof First, note that $M \vDash A$ is a $\Pi\Sigma WI$-set iff A is a $\Pi\Sigma WI$-set: Simply observe that $\Pi\Sigma WI \subseteq M$ by Proposition 51 (iii) means restricting the unrestricted quantifications of "A is a $\Pi\Sigma WI$-set" to M does not matter.

For $\Pi\Sigma WI$-AC, it thus suffices to observe that Proposition 51 (ii) means that any choice function $f : \Pi A.B$ with $A \in \Pi\Sigma WI$ already has $f \in M$.

For $\Pi\Sigma WI$-PAx, observe that $A \in M = H(\Pi\Sigma WI)$ means there is a $B \in PSWI$ and an $f : B \to M$ such that $A = \mathrm{im}(f)$. Again, by Proposition 51 (ii), $f \in M$. ∎

It remains to show that M actually is an inner model of CZF. For this, we give an M-analogon to the translation $|\varphi| : U$ for restricted sentences φ. It is needed to prove that $M \vDash$ Restricted Separation.

Lemma 53 (CZF + REA + ΠΣWI-AC) For any restricted sentence φ with parameters in M there exists a $\Pi\Sigma WI$-set $|\varphi|^M$ such that φ holds iff $\exists x.x \in |\varphi|^M$.

Proof We define $|\varphi|^M$ per recursion on φ.

- $\varphi = \bot$**:** Simply pick $|\bot|^M := \emptyset$ as $\emptyset$ has no elements.
- $\varphi = \psi \wedge \psi'$: We pick $|\psi \wedge \psi'|^M := |\psi|^M \times |\psi'|^M$ and observe that

$$\psi \wedge \psi' \text{ iff } (\exists x.x \in |\psi|^M) \wedge (\exists x.x \in |\psi'|^M) \text{ iff } \exists x.x \in |\psi \wedge \psi'|^M$$

- $\varphi = \psi \vee \psi'$: We pick $|\psi \vee \psi'|^M := |\psi|^M + |\psi'|^M$ and reason similarly to $\psi \wedge \psi'$.
- $\varphi = \psi \to \psi'$: We pick $|\psi \to \psi'|^M := |\psi|^M \to |\psi'|^M$. If $f : |\psi|^M \to |\psi'|^M$ exists and ψ holds then there is some $x \in |\psi|^M$ and then $f(x) \in |\psi'|^M$ means that ψ' holds as well. Now suppose $\psi \to \psi'$ held, then clearly $\forall x \in |\psi|^M.\exists y \in |\psi'|^M$ using the IH. As $|\psi|^M$ is a base by $\Pi\Sigma WI$-AC, there thus exists a function $f : |\psi|^M \to |\psi'|^M$.
- $\varphi = \forall x \in A.\psi$: We know that $A = \mathrm{im}(f)$ for some $f : B \to M$ and $B \in \Pi\Sigma WI$. Now take $|\forall x \in A.\psi|^M := \Pi b \in B.|\psi[f(b)/x]|^M$. Correctness is similar to the case of $\psi \to \psi'$.
- $\varphi = \exists x \in A.\psi$: We know that $A = \mathrm{im}(f)$ for some $f : B \to M$ and $B \in \Pi\Sigma WI$. Now take $|\exists x \in A.\psi|^M := \Sigma b \in B.|\psi[f(b)/x]|^M$. Correctness is similar to the case of $\psi \wedge \psi'$.
- $\varphi = (A = A')$: We define and verify $|A = A'|^M$ per set-induction on A. We know $A = \mathrm{im}(f)$ and $A' = \mathrm{im}(f')$ for $f : B \to M, f' : B' \to M$ and $B, B' \in \Pi\Sigma WI$. Then we define

  $$|A = A'|^M := (\Pi b \in B.\Sigma b' \in B'.\, |f(b) = f'(b')|^M) \times (\Pi b' \in B'.\Sigma b \in B.\, |f(b) = f'(b')|^M)$$

  This is well-defined as we may assume each $|f(b) = x|^M$ to be defined per IH. Combining the IH, the results for the logical connectives, and that $A = \mathrm{im}(f)$ and $A' = \mathrm{im}(f')$ we conclude that $\exists x.x \in |A = A'|^M$ iff $A = A'$ by extensionality.
- $\varphi = (A \in A')$: We know that $A' = \mathrm{im}(f)$ for $f : B \to M$ and $B \in \Pi\Sigma WI$, and pick $|A \in A'|^M := \Sigma b \in B.|A = f(b)|^M$. The correctness of that definition directly follows from that of $|A = f(b)|^M$. ∎

Observe that all definitions above are exactly the same as those for $|\varphi| : U$, simply expressed in set theory instead of type theory.

Theorem 54 (CZF + REA + $\Pi\Sigma WI$-AC) *M is a regular, inner model of CZF*

Proof For regularity, observe that M is transitive as ever $M \ni A = \mathrm{im}(f)$ for some $f : B \to M$ and thus $A \subseteq M$. Now suppose there was some $R : A \ltimes C$. By $\Pi\Sigma WI$-AC this induces a function $g : B \to C$ with $R : A \bowtie \mathrm{im}(g)$ and $\mathrm{im}(g) \in M$.

Now we show that M satisfies all axioms of CZF.

- **Equality:** This simply carries over from the ambient CZF.
- **Paring:** This has been proven in Proposition 51 (i).
- **Union:** Pick $M \in A = \mathrm{im}(f : B \to M)$. Then for each $b \in B$, $f(b) \in M$ and there thus is a C_b with $f(b) = \mathrm{im}(g_b : C_b \to M)$. Then $\bigcup A = \mathrm{im}(h : \Sigma B.C \to M)$ where $h((b,c)) = g_b(c)$ is defined as $g_- : B \to C_b \to M$ can be obtained because B is a base by the $\Pi\Sigma WI$-AC.
- **Restricted Separation:** Let $M \ni A = \mathrm{im}(f : B \to M)$ and $\varphi(x)$ be a restricted formula. Then $\{a \in A \mid \varphi(a)\} = \mathrm{im}(g : \Sigma b \in B.|\varphi(f(b))|^M \to M)$ where $g(b,p) = f(b)$.

- **Strong collection:** This follows directly from the regularity of M.
- **Subset collection:** Pick $A, B \in M$ with $A = \mathrm{im}(f : C \to M)$ and $B = \mathrm{im}(g : D \to M)$ and a formula $\varphi(x, y, z)$. Then the set $\mathrm{im}(h : (C \to D) \to M)$ given by $h(r : C \to D) := \mathrm{im}(g \circ r : C \to B)$ has the desired property: Suppose there was some $U \in M$ such that $\overrightarrow{\varphi}(A, B, U)$ then by $\Pi\Sigma WI$-AC this induces a function $r : C \to D$ with $\varphi(f(c), g(r(c)), U)$. Then, clearly, $\overleftrightarrow{\varphi}(A, h(r), U)$.
- **Infinity:** We have shown that $\omega \in M$ in Proposition 51 (iii).
- **Set induction:** This simply carries over from the ambient CZF. ∎

Proposition 55 (CZF + REA + DC) $M \vDash \mathrm{DC}$

Proof Suppose $A \in M$ and pick a formula $\varphi(x, y)$ with $\forall a \in A.\exists b \in A.\varphi(a, b)$. For a given $a \in A$ there is a choice function $f : \omega \to A$ by DC. It remains to show that $f \in M$. For this, simply observe that $f = \mathrm{im}(g : \omega \to M)$ with $g(n) := (n, f(n))$ where we know that $f(n) \in M$ as $A \in M$ and by the transitivity of M. ∎

Proposition 56 (CZF + REA + $\Pi\Sigma WI$-AC) $M \vDash \mathrm{REA}$

Proof By Lemma 15 we may pick some transitive $A \in M$. We know $\mathrm{im}(f : B \to M) = A$ and each $A \ni a = (f_a : B_a \to M)$. By $\Pi\Sigma WI$-AC we can obtain from this $B : A \to M$ and $f : \Pi a \in A.B_a \to M$. Now consider $C := W a \in A.B_a$ and define $D := \mathrm{im}(g : C \to M)$ with $g(a, f) := \mathrm{im}(g \circ f)$. We claim that D is the regular extension of A.

- $A \subseteq D$**:** As A is transitive, we may prove this per set-induction on $a \in A$: Suppose each $b \in a$ was in D. With the $\Pi\Sigma WI$-AC, this yields a function $h : B_a \to C$ with $f_a(b) = g(h(b))$ for each $b \in B_a$. Thus $a = \mathrm{im}(h) = g(a, h)$ and thereby $a \in D$.
- D **is transitive:** Pick $d \in D$ then $d = g(a, h)$ for $a \in A$ and $h : B_a \to C$. But this means for each $d' \in d$ there is a $b \in B_a$ such that $d' = g(h(b))$, meaning $d' \in D$.
- D **is closed under relational collection:** If $d = g(a, h) \in D$ and there is an $R : d \ltimes D$ this induces, by $\Pi\Sigma WI$-AC, a function $c : B_a \to C$ such that $(g(h(b)), g(c(b))) \in R$. Then take $d' := g(a, c)$ for a set $d' \in D$ with $R : d \bowtie d'$. ∎

References

[1] Peter Aczel. "The type theoretic interpretation of constructive set theory". In: **Studies in Logic and the Foundations of Mathematics**. Vol. 96. Elsevier, 1978, pp. 55–66.

[2] Peter Aczel. "The type theoretic interpretation of constructive set theory: choice principles". In: **Studies in Logic and the Foundations of Mathematics**. Vol. 110. Elsevier, 1982, pp. 1–40.

[3] Peter Aczel. “The type theoretic interpretation of constructive set theory: inductive definitions”. In: **Studies in Logic and the Foundations of Mathematics**. Vol. 114. Elsevier, 1986, pp. 17–49.

[4] Peter Aczel. “The Relation Reflection Scheme”. In: **Mathematical Logic Quarterly** 54.1 (2008). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/malq.200710035, pp. 5–11. ISSN: 1521-3870. DOI: 10.1002/malq.200710035. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/malq.200710035 (visited on 08/31/2022).

[5] Errett Bishop. **Foundations of constructive analysis**. Vol. 60. McGraw-Hill New York, 1967.

[6] Errett Bishop. “Mathematics as a numerical language”. In: **Studies in Logic and the Foundations of Mathematics**. Vol. 60. Elsevier, 1970, pp. 53–71.

[7] Thierry Coquand and Gérard Huet. “The calculus of constructions”. PhD thesis. INRIA, 1986.

[8] Laura Crosilla. “Set Theory: Constructive and Intuitionistic ZF”. In: **The Stanford Encyclopedia of Philosophy**. Ed. by Edward N. Zalta. Summer 2020. Metaphysics Research Lab, Stanford University, 2020.

[9] Radu Diaconescu. “Axiom of choice and complementation”. In: **Proceedings of the American Mathematical Society** 51.1 (1975), pp. 176–178.

[10] Harvey Friedman. “Set theoretic foundations for constructive analysis”. In: **Annals of Mathematics** (1977), pp. 1–28.

[11] Dov M Gabbay and Ruy JGB De Queiroz. “Extending the Curry-Howard interpretation to linear, relevant and other resource logics”. In: **Journal of Symbolic Logic** (1992), pp. 1319–1365.

[12] Jean-Yves Girard. “Interprétation fonctionnelle et élimination des coupures de l’arithmétique d’ordre supérieur”. PhD thesis. Éditeur inconnu, 1972.

[13] Jean-Yves Girard. “Linear logic”. In: **Theoretical computer science** 50.1 (1987), pp. 1–101.

[14] Nicolas D Goodman and John Myhill. “The formalization of Bishop’s constructive mathematics”. In: **Toposes, Algebraic Geometry and Logic**. Springer, 1972, pp. 83–96.

[15] William A Howard. “The formulae-as-types notion of construction”. In: **To HB Curry: essays on combinatory logic, lambda calculus and formalism** 44 (1980), pp. 479–490.

[16] Per Martin-Löf. “An intuitionistic theory of types: Predicative part”. In: **Studies in Logic and the Foundations of Mathematics**. Vol. 80. Elsevier, 1975, pp. 73–118.

[17] Per Martin-Löf. “Constructive mathematics and computer programming”. In: **Studies in Logic and the Foundations of Mathematics**. Vol. 104. Elsevier, 1982, pp. 153–175.

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

[19] John Myhill. “Constructive set theory”. In: **The Journal of Symbolic Logic** 40.3 (1975), pp. 347–382.

[20] Michel Parigot. “$\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction”. In: **International Conference on Logic for Programming Artificial Intelligence and Reasoning**. Springer. 1992, pp. 190–201.

[21] Michael Rathjen. “Choice principles in constructive and classical set theories”. In: **Logic Colloquium**. Vol. 2. Cambridge University Press. 2002, pp. 299–326.

[22] Michael Rathjen. “The anti-foundation axiom in constructive set theories”. In: **Games, logic, and constructive sets** (2003), pp. 87–108.

[23] Moses Schönfinkel. “Über die Bausteine der mathematischen Logik”. In: **Mathematische annalen** 92.3-4 (1924), pp. 305–316.

[24] Anne Sjerp Troelstra et al. “History of constructivism in the 20th century”. In: **Set Theory, Arithmetic, and Foundations of Mathematics** (2011), pp. 150–179.

[25] Jean Van Heijenoort. **From Frege to Gödel: a source book in mathematical logic, 1879-1931**. Harvard University Press, 2002.

[26] Vladimir Voevodsky. “Univalent foundations project”. In: **NSF grant application** (2010).