Zermelo's Well-Ordering Theorem in Type Theory

Danko Ilik

DCS Master Programme, Chalmers University of Technology

Abstract. Taking a 'set' to be a type together with an equivalence relation and adding an extensional choice axiom to the logical framework (a restricted version of constructive type theory) it is shown that any 'set' can be well-ordered. Zermelo's first proof from 1904 is followed, with a simplification to avoid using comparability of well-orderings. The proof has been formalised in the system AgdaLight.

1 Introduction

The well-ordering theorem is a proposition of set theory stating that any set can be well-ordered. A set M is well-ordered if there is a binary relation $<$ on M which is a linear order and for which every non-empty subset of M has a minimal element.

Georg Cantor, in the beginnings of his founding work on set theory, took this as a fact and called it the well-ordering *principle*. Later, he made attempts to prove it, thus suggesting that it should be regarded a theorem.

The first successful proof was displayed by Ernst Zermelo in a paper [1] published in 1904. In this proof he had used a principle which was later called the Axiom of Choice – he was the first to explicitly state this principle in a paper. A big debate over it arose between mathematicians in the following years.

The theorem itself was also controversial, since, for example, it implied that the set of real numbers could be well-ordered, though no such ordering was known[1]. Although that situation was controversial, it was not contradictory, since the principle of excluded middle allowed one to prove statements about the existence of an object, without requiring one to exhibit a sample of the object whose existence is proved.

The two mentioned principles, the one of excluded middle and the one of choice, were subject of much discussion in the field of foundation of mathematics during a large part of the 20th century, but in spite of that no one came to the idea that they could be simply correlated, and in this way: the principle of choice implies the principle of excluded middle. This was concluded for the first time by Diaconescu in 1975 for topos theory [4]; later there followed proofs in various other theories.

[1] Later [2] it was even shown that such an ordering can not be defined. More precisely, "there is no formula of ZF set theory which can be proved in ZFC to be a well-ordering of the reals" [3] p.423

1.1 Motivation for the Present Work

The goal of this work was to investigate whether it is possible to use type theory strengthened by an extensional choice axiom (ExtAC), instead of set theory, to prove the well-ordering theorem.

This addition allows us to derive the law of excluded middle (LEM). Thus, every proposition is decidable (in a constructive sense). As subsets in type theory are usually defined as propositional functions, we can equivalently define a subset to be a function into N_2, in which case the collection of subsets of a set, the *power-set*, is a set, hence it is possible to quantify over it.

Having ExtAC also allows us to define the function γ from Zermelo's proof, which takes a nonempty subset into one of its elements. This, and it being very clear and intuitive, makes Zermelo's first proof from 1904 a good candidate to follow. His second proof from 1908 [5], much like modern ones, use some set theoretic machinery which clutters the intuition behind it.

2 The Framework

We will work in constructive type theory (CTT) as explained in [6,7]. The theory we shall be concerned with will contain a base type Set and the constants $\Pi, \Sigma, N_0, N_1, N_2$: Set, together with their introduction and elimination rules. To these we will add the extensional axiom of choice and a constant T which lifts boolean values to propositions, defined by pattern-matching:

$$\begin{aligned}&\mathrm{T} : \mathrm{N}_2 \rightarrow \mathrm{Set}\\&\mathrm{T}\ 0 \equiv \mathrm{N}_0\\&\mathrm{T}\ 1 \equiv \mathrm{N}_1\end{aligned}$$

We also need a small set universe containing codes for N_0 and N_1, for defining T and $=_2$ (below) by pattern-matching and for having $0 \neq 1$.

2.1 Axioms of Choice

The benefit of using an intensional theory like CTT is that we can make more distinctions, such as the one between *intensional* and *extensional* axioms of choice.

The first of these (IntAC) can be proved in the type theory. It reads:

$$\forall A, B^{\mathrm{Set}}.\ \forall R^{A \rightarrow B \rightarrow \mathrm{Set}}.\ \big(\forall x^A.\ \exists y^B.\ R\ x\ y\big)\ \rightarrow\ \exists f^{A \rightarrow B}.\ \forall x^A.\ R\ x\ fx \quad (1)$$

This is not surprising, because in type theory a proof of $\big(\forall x^A.\ \exists y^B.\ R\ x\ y\big)$ is exactly a function as the one required.

The second, the extensional axiom of choice (ExtAC), knows no justification in type theory. It reads:

$$\begin{aligned}
&\forall A, B^{\mathrm{Set}}.\ \forall R^{A\to B\to \mathrm{Set}}.\ \forall =_A^{A\to A\to \mathrm{Set}}.\ \forall =_B^{B\to B\to \mathrm{Set}}.\\
&\qquad (=_A \text{ equivalence on } A) \to\ (=_B \text{ equivalence on } B) \to\\
&\qquad\quad \big(\forall x, y^A.\ x =_A y \to \forall z^B.\ R\ x\ z \to R\ y\ z\big) \to\\
&\qquad\quad \big(\forall x, y^B.\ x =_B y \to \forall z^A.\ R\ z\ x \to R\ z\ y\big) \to\\
&\qquad\qquad\quad \big(\forall x^A.\ \exists y^B.\ R\ x\ y\big) \to\\
&\qquad\quad \exists f^{A\to B}.\ \big(\forall x^A.\ R\ x\ fx\big) \wedge \big(\forall a, b^A.\ a =_A b \to fa =_B fb\big) \qquad (2)
\end{aligned}$$

In words, what is required here in addition is that the function f must respect whatever equivalence relations may be defined on A and B, which the relation R preserves. It is this ability that allows one to 'smuggle in' non-constructive principles, by encoding them into an equivalence relation on which ExtAC is applied.

2.2 Derivation of the Law of Excluded Middle

The possibility of deriving the law of excluded middle (LEM) from ExtAC is well known. It has been carried out in various theories: topos theory [4], intuitionistic set theory [8] and intensional type theory [9].

The proof here is closest to the one from [10], the difference being that we use a (non-substitutive) equivalence relation, instead of the set Id. This relation, $=_2$, is defined only in terms of T and the elimination rules of N_2; it is defined to be N_1 for two elements of N_2 when they reduce to the same canonical element, and N_0 when they do not reduce to the same canonical element.

Now, let ExtAC be given and let P be a proposition (P : Set). Define a relation R ($R : \mathrm{Rel}\ \mathrm{N}_2$) as follows:

$$R\ a\ b \equiv a =_2 b \vee P$$

We show that there exists a function $f : \mathrm{N}_2 \to \mathrm{N}_2$ such that $P \leftrightarrow f0 =_2 f1$, meaning P is decidable.

We will use (2); let us satisfy the hypotheses: for A, B take N_2, for R take the R defined above, for the equivalence on A take R again and for the equivalence on B take $=_2$. Clearly, R is an equivalence relation on N_2.

By symmetry and transitivity of R, R is left-extensional for R itself. By transitivity of R and or-introduction, R is right-extensional for $=_2$. By reflexivity of R, for any $x : \mathrm{N}_2$ there exists a $y : \mathrm{N}_2$ such that $R\ x\ y$, namely x is such a y itself.

Thus, we get the following consequence of (2):

$$\exists f^{\mathrm{N}_2\to \mathrm{N}_2}.\ \big(\forall x^{\mathrm{N}_2}.\ R\ x\ fx\big) \wedge \big(\forall a, b^{\mathrm{N}_2}.\ R\ a\ b \to fa =_2 fb\big) \qquad (3)$$

From the definition of R we have $P \to R\ 0\ 1$. From the right conjunct of (3) we have $R\ 0\ 1 \to f0 =_2 f1$. Thus

$$P \to f0 =_2 f1 \tag{4}$$

To establish the other direction, first we prove $\forall a, b^{\mathrm{N}_2}.\ fa =_2 fb \to R\ a\ b$. Let a, b be given and let $fa =_2 fb$. From the fact that R is right-extensional for $=_2$ and the left conjunct of (3) we get $R\ a\ fb$. From the same conjunct and the symmetry of R we get $R\ fb\ b$. From these and the transitivity of R we get $R\ a\ b$.

From the definition of R and decidability of $=_2$ we get $R\ 0\ 1 \to P$. From this and the conclusion of the previous paragraph

$$f0 =_2 f1 \to P \tag{5}$$

(4) and (5) establish the decidability of P.

3 The Theorem

We present the definition of an extensional set and its subsets and define operations on them. After further definitions of special kinds of subsets, we state the well-ordering theorem in terms of those. The proof follows, divided into several propositions which are numbered in the same way as their parallels in Zermelo's proof from 1904 – the difference being that our proof is more detailed.

3.1 Representation of Sets and Subsets

We introduce the notion of *extensional set*, Xet[2]. An extensional set is an object of type Set, accompanied by a relation, accompanied by a proof that the relation is an equivalence one. Two such objects are equal if their Set-objects are equal and their relations are equal.

$$\text{Xet type}$$

All judgements $\Box$ we make will be hypothetical, i.e. of the form

$$\Box\ [X : \text{Set}][=_X : X \to X \to \text{Set}][=_X \text{ equivalence on } X]$$

but we will make this hypotheticalness implicit, in order to lighten the notation. So, let an object $(X, =_X, equivX) : \text{Xet}$ be given.

We define

$$\begin{aligned}&\text{ext} : (X \to \text{Set}) \to \text{Set}\\&\text{ext}\ f \equiv \forall a, b^X.\ a =_X b \to fa \to fb\end{aligned}$$

[2] As pointed out by one of the referees, this is just the known notion of *setoid*; see [11], for example.

Subsets of a Xet object will be the boolean functions on X that are extensional:

$$\begin{aligned}&\mathcal{P} : \mathrm{Set}\\ &\mathcal{P} \equiv \Sigma\,(X \to \mathrm{N}_2, \mathrm{ext}\,([U,x]\mathrm{T}\,(Ux)))\end{aligned}$$

Inhabited, or *non-empty*, subsets are subsets that contain an element:

$$\begin{aligned}&\mathcal{P}' : \mathrm{Set} && \mathrm{nonempty} : \mathcal{P} \to \mathrm{Set}\\ &\mathcal{P}' \equiv \Sigma\,(\mathcal{P}, \mathrm{nonempty}) && \mathrm{nonempty}\ U \equiv \exists a^X.\ \mathrm{T}\ \ (U.1\ a)\end{aligned}$$

The suffix $.n$ of U is a selector, which picks the n-th component of an object of type Σ.

We also need some operations:

$$\begin{aligned}\in\, : X \to \mathcal{P} \to \mathrm{Set} &\qquad \in' : X \to \mathcal{P}' \to \mathrm{Set}\\ a \in U \equiv \mathrm{T}\ \ (U.1\ a) &\qquad a \in' U \equiv a \in U.1\end{aligned}$$

$$\begin{aligned}\subseteq\, : \mathcal{P} \to \mathcal{P} \to \mathrm{Set} &\qquad =\, : \mathcal{P} \to \mathcal{P} \to \mathrm{Set}\\ U \subseteq V \equiv \forall a^X.\ a \in U \to a \in V &\qquad U = V \equiv U \subseteq V \wedge V \subseteq U\end{aligned}$$

$$\begin{aligned}\subseteq' : \mathcal{P}' \to \mathcal{P}' \to \mathrm{Set} &\qquad =' : \mathcal{P}' \to \mathcal{P}' \to \mathrm{Set}\\ U \subseteq' V \equiv U.1 \subseteq V.1 &\qquad U =' V \equiv U.1 = V.1\end{aligned}$$

And some syntactic shortcuts:

$$\begin{aligned}\forall a \in U.\ \square &\equiv \forall a^X.\ a \in U \to \square\\ \exists a \in U.\ \square &\equiv \exists a^X.\ a \in U \wedge \square\end{aligned}$$

LEM allows us to create subsets which consist of elements of X which satisfy a given extensional property; we will write this in a form of set comprehension:

$$\begin{aligned}&\{|\} : \mathrm{ExtPred} \to \mathcal{P}\\ &\{x|P\} \equiv (\mathrm{theSubset}\ P.1, \mathrm{theExt}\ P.1)\end{aligned}$$

where x is a placeholder for the free variable in P.1 (we want to mirror set theoretic notation), where $\mathrm{ExtPred} \equiv \Sigma\,(X \to \mathrm{Set}, \mathrm{ext})$ and where

$$\begin{aligned}&\mathrm{theSubset} : (X \to \mathrm{Set}) \to (X \to \mathrm{N}_2)\\ &\mathrm{theSubset}\ P \equiv \mathrm{IntAC}\ X\ \mathrm{N}_2\ \ \big([x,b]\ \mathrm{T}b \leftrightarrow \big(Px \wedge \forall y^X.\ y =_X x \to Py\big)\big)\ \ (\cdots)\end{aligned}$$

$$\begin{aligned}&\mathrm{theExt} : (P : X \to \mathrm{Set}) \to \mathrm{ext}\,([x]T\,((\mathrm{theSubset}\ P)\,x))\\ &\mathrm{theExt}\ P \equiv (\cdots)\end{aligned}$$

To complete the proof of theSubset we need to prove $\forall x^X.\ \exists b^{\mathrm{N}_2}.\ \mathrm{T}b \leftrightarrow \big(Px \land \forall y^X.\ y =_X x \to Py\big)$, but this is immediate if we apply LEM to the right hand side of the equivalence – for b take 1 if it holds, 0 if it does not hold. The right hand side of the equivalence also gives us theExt immediately.

All predicates we shall apply comprehension on will be extensional.

Now, we have notation sufficient to mimic a set theoretic proof. We will just define a few more operators:

$$\begin{array}{lll}
\complement : \mathcal{P} \to \mathcal{P} & \setminus : \mathcal{P} \to \mathcal{P} \to \mathcal{P} & \cap : \mathcal{P} \to \mathcal{P} \to \mathcal{P} \\
\complement\, U \equiv \{x \mid x \notin U\} & U \setminus V \equiv \{x \mid x \in U \land x \notin V\} & U \cap V \equiv \{x \mid x \in U \land x \in V\}
\end{array}$$

$$\begin{array}{lll}
\{\} : X \to \mathcal{P} & \cup : \mathcal{P} \to \mathcal{P} \to \mathcal{P} & \emptyset : \mathcal{P} \\
\{a\} \equiv \{x \mid x =_X a\} & U \cup V \equiv \{x \mid x \in U \lor x \in V\} & \emptyset \equiv \{x \mid \mathrm{N}_0\}
\end{array}$$

3.2 Statement of the Theorem

We will need to be able to quantify over relations, thus we need *decidable* relations. We can lift a decidable relation into a normal one and vice-versa, since every proposition is decidable.

$$\begin{array}{ll}
\mathrm{DRel} : \mathrm{Set} & \mathrm{Rel} : \mathit{Type} \\
\mathrm{DRel} \equiv X \to X \to \mathrm{N}_2 & \mathrm{Rel} \equiv X \to X \to \mathrm{Set}
\end{array}$$

$$\begin{array}{ll}
\mathrm{dRel} : \mathrm{DRel} \to \mathrm{Rel} & \mathrm{rRel} : \mathrm{Rel} \to \mathrm{DRel} \\
\mathrm{dRel}\ D \equiv [a,b]\ \mathrm{T}\ \ (D\ a\ b) & \mathrm{rRel}\ R \equiv \cdots
\end{array}$$

For the definition of rRel we use IntAC; for details see the formalisation.

Now, some classes of relations *on subsets*. When a relation is trichotomous, transitive and linear:

$$\begin{array}{l}
\mathrm{trich} : \mathcal{P} \to \mathrm{Rel} \to \mathrm{Set} \\
\mathrm{trich}\ U < \ \equiv \forall a, b \in U.\ \ (a < b \leftrightarrow b \not< a \land a \neq_X b) \land (a =_X b \leftrightarrow a \not< b \land b \not< a)
\end{array}$$

$$\begin{array}{l}
\mathrm{trans} : \mathcal{P} \to \mathrm{Rel} \to \mathrm{Set} \\
\mathrm{trans}\ U < \ \equiv \forall a, b, c \in U.\ a < b \to b < c \to a < c
\end{array}$$

$$\begin{array}{l}
\mathrm{linear} : \mathcal{P} \to \mathrm{Rel} \to \mathrm{Set} \\
\mathrm{linear}\ U < \ \equiv (\mathrm{trich}\ U <) \land\ \ (\mathrm{trans}\ U <)
\end{array}$$

We also need a property expressing that a subset has a minimal element:

$$\begin{array}{l}
\mathrm{hasLeast} : \mathcal{P} \to \mathrm{Rel} \to \mathrm{Set} \\
\mathrm{hasLeast}\ U < \ \equiv \exists a \in U.\ \forall b \in U.\ b \not< a
\end{array}$$

And a property expressing that a subset is well-ordered:

$$\begin{aligned}&\text{wellOrdered} : \mathcal{P} \to \text{Rel} \to \text{Set}\\ &\text{wellOrdered } U < \; \equiv (\text{linear } U <) \wedge \left(\forall V^{\mathcal{P}'}.\ V.1 \subseteq U \to \text{hasLeast } V.1 <\right)\end{aligned}$$

We are ready to state

Theorem 1 (Zermelo's Well-Ordering) *Any extensional set can be well-ordered.*

$$\left(\exists R^{\text{DRel}}.\ \forall U^{\mathcal{P}}.\ \text{wellOrdered } U\,(\text{dRel } R)\right)$$

3.3 Proof

We will now proceed with the proof following the one from 1904, enumerating the steps like it is done there. The key idea will be to use a choice function, γ, in defining a well-ordering relation $<$ in such a way that γ picks the $<$-least element of any subset.

(2) The Function γ. There is a function which takes a non-empty subset of X and gives an element of X which is contained in the subset. This function is extensional in respect to $='$, $=_X$. Formally:

$$\exists \gamma^{\mathcal{P}' \to X}.\ \left(\forall U^{\mathcal{P}'}.\ \gamma U \in' U\right) \wedge \left(\forall U, V^{\mathcal{P}'}.\ U =' V \to \gamma U =_X \gamma V\right)$$

Proof. We will use the extensional axiom of choice. Put $\mathcal{P}'$ for A, X for B, $(x \in' U)$ for R, $='$ for $=_A$ and $=_X$ for $=_B$. It is easy to see that $='$ is an equivalence relation, and $=_X$ is such by hypothesis. To get the desired function, we need only prove the following three things:

- $\forall U, V^{\mathcal{P}'}.\ U =' V \to \forall z^X.\ z \in' U \to z \in' V$. This we get immediately from the definition of $='$.
- $\forall x, y^X.\ x =_X y \to \forall W^{\mathcal{P}'}.\ x \in' W \to y \in' W$. This is immediate from the extensionality of subsets.
- $\forall U^{\mathcal{P}'}.\ \exists y^X.\ y \in' U$. This follows from the non-emptiness of U.

(3) γ-Sets. An *initial segment* of a subset, for a given element of X and a relation, is the subset of all those elements which are in relation with the given one. Formally:

$$\begin{aligned}&\text{IS} : \mathcal{P} \to X \to \text{Rel} \to \mathcal{P}\\ &\text{IS } U\ a < \; \equiv \{x \mid x \in U \wedge x < a\}\end{aligned}$$

A subset is called a γ-*set*, for a given relation, if it is well-ordered by the relation and if for any element a therein, γ takes the complement of the initial segment for a, into a itself. Formally:

$$\begin{aligned}&\text{GS} : \mathcal{P} \to \text{Rel} \to \text{Set}\\ &\text{GS } U < \; \equiv (\text{wellOrdered } U <) \wedge\\ &\left(\forall a \in U.\ \forall ne^{\text{nonempty} \complement (\text{IS } U\ a<)}.\ a =_X \gamma\left(\left(\complement\left(\text{IS } U\ a <\right)\right), ne\right)\right)\end{aligned}$$

(4) Example Subsets of X Which Are γ-Sets. Suppose X is inhabited, $\mathcal{X} \equiv \{x \mid \mathrm{N}_1\}$ is a subset containing all elements of X, ne : nonempty$\mathcal{X}$ and take the following subset:

$$\begin{aligned} &M' : \mathcal{P} && m_1 : X \\ &M' \equiv \{x \mid x =_X m_1\} && m_1 \equiv \gamma\,(\mathcal{X}, ne) \end{aligned}$$

Define the ordering:

$$\begin{gathered} <_1 \colon \mathrm{Rel} \\ x <_1 y \equiv \mathrm{N}_0 \end{gathered}$$

It is easy to check that $<_1$ makes M' a γ-set. Similarly, the subset $\{x \mid x =_X m_1 \vee x =_X m_2\}$, where $m_2 \equiv \gamma(\mathcal{X} \setminus \{m_1\}, ne')$ and ne' : nonempty$(\mathcal{X} \setminus \{m_1\})$, is a γ-set.

(5) If M_1, M_2 Are Different γ-Sets, Then One Is an Initial Segment of the Other. Formally:

$$\begin{aligned} &\forall M_1, M_2^{\mathcal{P}}.\ \forall <_1, <_2^{\mathrm{Rel}}.\ \mathrm{GS}\ M_1 <_1 \wedge\ \mathrm{GS}\ M_2 <_2 \rightarrow \\ &\qquad (M_1 = M_2) \vee (\exists x_1 \in M_1.\ \mathrm{S}_1 x_1 = M_2) \vee (\exists x_2 \in M_2.\ \mathrm{S}_2 x_2 = M_1) \end{aligned}$$

where

$$\mathrm{S}_\Box \equiv [x]\mathrm{IS}\ M_\Box\ x <_\Box$$

In the original paper, as well as modern papers like [12], this step is proven by using the comparability of well-orderings, which grants that there is an order-preserving injection from one of M_1, M_2 into the other. Then one proceeds to prove that this injection must be the identity. As the comparability is not easier to prove than the well-ordering theorem itself, we provide a direct proof using well-founded induction.

Proof. Let $M_1, <_1, M_2, <_2$ be given and let them be γ-sets. We need the following lemma:

Lemma 1. *An initial segment of M_1 is an initial segment of M_2 or is M_2; or a smaller initial segment of M_1 is M_2.*

$$\forall x \in M_1.\ (x \in M_2 \wedge \mathrm{S}_1 x = \mathrm{S}_2 x) \vee (\exists x_1 \in \mathrm{S}_1 x.\ \mathrm{S}_1 x_1 = M_2) \vee (\mathrm{S}_1 x = M_2)$$

Proof. M_1 is well-ordered, thus we can use well-founded induction on it[3]: for $P : X \rightarrow \mathrm{Set}$, we have that $(\forall x \in M_1.\ (\forall y \in M_1.\ y <_1 x \rightarrow Py) \rightarrow Px) \rightarrow \forall x \in$

[3] Suppose that a subset U is well-ordered and not well-founded, take the minimal element t of U for which P does not hold, and derive a contradiction. All the details are in the formalisation.

$M_1.\ Px$. For P we take the expression in the scope of the universal quantifier from the formulation of the lemma.

Let $x \in M_1$ be given. We use the classical tautology (for $R, A, B, C : X \to \mathrm{Set}$):

$$\begin{aligned}(\forall x^X.\ Rx \to Ax \vee Bx \vee Cx) \to& \\ (\forall x^X.Rx \to Ax) \vee (\exists x^X.Rx \wedge Bx) \vee (\exists x^X.Rx \wedge Cx)& \qquad (6)\end{aligned}$$

on the induction hypothesis, and get these 3 cases:

1. $\forall y \in M_1.\ y <_1 x \to (y \in M_2 \wedge \mathrm{S}_1 y = \mathrm{S}_2 y)$. Thus, $\mathrm{S}_1 x \subseteq M_2$. We look into the following two cases:
   (a) $\mathrm{S}_1 x = M_2$.
   (b) $\mathrm{S}_1 x \neq M_2$. $\mathrm{S}_1 x \subseteq M_2$. Let t be the least element of the subset $M_2 \setminus \mathrm{S}_1 x$ for $<_2$. We will show that $\mathrm{S}_1 x = \mathrm{S}_2 t$:
      - Let $a \in \mathrm{S}_1 x$. Then $a \in M_2$ and we need to show that $a <_2 t$. If $a \not<_2 t$, then $t <_2 a$ or $a =_X t$. $a =_X t$ is not possible as $t \notin \mathrm{S}_1 x$ by definition. If $t <_2 a$, $t \in \mathrm{S}_2 a$ and by the induction hypothesis $\mathrm{S}_2 a = \mathrm{S}_1 a \subseteq \mathrm{S}_1 x \ni t$, again a contradiction with the definition of t. So, $a \in \mathrm{S}_2 t$.
      - Let $b \in \mathrm{S}_2 t$. If $b \notin \mathrm{S}_1 x$, then $b \in M_2 \setminus \mathrm{S}_1 x$ and then, since t is minimal, it must be that $b \not<_2 t$, a contradiction with $b \in \mathrm{S}_2 t$. So, $b \in \mathrm{S}_1 x$.

      We have that $\mathrm{S}_1 x = \mathrm{S}_2 t$. From $\mathrm{S}_1, \mathrm{S}_2$ being initial segments of the γ-sets M_1, M_2, $x =_X \gamma(\mathsf{C}(\mathrm{S}_1 x)) =_X \gamma(\mathsf{C}(\mathrm{S}_2 t)) =_X t$. Thus, $\mathrm{S}_1 x = \mathrm{S}_2 x$.
2. $\exists y \in M_1.\ y <_1 x \wedge (\exists x_1 \in \mathrm{S}_1 y.\ \mathrm{S}_1 x_1 = M_2)$. Let such y, x_1 be given. Then $x_1 \in \mathrm{S}_1 x$, so we get the 2nd disjunct of Px.
3. $\exists y \in M_1.\ y <_1 x \wedge (\mathrm{S}_1 y = M_2)$. Taking y for x_1, we immediately get the 2nd disjunct of Px.

We use tautology (6) again, now on the lemma itself and thus get 3 cases:

1. $\forall x \in M_1.\ x \in M_2 \wedge \mathrm{S}_1 x = \mathrm{S}_2 x$. Define the following subsets:

$$\begin{aligned}S &\equiv \{y \mid \exists z \in M_1.\ y \in \mathrm{S}_1 z\}\\ T_1 &\equiv M_1 \setminus S\\ T_2 &\equiv M_2 \setminus S\end{aligned}$$

   S is the subsets of all elements of M_1 which belong to some initial segment of M_1. T_1, T_2 contain the remaining elements. From the hypothesis we have $M_1 \subseteq M_2$ and $S \subseteq M_2$. We will distinguish on the emptiness of T_1, T_2:
   (a) $T_1 = \emptyset$. As $S \subseteq M_1$ and $\emptyset = M_1 \setminus S$, $M_1 = S$.
      i. $T_2 = \emptyset$. As $S \subseteq M_1 \subseteq M_2$ and $\emptyset = M_2 \setminus S$, $M_2 = S = M_1$.
      ii. $T_2 \neq \emptyset$. Let t be the least element of T_2 for $<_2$. We want to show that $\mathrm{S}_2 t = S = M_1$:
         - if $a \in \mathrm{S}_2 t$, $a <_2 t$, so $a \notin T_2$, because t is the minimal of T_2. As $a \in M_2$ and $a \notin T_2$, $a \in S$.

- let $a \in S$; then $a \notin T_2$. Does $a \in M_2$ and $a <_2 t$? $a \in M_1 \subseteq M_2$. Let $a \not<_2 t$:
    - if $t <_2 a$, then $t \in S$ as, from the hypothesis, $\mathrm{S}_1 a = \mathrm{S}_2 a$; but, $t \notin S$ by definition.
    - if $a =_X t$, $a \in T_2$, a contradiction.

  Thus, $a <_2 t$ and $a \in \mathrm{S}_2 t$.

(b) $T_1 \neq \emptyset$. We show that T_1 can contain only one element: let $t_1, t_2 \in T_1$ and, without loss of generality, let $t_1 <_1 t_2$; then $t_1 \in \mathrm{S}_1 t_2$, thus $t_1 \in S$, thus $t_1 \notin T_1$, which is a contradiction. So, T_1 has exactly one element; call it t.

From $M_1 \subseteq M_2$ and the definitions of T_1, T_2, $T_1 \subseteq T_2$ and $t \in T_2$.

i. $T_2 = \{t\}$. Then $M_2 = S \cup T_2 = S \cup T_1 = M_1$.

ii. $T_2 \neq \{t\}$. Let t' be the least element of the subset $T_2 \setminus \{t\}$. Then $t <_2 t'$: if $t' =_X t$, then $t \in T_2 \setminus \{t\}$, a contradiction; if $t' <_2 t$, by the main hypothesis $\mathrm{S}_1 t = \mathrm{S}_2 t$, so $t' \in \mathrm{S}_1 t$ and $t \in S$, a contradiction.
Thus, $t <_2 t'$ and we have that t is the minimal of T_2 for $<_2$. Using this, like in case (a.ii) we get $S = \mathrm{S}_2 t$ and $M_1 = S \cup \{t\} = \mathrm{S}_2 t \cup \{t\}$.
We show that $M_1 = \mathrm{S}_2 t'$:
- if $x \in M_1$, then $x \in \mathrm{S}_2 t$ or $x =_X t$. If $x \in \mathrm{S}_2 t$, then $x <_2 t <_2 t'$, thus $x \in \mathrm{S}_2 t'$. If $x =_X t$, then $x <_2 t'$, thus $x \in \mathrm{S}_2 t'$.
- if $x \in \mathrm{S}_2 t'$, then $x <_2 t'$. We look at the 3 cases:
    - $x =_X t$. Then $x \in T_1 \subseteq M_1$.
    - $x <_2 t$. Then $x \in \mathrm{S}_2 t = M_1$.
    - $t <_2 x$. Then $t <_2 x <_2 t'$, so t' is not the minimal element of $T_2 \setminus \{t\}$.

2. $\exists x \in M_1.\ \exists x_1 \in M_1.\ x_1 <_1 x \wedge \mathrm{S}_1 x_1 = M_2$. Thus, M_2 is an initial segment of M_1. QED
3. $\exists x \in M_1.\ \mathrm{S}_1 x = M_2$. Again, M_2 is an initial segment of M_1. QED

(6) A Consequence. If two γ-sets have an element a in common, then their initial segments for a are the same. Formally:

$$\forall M_1, M_2^{\mathcal{P}}.\ \forall <_1, <_2^{\mathrm{Rel}}.\ \mathrm{GS}\ M_1 <_1 \wedge\ \mathrm{GS}\ M_2 <_2 \rightarrow$$
$$\forall a \in M_1 \cap M_2 \rightarrow (\mathrm{S}_1 a = \mathrm{S}_2 a)$$

Proof. We can use (5) to decide which of the γ-sets is an initial segment of the other. The required follows from the definition of initial segment.

(7) *X* Is Well-Ordered. Define the following relation on X:

$$a < b \equiv \exists M_a^{\mathcal{P}}.\ \exists D_a^{\mathrm{DRel}}.\ \mathrm{GS}\ M_a\ (\mathrm{dRel}\ D_a) \wedge a \in M_a \wedge$$
$$\forall M_b^{\mathcal{P}}.\ \forall D_b^{\mathrm{DRel}}.\ \mathrm{GS}\ M_b\ (\mathrm{dRel}\ D_b) \rightarrow b \in M_b \rightarrow$$
$$\exists \beta . \beta \in M_b \wedge \mathrm{IS}\ M_b\ \beta\ (\mathrm{dRel}\ D_b) = M_a$$

This relates two elements of X, if they are γ-elements and a γ-set containing the first element is an initial segment of a γ-set containing the other.

Call $x : X$ a *γ-element* if there exists a γ-set, for the relation $<$, which contains it:

$$\begin{aligned}&\mathrm{GE} : X \to \mathrm{Set}\\ &\mathrm{GE}\ x \equiv \exists M_\gamma^{\mathcal{P}}.\ x \in M_\gamma \wedge \mathrm{GS}\ M_\gamma <\end{aligned}$$

Let L_γ be the subset of all γ-elements:

$$\begin{aligned}&L_\gamma : \mathcal{P}\\ &L_\gamma \equiv \{x \mid \mathrm{GE}\ x\}\end{aligned}$$

To establish that X is well-ordered, in the following 5 lemmas, we show that L_γ is well-ordered and that $\mathcal{X} \subseteq L\gamma$. Recall that $\mathcal{X}$ is a subset containing all elements of X.

(7-I) $<$ Is Trichotomous on L_γ. First, we lighten the notation by writing $M_a \prec M_b$ when M_a is an initial segment of M_b, and by omitting the relations, which are always quantified together with their corresponding γ-sets.

- Let $a, b \in L_\gamma$ and $a < b$. Then there exist a γ-set M_a containing a, such that for any M_b containing γ-set of b, $M_a \prec M_b$.
  If $a =_X b$, then M_a is a containing γ-set of b as well, and we have $M_a \prec M_a$, which is not possible.
  If $b < a$, then there exists $L_b \ni b$ s.t. for every $L_a \ni a$, $L_b \prec L_a$. If we put L_b in place of M_b and M_a in place of L_a, we get both $L_b \prec M_a$ and $M_a \prec L_b$, which is not possible.
- Let $a, b \in L_\gamma$ and $b \not< a$ and $a \neq_X b$. From $b \not< a$ we have $\forall L_b.\ \exists L_a.\ L_b \not\prec L_a$. We will use the fact that b is a γ-element, to extract a containing W_b, which is a γ-set for $<$. We get that there exists a gamma set $L_a \ni a$ such that $W_b \not\prec L_a$. From step (5) we have that $W_b = L_a$ or $L_a \prec W_b$. In any case, $a \in W_b$ and we can use the hypotheses and the trichotomy of $<$ on W_b to complete the proof.

(7-II) $<$ Is Linear. We need to show that $<$ is transitive. Let $a, b, c \in L_\gamma$ and $a < b, b < c$. From $\exists M_a.\ \forall M_b.\ M_a \prec M_b$ and $\exists M_b.\ \forall M_c.\ M_b \prec M_c$, we have $\exists M_a.\ \forall M_c.\ M_a \prec M_c$, i.e. $a < c$.

(7-III) $<$ Well-Orders L_γ. Let $L' \subseteq L_\gamma, L' \neq \emptyset$. Pick $a \in L'$ and define $L'' \equiv \{x \mid (x \in \mathrm{IS}\ L'\ a <) \vee (x =_X a)\}$. If M' is a witnessing γ-set of a, then (by step (6)) $L'' \subseteq M'$. Since L'' is not empty (it has at least a) and is a subset of a well-ordered M', L'' has a minimal element, which (because of the definition of L'') must be a minimal of L' as well.

(7-IV) L_γ Is a γ-Set. Let $a \in L_\gamma$, M_a be its witnessing γ-set for $<$; let $B \equiv \mathrm{IS}\ M_a\ a <$ and let $A \equiv \mathrm{IS}\ L_\gamma\ a <$. We will show that $A = B$; from this will follow that $\gamma(\complement A) =_X \gamma(\complement B) =_X a$.

- Let $x \in A$. Then $x < a$, so there is a containing γ-set M_x, such that $M_x \prec M_a$. So, $x \in M_a$ and $x < a$, thus $x \in B$.
- Let $x \in B$. Then it is a γ-element, since it belongs to M_a, so $x \in A$.

(7-V) $\mathcal{X} \subseteq L_\gamma$. If the Set X is not inhabited, then $\mathcal{X} = \emptyset$ and trivially $\mathcal{X} \subseteq L_\gamma$.

If the Set X is inhabited, then let $x \in \mathcal{X}$ and let $x \notin L_\gamma$. Then, $x \in \complement L_\gamma$, thus this complement is not empty, $ne : \mathrm{nonempty}\complement L_\gamma$, and we can define

$$\begin{aligned} &m : X \\ &m \equiv \gamma(\complement L_\gamma, ne) \end{aligned}$$

Now, the relation $<$ makes m larger than all elements in the subset:

$$\begin{aligned} &L' : \mathcal{P} \\ &L' \equiv \{x \mid (x \in L_\gamma) \vee (x =_X m)\} \end{aligned}$$

It is not hard, but it takes some work to check that L' is a γ-set for $<$ (for details, see the formalisation). Since $m \in L'$, m is a γ-element, thus it must be that $m \in L_\gamma$, which is a contradiction. So, indeed, $\mathcal{X} \subseteq L_\gamma$, and $\mathcal{X}$ is well-ordered.

4 Formalisation

The presented proof served as a sketch for a formalisation [13] that was checked using AgdaLight [14], a version of the Agda [15] proof checker for constructive type theory.

In Agda a proof term is not constructed by using tactics, but is directly given. We use nested let-expressions and explicit type annotations to give structure to the proofs. This style of writing comes close to the requirements of Leslie Lamport's proof style[16]. We hope to have produced a readable formalised document.

Further work of the formalisation is possible, especially in respect to handling more systematically subsets created by set comprehension.

5 Related Work

In [17], Peter Aczel has shown how to interpret full Zermelo-Fraenkel set theory in constructive type theory + LEM. The type theory used is a standard one (with W), thus stronger than the one we use.

In [18], Per Martin-Löf shows that in type theory, the extensional axiom of choice is equivalent to Zermelo's axiom of choice. As a consequence of the work from Peter Aczel, full ZFC can be interpreted in constructive type theory + ExtAC.

Acknowledgements

The topic of this text came into being during the Types 2005 summer school in Göteborg, during a conversation with Thierry Coquand, my master's thesis' supervisor, and Per Martin-Löf, who on this school held a lecture in which he used constructive type theory to analyse Zermelo's axiom of choice. I thank Thierry for his good advises, the Swedish Institute for their financial support and the referees for the detailed comments.

References

1. Zermelo, E.: Beweis, daß jede menge wohlgeordnet werden kann. Mathematische Annalen **59** (1904) 514–516 English translation in van Heijenoort, 1967.
2. Feferman, S.: Some applications of the notions of forcing and generic sets. Fundamenta Mathematicae **56** (1964) 325–345
3. Beeson, M.J.: Foundations of Constructive Mathematics: Metamathematical Studies. Springer-Verlag (1985)
4. Diaconescu, R.: Axiom of choice and complementation. Proceedings of A.M.S. **51** (1975) 176–178
5. Zermelo, E.: Neuer beweis für die möglichkeit einer wohlordnung. Mathematische Annalen **65** (1908) 107–128 English translation in van Heijenoort, 1967.
6. Nordström, B., Petersson, K., Smith, J.M.: Martin-Löf's Type Theory. In: Handbook on Logic in Computer Science, Oxford University Press. Volume 5. Oxford University Press (2000)
7. Martin-Löf, P.: On the meanings of the logical constants and the justifications of the logical laws. Nordic Journal of Philosophical Logic **1**(1) (1996) 11–60 Text of lectures originally given in 1983 and distributed in 1985.
8. Goodman, N.D., Myhill, J.: Choice implies excluded middle. Zeitschrift für Mathematische Logik und Grundlagen der Mathematik **24** (1978) 461
9. Maietti, M.E., Valentini, S.: Can you add power-sets to martin-löf's intuitionistic set theory? Mathematical Logic Quarterly **45** (1999) 521–532
10. Carlström, J.: EM + ext- + ACint is equivalent to ACext. Mathematical Logic Quarterly **50**(3) (2004) 236–240
11. Barthe, G., Capretta, V., Pons, O.: Setoids in type theory. Journal of Functional Programming **13**(2) (2003) 261–293
12. Kanamori, A.: Zermelo and set theory. The Bulletin of Symbolic Logic **10**(4) (2004) 487–553
13. Ilik, D.: Formalisation of zermelo's well-ordering theorem in type theory. `http://www.mdstud.chalmers.se/~danko/` (2006)
14. Norell, U.: Agdalight. `http://www.cs.chalmers.se/~ulfn/agdaLight/` (2006)
15. Coquand, C.: Agda. `http://agda.sourceforge.net/` (2000)
16. Lamport, L.: How to write a proof (1993)
17. Aczel, P.: The type theoretic interpretation of constructive set theory. In Macintyre, A., Pacholski, L., Paris, J., eds.: Logic Colloquium '77, North-Holland Publishing Company (1978) 55–66
18. Martin-Löf, P.: 100 years of zermelo's axiom of choice: what was the problem with it? (2004)