A COQ VERSION OF ZERMELO'S 1908 PROOF OF THE WELL-ORDERING THEOREM

CHAD E. BROWN

We briefly describe Zermelo's second proof of the well-ordering theorem [2]. The presentation corresponds to a formalized version in Coq. In order to make the connection to the Coq formalization clear, we give the informal description in the language of type theory instead of set theory.

Let A be a type. We will refer to elements p, q of type $A \to \mathsf{Prop}$ as *sets* and elements D, E of type $(A \to \mathsf{Prop}) \to \mathsf{Prop}$ as *properties*. We say an element x of type A is *in* a set p when px holds. We will use $p \subseteq q$ as notation for $\forall x.px \to qx$ and $D \subseteq E$ as notation for $\forall p.Dp \to Ep$. Given a property D, $\bigcap D$ is defined to be the set $\lambda x.\forall p.Dp \to px$.

Assume $\varepsilon : (A \to \mathsf{Prop}) \to A$ is a choice operator on A. That is, we assume for every nonempty set p, $p(\varepsilon p)$ holds. We also assume ε is extensional: $\varepsilon p = \varepsilon q$ if $p \subseteq q$ and $q \subseteq p$.

Given a set p, p' is defined to be the set $\lambda x.px \wedge x \neq \varepsilon p$. That is, p' contains precisely the elements of p except εp.

Our goal is to define a relation $\leq : A \to A \to \mathsf{Prop}$ such that $\leq$ is a well-ordering of A. That is, $\leq$ must be a linear ordering ($\leq$ must reflexive, transitive, antisymmetric and linear) and must have the following well-ordering property: For every nonempty set p, there is an element x such that px and $\forall y.py \to y \leq x$.

In order to define $\leq$, we first inductively define a property C.

$$C_2\ \frac{Cp}{Cp'} \qquad\qquad C_3\ \frac{D \subseteq C}{C(\bigcap D)}$$

Zermelo [2] calls this property M and defines it as the intersection of all Θ-chains, where a Θ-chain is defined (up to some minor details) as a property closed under the rules above.

We will now prove the sets satisfying C are linearly ordered by $\subseteq$. The idea for this proof can be found in [2].

Lemma 1. *If Cp and Cq, then $p \subseteq q$ or $q \subseteq p$.*

Proof. We prove $\forall p.Cp \to \forall q.Cq \to p \subseteq q \vee q \subseteq p$ by induction on Cp. The case for the rule C_3 is easier to argue so we present it first. In this case we have $D \subseteq C$ and assume as inductive hypothesis

$$\forall p.Dp \to \forall q.Cq \to p \subseteq q \vee q \subseteq p.$$

Date: March 6, 2014.

We must prove $\forall q.Cq \to \bigcap D \subseteq q \vee q \subseteq \bigcap D$. Let q such that Cq be given. By excluded middle, there is either some p in D such that $p \subseteq q$ or there is no such p. If there is such a p, then clearly $\bigcap D \subseteq q$. Otherwise, the inductive hypothesis implies $\forall p.Dp \to q \subseteq p$ and $q \subseteq \bigcap D$ follows.

All that remains is to argue the C_2 case. We assume

$$\forall q.Cq \to p \subseteq q \vee q \subseteq p \tag{1}$$

as the inductive hypothesis and must prove

$$\forall q.Cq \to p' \subseteq q \vee q \subseteq p'.$$

In order to prove this, we argue by induction on Cq.

As above, we argue the C_3 subcase first. Assume $E \subseteq C$ and the inductive hypothesis

$$\forall q.Eq \to p' \subseteq q \vee q \subseteq p'.$$

We must prove $p' \subseteq \bigcap E$ or $\bigcap E \subseteq p'$. By excluded middle, there is either a q in E such that $q \subseteq p'$ or there is no such q. If there is such a q, then $\bigcap E \subseteq p'$. If there is no such q, then the inductive hypothesis implies $\forall q.Eq \to p' \subseteq q$ and $p' \subseteq \bigcap E$ follows.

Finally, we argue the C_2 subcase. In this case we assume Cq and an inductive hypothesis $p' \subseteq q \vee q \subseteq p'$. We must prove $p' \subseteq q'$ or $q' \subseteq p'$. If $q \subseteq p'$, then $q' \subseteq p'$ and we are done. Assume $p' \subseteq q$. If εq is not in p', then $p' \subseteq q'$ and we are done. Assume εq is in p'. By (1) for q' we know either $p \subseteq q'$ or $q' \subseteq p$. If $p \subseteq q'$, then $p' \subseteq q'$ and we are done. Assume $q' \subseteq p$. If εp is not in q', then $q' \subseteq p'$ and we are done. Assume εp is in q'. In this final subcase, we will prove a contradiction. Since εp is in q', we know εp is in q and $\varepsilon p \neq \varepsilon q$. To obtain a contradiction, we will prove $\varepsilon p = \varepsilon q$. By extensionality of ε, it suffices to prove $p \subseteq q$ and $q \subseteq p$.

To prove $p \subseteq q$, assume x is in p. If $x = \varepsilon p$, then we already know x is in q since εp is in q'. If $x \neq \varepsilon p$, then x is in p' and is hence in q since $p' \subseteq q$.

To prove $q \subseteq p$, assume x is in q. If $x = \varepsilon q$, then we already know x is in p since εq is in p'. If $x \neq \varepsilon q$, then x is in q' and is hence in p since $q' \subseteq p$. □

The following lemma is a consequence of the lemma above.

Lemma 2. *If Cp, Cq and εp is in q, then $p \subseteq q$.*

Proof. Assume Cp, Cq and εp is in q. Since Cp' we can apply Lemma 1 to conclude either $p' \subseteq q$ or $q \subseteq p'$. We cannot have $q \subseteq p'$ since εp is in q but is not in p'. Hence $p' \subseteq q$. Since εp is in q, this is enough to conclude $p \subseteq q$. □

For each set p, let $\overline{p}$ be the least set satisfying C such that $p \subseteq \overline{p}$. In other words, $\overline{p}$ is the intersection of all q such that Cq and $p \subseteq q$. We call $\overline{p}$ the *closure of* p.

By the definition of $\overline{p}$ and C_3 it is clear that $p \subseteq \overline{p}$ and $C\overline{p}$ hold. We can also prove that if p is nonempty, then $\varepsilon\overline{p}$ is in p.

Lemma 3. *If p is a nonempty set, then $\varepsilon\overline{p}$ is in p.*

Proof. Let p be a given nonempty set. Assume $\varepsilon\overline{p}$ is not in p. Let q be $\overline{p}'$. We prove q is a set satisfying C such that $p \subseteq q$. We know Cq by C_2 and $C\overline{p}$. In order to prove $p \subseteq q$, let x in p be given. We know x is in $\overline{p}$ since $p \subseteq \overline{p}$. We know $x \neq \varepsilon\overline{p}$ since we have assumed $\varepsilon\overline{p}$ is not in p. Hence x is in q.

The definition of $\overline{p}$ implies $\overline{p} \subseteq q$. Since p is nonempty and $p \subseteq \overline{p}$, we know $\overline{p}$ is nonempty and so $\varepsilon\overline{p}$ is in $\overline{p}$. Hence $\varepsilon\overline{p}$ is in q, contradicting the choice of q as $\overline{p}'$. □

Let $\{a\}$ be the set $\lambda x.x = a$.

Lemma 4. $\varepsilon\overline{\{a\}} = a$

Proof. By Lemma 3 we know $\varepsilon\overline{\{a\}}$ is in $\{a\}$. That is, $\varepsilon\overline{\{a\}} = a$ □

We define $a \leq b$ to mean b is in $\overline{\{a\}}$. We prove $\leq$ is the desired well-ordering.

Theorem 1. *$\leq$ is a well-ordering on A. That is, we have the following:*

(1) $\leq$ is reflexive.
(2) $\leq$ is transitive.
(3) $\leq$ is antisymmetric.
(4) $\leq$ is linear.
(5) Every nonempty set has a $\leq$-least element.

Proof.

(1) To prove $a \leq a$, we must prove a is in $\overline{\{a\}}$. This is obvious since $\{a\} \subseteq \overline{\{a\}}$.

(2) Assume $a \leq b$ and $b \leq c$. We prove $a \leq c$. That is, we prove c is in $\overline{\{a\}}$. Let p be such that Cp and $\{a\} \subseteq p$. Since $a \leq b$, b is in p. Hence $\{b\} \subseteq p$. Since $b \leq c$, c is in p. Hence c is in $\overline{\{a\}}$.

(3) Assume $a \leq b$ and $b \leq a$. We prove $a = b$. By Lemma 4 it suffices to prove $\varepsilon\overline{\{a\}} = \varepsilon\overline{\{b\}}$. By extensionality of ε it suffices to prove $\overline{\{a\}} \subseteq \overline{\{b\}}$ and $\overline{\{b\}} \subseteq \overline{\{a\}}$. If c is in $\overline{\{a\}}$ (i.e., $a \leq c$), then c is in $\overline{\{b\}}$ (i.e., $b \leq c$) since $b \leq a$ and we have already proven $\leq$ is transitive. If c is in $\overline{\{b\}}$ (i.e., $b \leq c$), then c is in $\overline{\{a\}}$ (i.e., $a \leq c$) since $a \leq b$ and we have already proven $\leq$ is transitive.

(4) Let a and b be given. By Lemma 1 either $\overline{\{a\}} \subseteq \overline{\{b\}}$ or $\overline{\{b\}} \subseteq \overline{\{a\}}$. If $\overline{\{a\}} \subseteq \overline{\{b\}}$, then $b \leq a$. If $\overline{\{b\}} \subseteq \overline{\{a\}}$, then $a \leq b$.

(5) Let p be a nonempty set. Let x be $\varepsilon\overline{p}$. We will prove x is the least element of p. We know x is in p by Lemma 3. Let y in p be given. We will prove $x \leq y$. That is, we prove y is in $\overline{\{x\}}$. Let q be such that Cq and $\{x\} \subseteq q$. We must prove y is in q. Since x is in q, Lemma 2 implies $\overline{p} \subseteq q$. Hence y is in q as desired.

□

References

[1] van Heijenoort, J.: From Frege to Gödel. A Source Book in Mathematical Logic 1879–1931. Harvard University Press, Cambridge, Massachusetts (1967)

[2] Zermelo, E.: Neuer Beweis fr die Mglichkeit einer Wohlordnung. Mathematische Annalen **65**, 107–128 (1908). English translation, "The Possibility of a Well-Ordering" in [1], pages 183–198