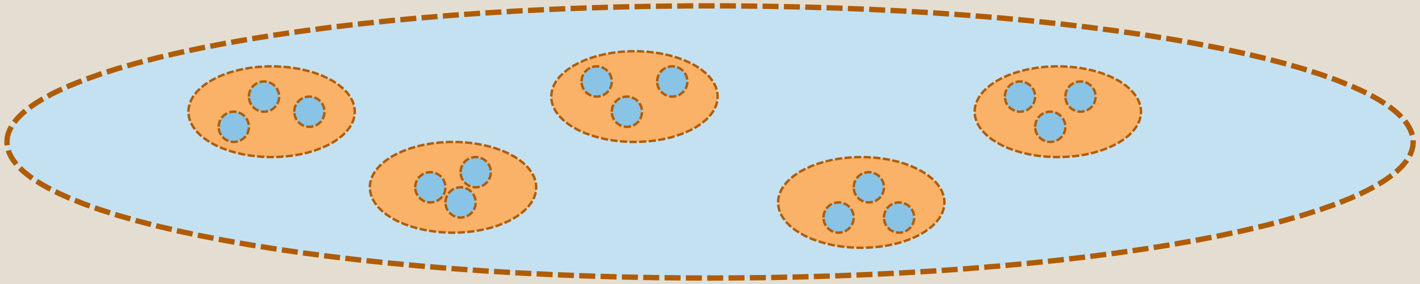
Formalization of Zermelo's Well-Ordering Theorem

INITIAL BACHELOR SEMINAR TALK
DOMINIK KIRST

Facts

- Topic: Axiom of Choice → Well-Ordering Principle
- Fundament: axioms of ZF-set-theory
- Formalization: Coq extended with XM
- Advisor: Jonas Kaiser
- Supervisor: Prof. Gert Smolka

Axiom of Choice (AC)



$$AC \equiv \forall M.\ \exists \gamma.\ \forall X \in M.\ X \neq \emptyset \rightarrow \gamma(X) \in X$$

- Intuitive principle consistent with ZF
- Used in analysis and topology as well
- Key-assumption in Zermelo's proofs

3 Ideas of Well-Ordering (WO)

1. $\mathrm{WO}(M) \equiv \exists\, R \subseteq M^2$ such that:

   R antisymmetric, irreflexive, transitive, linear, well-founded

2. γ-style: $O \subseteq \wp(M)$ represents the initial segments:

   O := {{}, {M1}, {M1,M2}, {M1,M2,M3}, … }

3. Θ-style: O $\subseteq \wp(M)$ represents the rest segments:

   O := {M, M-{M1}, M-{M1,M2}, M-{M1,M2,M3}, … }

Zermelo's 1904 Proof[1]

Given γ and M, construction of O in γ-style:

- γ-set: initial segment of $\gamma(M)$, $\gamma(M\text{-}\{\gamma(M)\})$, ...
- O: set of all γ-sets

Remark:

- In fact, Zermelo constructs Γ as set of all γ-elements
- It follows: $\Gamma=M$ and Γ has canonic ordering

1: Zermelo 1904

Zermelo's 1908 Proof[2]

Given γ and M, construction of O in Θ-style:

- Θ-chain: contains M, A-$\{\gamma(A)\}$ if A, $\bigcap S$ for subsets S
- O: intersection of all Θ-chains and itself a Θ-chain

Remark:

- Zermelo gave second proof in response to criticism
- First axiomatization to be found in this paper
- Θ-chains are essentially an inductive type

4th Idea - Ordinal Numbers

What they are:

- M transitive $\equiv \forall M' \in M.\ M' \subseteq M$
- λ ordinal $\equiv$ λ transitive and λ well-ordered by $\in$

What they do:

- Generalize natural numbers (induction/recursion)
- Represent well-orderings:

$$\mathrm{WO}(M) \leftrightarrow \exists \lambda \in Ord.\ \lambda \cong M$$

Modern Proof[3]

1. Define sequence f by transfinite recursion ($a \notin M$):

$$f(0) := \gamma(M)$$

$$f(1) := \gamma(M\text{-}\{\gamma(M)\}) = \gamma(M\text{-}\{f(0)\}) = \gamma(M\text{-}ran(f|_1))$$

$$f(2) := \gamma(M\text{-}\{f(1), f(2)\}) = \gamma(M\text{-}ran(f|_2))$$

$$\Rightarrow f(\alpha) := \begin{cases} \gamma(M\text{-}ran(f|_\alpha)) & \text{if } M\text{-}ran(f|_\alpha) \neq \emptyset, \\ a & \text{otherwise.} \end{cases}$$

2. Find the least λ with $f(\lambda) = a$, then $\lambda \cong M$

3: Hrbacek & Jech 1999

Hartogs Numbers

Definition:

$h(M)$:= least ordinal not isomorphic to a subset of M

Theorem: $h(M)$ exists for all M

Idea: $h(M) := \{\alpha \in Ord \mid \exists M' \subseteq M.\ \alpha \cong M'\}$

Result:

Obviously $f(h(M)) = a \quad \Rightarrow \quad h(M)$ is upper bound for λ

Implementation Issues

- sets as types coming with en ∈-relation

```
Parameter set: Type.
Parameter el: set -> set -> Prop.
```

- assuming ZF-axioms we define usual set-operations

```
Parameter power: set -> set.
Axiom Power: forall S X, X <e (power S) <-> X c= S.
```

- ordered pairs in Kuratowski-style lead to functions

```
Definition opair A B := pair (singleton A) (pair A B).
Definition relation' R A B := R c= product A B.
```

Thanks for your attention!

References:

- Ernst Zermelo 1904:
  „Beweis, daß jede Menge wohlgeordnet werden kann.“
- Ernst Zermelo 1908:
  „Neuer Beweis für die Möglichkeit einer Wohlordnung.“
- Akihiro Kanamori 2004:
  „Zermelo and Set Theory“
- Danko Ilik 2007:
  „Zermelo's Well-Ordering Theorem in Type Theory
- Karel Hrbacek & Thomas Jech 1999:
  „Introduction to Set Theory“

Website: https://www.ps.uni-saarland.de/~kirst