Large Model Constructions for Second-Order ZF in Dependent Type Theory

CPP 2018

Dominik Kirst and Gert Smolka

Saarland University
Programming Systems Lab
SECOND-ORDER SET THEORY

To avoid the logical antinomies, axiomatic set theory asserts the existence only of sets built up from specific operations:

$$\emptyset, \ \{x, y\}, \ \bigcup x, \ \mathcal{P}x$$
SECOND-ORDER SET THEORY

To avoid the logical antinomies, axiomatic set theory asserts the existence only of sets built up from specific operations:

\[ \emptyset, \{ x, y \}, \bigcup x, \mathcal{P}x \]

Two further operations have a higher-order character:

**Separation:** \( \{ y \in x \mid P y \} \) for a "definite property" \( P \)

**Replacement:** \( \{ z \mid \exists y \in x. R y z \} \) for a "functional relation" \( R \)

[Zermelo, 1930]
SECOND-ORDER SET THEORY

To avoid the logical antinomies, axiomatic set theory asserts the existence only of sets built up from specific operations:

\[ \emptyset, \quad \{ x, y \}, \quad \bigcup x, \quad \mathcal{P} x \]

Two further operations have a higher-order character:

**Separation:** \( \{ y \in x \mid P \, y \} \) for a "definite property" \( P \)
**Replacement:** \( \{ z \mid \exists y \in x. \, R \, y \, z \} \) for a "functional relation" \( R \)

Depending on the meta logic, they can be stated differently:

**First-order:** \( P \) and \( R \) are formulas and the axioms are schematic

**Second-order:** \( P \) and \( R \) are predicates and single axioms suffice

[Zermelo, 1930]
SECOND-ORDER SET THEORY

To avoid the logical antinomies, axiomatic set theory asserts the existence only of sets built up from specific operations:

\[ \emptyset, \{x, y\}, \bigcup x, \mathcal{P}x \]

Two further operations have a higher-order character:

**Separation:** \( \{ y \in x \mid P y \} \) for a "definite property" \( P \)

**Replacement:** \( \{ z \mid \exists y \in x. R y z \} \) for a "functional relation" \( R \)

Depending on the meta logic, they can be stated differently:

**First-order:** \( P \) and \( R \) are formulas and the axioms are schematic

**Second-order:** \( P \) and \( R \) are predicates and single axioms suffice

\[ \implies \text{Second-order ZF is quasi-categorical whereas ZF is not} \]

[Zermelo, 1930]
QUASI-CATEGORICITY

- Previous paper: formalisation of Zermelo’s embedding theorem for concrete second-order axiomatisation ZF:
  
  "Any two models of ZF are either isomorphic or one embeds as an initial segment into the other."

- As a consequence, models of ZF only differ in their height, i.e. ordinality of nested Grothendieck universes

- Extended axiomatisations ZFₙ asserting exactly n universes are hence categorical

[Zermelo, 1930][Kirst and Smolka, 2017]
QUASI-CATEGORICITY

- Previous paper: formalisation of Zermelo’s embedding theorem for concrete second-order axiomatisation ZF:

  "Any two models of \( \text{ZF} \) are either isomorphic or one embeds as an initial segment into the other."

- As a consequence, models of \( \text{ZF} \) only differ in their height, i.e. ordinality of nested Grothendieck universes

- Extended axiomatisations \( \text{ZF}_n \) asserting exactly \( n \) universes are hence categorical

  Question: Do models of every \( \text{ZF}_n \) exist in Coq(+X)?
Type-Theoretical Models

Aczel’s sets-as-trees interpretation:

- Inductive type $\mathcal{T}$ of well-founded trees
- Membership is implemented by children
- (Most) set operations can be implemented directly
- Intensional in that distinct trees of same structure exist

[Aczel, 1978], [Werner, 1997], [Barras, 2010]
Type-Theoretical Models

Aczel’s sets-as-trees interpretation:

- Inductive type $\mathcal{T}$ of well-founded trees
- Membership is implemented by children
- (Most) set operations can be implemented directly
- Intensional in that distinct trees of same structure exist

Assuming a strong quotient axiom for $\mathcal{T}$ we obtain:

- Extensional models
- Large models: since Coq has a hierarchy of type levels, we can iteratively embed $\mathcal{T}$ into itself and obtain universes

$\implies$ Models of all $\mathsf{ZF}_n$

[Aczel, 1978], [Werner, 1997], [Barras, 2010]
**Set Structures**

A **set structure** is a type $\mathcal{M}$ coming with a binary relation $\_ \in \_ : \mathcal{M} \to \mathcal{M} \to \text{Prop}$ called membership.


**Set Structures**

A **set structure** is a type $\mathcal{M}$ coming with a binary relation $\in : \mathcal{M} \to \mathcal{M} \to \text{Prop}$ called membership.

- **Inclusion** $x \subseteq y := \forall z \in x. z \in y$
- **Equivalence** $x \equiv y := x \subseteq y \land y \subseteq x$
- **Equivalence classes** $[x] := \lambda y. x \equiv y$
- A set $x$ is **transitive** if $y \in x$ implies $y \subseteq x$. 
**Set Structures**

A **set structure** is a type $\mathcal{M}$ coming with a binary relation $\_ \in \_ : \mathcal{M} \to \mathcal{M} \to \text{Prop}$ called membership.

- **Inclusion** $x \subseteq y := \forall z \in x. z \in y$
- **Equivalence** $x \equiv y := x \subseteq y \land y \subseteq x$
- **Equivalence classes** $[x] := \lambda y. x \equiv y$
- A set $x$ is **transitive** if $y \in x$ implies $y \subseteq x$.

We define the inductive class $WF$ of **well-founded sets** by:

\[
\begin{align*}
   x \subseteq WF & \quad \Rightarrow \quad x \in WF \\
   x \in WF & \quad \Rightarrow \quad x \subseteq WF
\end{align*}
\]

The derived (strong!) induction principle is called $\in$-induction.
ZF-STRUCTURES

A **ZF-structure** is a set structure $M$ together with constants

\[
\emptyset : M \\
\{,\} : M \to M \to M \\
\cup : M \to M \\
\mathcal{P} : M \to M \\
\_ \cap \_ : (M \to \text{Prop}) \to M \to M \\
\_@\_ : (M \to M) \to M \to M \\
\delta : (M \to \text{Prop}) \to M
\]

for empty set, pairing, union, power set, separation, replacement, and description.
**EXTENSIONAL AXIOMATISATION ZF**

**Extensionality:** \( x \equiv y \to x = y \)

**Foundation:** \( x \in \text{WF} \)

**Infinity:** \( \exists \omega. \forall x. x \in \omega \leftrightarrow \exists n : \mathbb{N}. x = \mathcal{P}^n \emptyset \)

**Emptiness:** \( x \not\in \emptyset \)

**Pairing:** \( z \in \{x, y\} \leftrightarrow z = x \lor z = y \)

**Union:** \( z \in \bigcup x \leftrightarrow \exists y \in x. z \in y \)

**Power:** \( y \in \mathcal{P}x \leftrightarrow y \subseteq x \)

**Separation:** \( y \in P \cap x \leftrightarrow y \in x \land y \in P \quad \forall P : \mathcal{M} \to \text{Prop} \)

**Replacement:** \( z \in F@x \leftrightarrow \exists y \in x. z = F y \quad \forall F : \mathcal{M} \to \mathcal{M} \)

**Description:** \( (\exists! x. x \in P) \to \delta P \in P \quad \forall P : \mathcal{M} \to \text{Prop} \)
## Intensional Axiomatisation \( \mathbf{ZF}_\equiv \)

<table>
<thead>
<tr>
<th>Axiom</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morphism:</td>
<td>( x \equiv x' \rightarrow x \in y \rightarrow x' \in y )</td>
</tr>
<tr>
<td>Foundation:</td>
<td>( x \in \text{WF} )</td>
</tr>
<tr>
<td>Infinity:</td>
<td>( \exists \omega. \forall x. x \in \omega \leftrightarrow \exists n : \mathbb{N}. x \equiv \mathcal{P}^n \emptyset )</td>
</tr>
<tr>
<td>Emptiness:</td>
<td>( x \not\in \emptyset )</td>
</tr>
<tr>
<td>Pairing:</td>
<td>( z \in {x, y} \leftrightarrow z \equiv x \lor z \equiv y )</td>
</tr>
<tr>
<td>Union:</td>
<td>( z \in \bigcup x \leftrightarrow \exists y \in x. z \in y )</td>
</tr>
<tr>
<td>Power:</td>
<td>( y \in \mathcal{P} x \leftrightarrow y \subseteq x )</td>
</tr>
<tr>
<td>Separation:</td>
<td>( y \in P \cap x \leftrightarrow y \in x \land y \in P ) ( \forall P : \mathcal{M} \rightarrow \text{Prop} )</td>
</tr>
<tr>
<td>Replacement:</td>
<td>( z \in F@x \leftrightarrow \exists y \in x. z \equiv F y ) ( \forall F : \mathcal{M} \rightarrow \mathcal{M} )</td>
</tr>
<tr>
<td>Description:</td>
<td>( (\exists x. P \approx [x]) \rightarrow \delta P \in P ) ( \forall P : \mathcal{M} \rightarrow \text{Prop} ) ( P \approx P' \rightarrow \delta P = \delta P' ) ( \forall P, P' )</td>
</tr>
</tbody>
</table>
Grothendieck Universes

A transitive set $U$ is a **universe** if it is closed under all set operations. That is, for all $x, y \in U$, classes $P : M \rightarrow \text{Prop}$ and functions $F : M \rightarrow M$ the following properties hold:

\[
\begin{align*}
\emptyset & \in U \\
\{x, y\} & \in U \\
\bigcup x & \in U \\
P & \in U \\
P \cap x & \in U \\
P \cap x & \subseteq U \\
P \cap x & \subseteq U \\
P \cap x & \subseteq U
\end{align*}
\]
**Grothendieck Universes**

A transitive set $U$ is a **universe** if it is closed under all set operations. That is, for all $x, y \in U$, classes $P : M \to \text{Prop}$ and functions $F : M \to M$ the following properties hold:

- $\emptyset \in U$
- $\mathcal{P}x \in U$
- $\{x, y\} \in U$
- $P \cap x \in U$
- $\bigcup x \in U$
- $F@x \in U$ if $F@x \subseteq U$

Axiomatisations extending ZF (i.e. ZF without Infinity):

- $\text{ZF}_{\geq n}$ asserts at least $n$ universes
- $\text{ZF}_n$ asserts exactly $n$ universes
- $\text{ZF}_{\geq \omega}$ asserts infinitely many universes
### RELATIONAL REPLACEMENT

Replacement for functional relations $R : \mathcal{M} \to \mathcal{M} \to \text{Prop}$:

$$R@x := (\lambda y. \delta(R y))@(\text{dom}(R) \cap x)$$

$$z \in R@x \iff \exists y. y \in x \land R y z$$
Relational Replacement

Replacement for functional relations $R : \mathcal{M} \to \mathcal{M} \to \text{Prop}$:

$$R@x := (\lambda y. \delta(R y))@ (\text{dom}(R) \cap x)$$

$$z \in R@x \iff \exists y. y \in x \land R y z$$

Many other set operations can be reconstructed:

- $\{x, y\} = (\lambda ab. (a = \emptyset \land b = x) \lor (a = \mathcal{P}\emptyset \land b = y))@\mathcal{P}(\mathcal{P}\emptyset)$
- $P \cap x = (\lambda ab. a \in P \land a = b)@x$
- $F@x = (\lambda ab. b = Fa)@x$
- $\delta P = \bigcup((\lambda ab. b \in P)@\mathcal{P}\emptyset)$ if there is a unique $x \in P$

Hence a set $U$ is a universe iff it is transitive, contains $\emptyset$ and is closed under union, power and relational replacement.
Aczel’s Intensional Model

Define the inductive type $\mathcal{T} : \text{Type}$ of well-founded trees with a term constructor $\tau : \forall (A : \text{Type}) \ (f : A \to \mathcal{T}) \ . \ \mathcal{T}$

[Aczel, 1978]
Aczel’s Intensional Model

Define the inductive type $\mathcal{T}_i : \text{Type}_i$ of well-founded trees with a term constructor $\tau : \forall (A : \text{Type}_j) \ (f : A \rightarrow \mathcal{T}_i). \mathcal{T}_i$ for $j < i$. 

[Aczel, 1978]
Aczel’s Intensional Model

Define the inductive type $\mathcal{T} : \text{Type}$ of well-founded trees with a term constructor $\tau : \forall (A : \text{Type}) (f : A \rightarrow \mathcal{T}). \mathcal{T}$

\[
\tau A f = \begin{array}{c}
\bullet \\
\downarrow \\
f a & \ldots & f a'
\end{array}
\]

[Aczel, 1978]
**Aczel’s Intensional Model**

Define the inductive type $\mathcal{T} : \text{Type}$ of **well-founded trees** with a term constructor $\tau : \forall (A : \text{Type}) (f : A \to \mathcal{T}). \mathcal{T}$

\[
\tau A f = \bullet \\
\quad f a \quad \ldots \quad f a'
\]

**Tree equivalence** is the binary inductive predicate defined by

\[
\forall a : A. \exists b : B. f a \equiv_{\mathcal{T}} g b \quad \forall b : B. \exists a : A. f a \equiv_{\mathcal{T}} g b
\]

\[
\tau A f \equiv_{\mathcal{T}} \tau B g
\]

and **tree membership** is defined by $s \in \tau A f := \exists a : A. s \equiv_{\mathcal{T}} f a$. This makes $\mathcal{T}$ a set structure with $s \equiv t$ iff $s \equiv_{\mathcal{T}} t$.

[Aczel, 1978]
Aczel’s Intensional Model (ctd.)

Turn $\mathcal{T}$ into a ZF-structure without description by setting:
Aczel’s Intensional Model (ctd.)

Turn $\mathcal{T}$ into a ZF-structure without description by setting:

$$\emptyset := \tau \bot \text{elim}_\bot$$
Aczel’s Intensional Model (ctd.)

Turn $\mathcal{T}$ into a ZF-structure without description by setting:

$$\emptyset := \tau \bot \text{ elim}_\bot$$

$$\{s, t\} := \tau \bigcap (\lambda b. \text{ if } b \text{ then } s \text{ else } t)$$
Aczel’s Intensional Model (ctd.)

Turn $T$ into a ZF-structure without description by setting:

$$
\emptyset := \tau \perp \text{elim}_\perp \\
\{s, t\} := \tau \mathbb{B} (\lambda b. \text{if } b \text{ then } s \text{ else } t) \\
\bigcup (\tau A f) := \tau (\Sigma a. p_1(f a)) (\lambda (a, b). p_2(f a) b)
$$

[Aczel, 1978]
**Aczel's Intensional Model (ctd.)**

Turn $\mathcal{T}$ into a ZF-structure without description by setting:

$$
\emptyset := \tau \bot \text{elim}_{\bot} \\
\{s, t\} := \tau \mathbb{B} (\lambda b. \text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau A f) := \tau (\Sigma a. p_1(f a)) (\lambda (a, b). p_2(f a) b) \\
\mathcal{P}(\tau A f) := \tau (A \rightarrow \text{Prop}) (\lambda P. \tau (\Sigma a. a \in P) (f \circ \pi_1))
$$
**Aczel’s Intensional Model (ctd.)**

Turn \( \mathcal{T} \) into a ZF-structure without description by setting:

\[
\emptyset := \tau \perp \text{elim}_\perp \\
\{s, t\} := \tau \mathbb{B} (\lambda b. \text{if } b \text{ then } s \text{ else } t) \\
\bigcup (\tau A f) := \tau (\Sigma a. p_1(f a)) (\lambda (a, b). p_2(f a) b) \\
\mathcal{P}(\tau A f) := \tau (A \to \text{Prop}) (\lambda P. \tau (\Sigma a. a \in P) (f \circ \pi_1)) \\
P \cap (\tau A f) := \tau (\Sigma a. (f a) \in P) (f \circ \pi_1)
\]

[Aczel, 1978]
Aczel’s Intensional Model (ctd.)

Turn $\mathcal{T}$ into a ZF-structure without description by setting:

- $\emptyset := \tau \perp \text{elim}_\perp$
- $\{s, t\} := \tau \uplus (\lambda b. \text{if } b \text{ then } s \text{ else } t)$
- $\bigcup (\tau A f) := \tau (\Sigma a. p_1(f a)) (\lambda(a, b). p_2(f a) b)$
- $\mathcal{P}(\tau A f) := \tau (A \rightarrow \text{Prop}) (\lambda P. \tau (\Sigma a. a \in P) (f \circ \pi_1))$
- $P \cap (\tau A f) := \tau (\Sigma a. (f a) \in P) (f \circ \pi_1)$
- $F@ (\tau A f) := \tau A (\lambda a. F(f a))$

[Aczel, 1978]
**Aczel’s Intensional Model (ctd.)**

Turn $\mathcal{T}$ into a ZF-structure without description by setting:

$$\emptyset := \tau \downarrow \text{elim}_\bot$$

$$\{s, t\} := \tau \mathbb{B} (\lambda b. \text{if } b \text{ then } s \text{ else } t)$$

$$\bigcup (\tau A f) := \tau (\Sigma a. p_1(f a)) (\lambda (a, b). p_2(f a) b)$$

$$\mathcal{P}(\tau A f) := \tau (A \rightarrow \text{Prop}) (\lambda P. \tau (\Sigma a. a \in P) (f \circ \pi_1))$$

$$P \cap (\tau A f) := \tau (\Sigma a. (f a) \in P) (f \circ \pi_1)$$

$$F @ (\tau A f) := \tau A (\lambda a. F(f a))$$

$$\omega := \tau \mathbb{N} (\lambda n. \mathcal{P}^n \emptyset)$$

[Aczel, 1978]
**Aczel’s Intensional Model (ctd.)**

Turn $\mathcal{T}$ into a ZF-structure without description by setting:

$\emptyset := \tau \bot \text{elim}_\bot$

$\{s, t\} := \tau \mathbb{B} (\lambda b. \text{if } b \text{ then } s \text{ else } t)$

$\bigcup (\tau A f) := \tau (\Sigma a. p_1(f a)) (\lambda (a, b). p_2(f a) b)$

$\mathcal{P}(\tau A f) := \tau (A \rightarrow \text{Prop}) (\lambda P. \tau (\Sigma a. a \in P) (f \circ \pi_1))$

$P \cap (\tau A f) := \tau (\Sigma a. (f a) \in P) (f \circ \pi_1)$

$F@ (\tau A f) := \tau A (\lambda a. F (f a))$

$\omega := \tau \mathbb{N} (\lambda n. \mathcal{P}^n \emptyset)$

**Theorem**

$\mathcal{T}$ satisfies $\textbf{ZF}_\equiv$ without Description.
AN EXTENSIONAL MODEL

Assume a description operator $\delta : (\mathcal{T} \rightarrow \text{Prop}) \rightarrow \mathcal{T}$ satisfying the intensional version of Description and proof irrelevance.
**An Extensional Model**

Assume a description operator $\delta : (T \rightarrow \text{Prop}) \rightarrow T$ satisfying the intensional version of Description and proof irrelevance.

Define a normaliser $\gamma_s := \delta[s]$ with easy properties:

$$\gamma_s \equiv s \quad s \equiv t \iff \gamma_s = \gamma_t \quad \gamma(\gamma_s) = \gamma_s$$
AN EXTENSIONAL MODEL

Assume a description operator \( \delta : (\mathcal{T} \rightarrow \text{Prop}) \rightarrow \mathcal{T} \) satisfying the intensional version of Description and proof irrelevance.

Define a **normaliser** \( \gamma s := \delta[s] \) with easy properties:

\[
\gamma s \equiv s \quad s \equiv t \iff \gamma s = \gamma t \quad \gamma(\gamma s) = \gamma s
\]

Define the ZF-structure of **canonical representatives** \( S := (\Sigma s. \gamma s = s) \) with set operations lifted from \( \mathcal{T} \).
An Extensional Model

Assume a description operator $\delta : (T \to \text{Prop}) \to T$ satisfying the intensional version of Description and proof irrelevance.

Define a normaliser $\gamma_s := \delta[s]$ with easy properties:

$$\gamma s \equiv s \quad s \equiv t \iff \gamma s = \gamma t \quad \gamma (\gamma s) = \gamma s$$

Define the ZF-structure of canonical representatives $S := (\Sigma s. \gamma s = s)$ with set operations lifted from $T$.

Theorem

$T$ satisfies $\text{ZF}_{\equiv}$ and $S$ satisfies $\text{ZF}$. 

**Large Models: $\text{ZF}_{\geq n}$**

Intensional models $\mathcal{M} : \text{Type}_j$ embed into $\mathcal{T}_i$ if $j < i$:

$$\iota x := \tau (\Sigma y. y \in x) (\iota \circ \pi_1)$$

**Lemma**

$U_{\mathcal{M}} := \tau \mathcal{M} \iota$ is a universe. Moreover, if $\mathcal{M} \models \text{ZF}_{\geq n}$ then $U_{\mathcal{M}}$ contains $n$ universes and it follows that $S_i \models \text{ZF}_{\geq n+1}$. 
LARGE MODELS: \( \mathsf{ZF}_{\geq n} \)

Intensional models \( \mathcal{M} : \text{Type}_j \) embed into \( \mathcal{T}_i \) if \( j < i \):

\[
\iota x := \tau (\Sigma y. y \in x) (\iota \circ \pi_1)
\]

Lemma
\( U_\mathcal{M} := \tau \mathcal{M} \iota \) is a universe. Moreover, if \( \mathcal{M} \models \mathsf{ZF}_{\geq n} \) then \( U_\mathcal{M} \) contains \( n \) universes and it follows that \( S_i \models \mathsf{ZF}_{\geq n+1} \).

Theorem (informal)
\( \mathsf{ZF}_{\geq n} \) has a model for every \( n \).
**LARGE MODELS: $\mathbf{ZF}_{\geq n}$**

Intensional models $\mathcal{M} : \text{Type}_j$ embed into $\mathcal{T}_i$ if $j < i$:

$$\iota x := \tau (\Sigma y. y \in x) (\iota \circ \pi_1)$$

**Lemma**

$U_{\mathcal{M}} := \tau \mathcal{M} \iota$ is a universe. Moreover, if $\mathcal{M} \models \mathbf{ZF}_{\geq n}$ then $U_{\mathcal{M}}$ contains $n$ universes and it follows that $S_i \models \mathbf{ZF}_{\geq n+1}$.

**Theorem (informal)**

$\mathbf{ZF}_{\geq n}$ has a model for every $n$.

**Fact**

$$(\forall n : \mathbb{N}. \exists \mathcal{M} : \text{Type}_i. \mathcal{M} \models \mathbf{ZF}_{\geq n})$$
Large Models: $\textbf{ZF}_{\geq n}$

Intensional models $\mathcal{M} : \text{Type}_j$ embed into $\mathcal{T}_i$ if $j < i$:

$$\iota x := \tau (\Sigma y. y \in x) (\iota \circ \pi_1)$$

Lemma

$U_\mathcal{M} := \tau \mathcal{M} \iota$ is a universe. Moreover, if $\mathcal{M} \models \textbf{ZF}_{\geq n}$ then $U_\mathcal{M}$ contains $n$ universes and it follows that $S_i \models \textbf{ZF}_{\geq n+1}$.

Theorem (informal)

$\textbf{ZF}_{\geq n}$ has a model for every $n$.

Fact

$$(\forall n : \mathbb{N}. \exists \mathcal{M} : \text{Type}_i. \mathcal{M} \models \textbf{ZF}_{\geq n}) \rightarrow S_{i+1} \models \textbf{ZF}_{\geq \omega}$$
**Large Models:** \( \mathbf{ZF}_{\geq n} \)

Intensional models \( \mathcal{M} : \text{Type}_j \) embed into \( \mathcal{T}_i \) if \( j < i \):

\[
\iota x := \tau (\Sigma y \cdot y \in x) (\iota \circ \pi_1)
\]

**Lemma**

\( U_\mathcal{M} := \tau \mathcal{M} \iota \) is a universe. Moreover, if \( \mathcal{M} \models \mathbf{ZF}_{\geq n} \) then \( U_\mathcal{M} \) contains \( n \) universes and it follows that \( S_i \models \mathbf{ZF}_{\geq n+1} \).

**Theorem (informal)**

\( \mathbf{ZF}_{\geq n} \) has a model for every \( n \).

**Fact**

\[
(\forall n : \mathbb{N}. \exists \mathcal{M} : \text{Type}_i. \mathcal{M} \models \mathbf{ZF}_{\geq n}) \rightarrow S_{i+1} \models \mathbf{ZF}_{\geq \omega}
\]
LARGE MODELS: $\text{ZF}_n$

Sharpen last result using further ingredients:

- **Excluded Middle**: $\forall P : \text{Prop. } P \lor \neg P$
- **Cumulative Hierarchy**: well-ordered stratification
- **Truncation**: if $\text{ZF}_{\geq n}$ has a model so does $\text{ZF}_n$
- **Embedding**: any two models of $\text{ZF}$ are either isomorphic or one is an initial segment of the other [Zermelo, 1930]
- **Categoricity**: any two models of $\text{ZF}_n$ are isomorphic

[15] [Kirst and Smolka, 2017]
LARGE MODELS: \( \text{ZF}_n \)

Sharpen last result using further ingredients:

- **Excluded Middle**: \( \forall P : \text{Prop.} \, P \lor \neg P \)
- **Cumulative Hierarchy**: well-ordered stratification
- **Truncation**: if \( \text{ZF}_{\geq n} \) has a model so does \( \text{ZF}_n \)
- **Embedding**: any two models of \( \text{ZF} \) are either isomorphic or one is an initial segment of the other [Zermelo, 1930]
- **Categoricity**: any two models of \( \text{ZF}_n \) are isomorphic

Theorem (informal)

\( \text{ZF}_n \) has a unique model (up to isomorphism) for every \( n \).

[Kirst and Smolka, 2017]
What else is in the paper?

- General properties of membership embeddings
- Partial extensional models using weaker quotient axioms
- Least universe is the class of hereditarily finite sets (*)&
- Equivalence of \( \mathbf{ZF} \) and \( \mathbf{ZF}_{\geq 1} \) (*)
- Independence of Foundation over the rest of \( \mathbf{ZF} \) (*)

(*) Assuming Excluded Middle
COQ FOR SET THEORY

- Axiomatic freedom enables independence proofs
- Type classes for structures and axiom systems
- Well-founded recursion immediate on type-level
- Universe polymorphism allows feasible model embedding
- Compact development (4250 loc: 1600 spec, 2650 proof)

www.ps.uni-saarland.de/extras/cpp18-sets/
REFERENCES

The Type Theoretic Interpretation of Constructive Set Theory.

Barras, B. (2010).
Sets in Coq, Coq in Sets.

Categoricity Results for Second-Order ZF in Dependent Type Theory.

Sets in Types, Types in Sets.

Zermelo, E. (1930).
Über Grenzzahlen und Mengenbereiche: Neue Untersuchungen über die Grundlagen der Mengenlehre.
Fundamenta Mathematicae 16, 29–47.
Future Work

- Formalisation of first-order set theory: Independence of choice and continuum hypothesis by embedding of first-order syntax

- Type-theoretic versions of cardinality results:
  Hartogs: for any type there is a larger well-ordered type
  Sierpinski: GCH implies AC
## Development Details

<table>
<thead>
<tr>
<th>File</th>
<th>Spec</th>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prelims.v</td>
<td>236</td>
<td>92</td>
</tr>
<tr>
<td>Embeddings.v</td>
<td>92</td>
<td>227</td>
</tr>
<tr>
<td>Aczel.v</td>
<td>140</td>
<td>229</td>
</tr>
<tr>
<td>Quotient Constructions</td>
<td>244</td>
<td>377</td>
</tr>
<tr>
<td>Large.v</td>
<td>45</td>
<td>85</td>
</tr>
<tr>
<td>Basics.v</td>
<td>174</td>
<td>295</td>
</tr>
<tr>
<td>Uncountable.v</td>
<td>26</td>
<td>32</td>
</tr>
<tr>
<td>Stage.v</td>
<td>99</td>
<td>256</td>
</tr>
<tr>
<td>Infinity.v</td>
<td>132</td>
<td>348</td>
</tr>
<tr>
<td>Zermelo.v</td>
<td>177</td>
<td>304</td>
</tr>
<tr>
<td>Categoricity.v</td>
<td>15</td>
<td>30</td>
</tr>
<tr>
<td>Truncation.v</td>
<td>103</td>
<td>216</td>
</tr>
<tr>
<td>Permutation.v</td>
<td>108</td>
<td>168</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1591</td>
<td>2659</td>
</tr>
</tbody>
</table>
## Overview of Results

<table>
<thead>
<tr>
<th>Formal Statement</th>
<th>Axioms</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_i \models ZF'$</td>
<td>none</td>
</tr>
<tr>
<td>$S'_i \models Z$</td>
<td>CE, PI$_1$</td>
</tr>
<tr>
<td>$S_i \models ZF'$</td>
<td>CR, PI$_2$</td>
</tr>
<tr>
<td>$T_i \models ZF_{\equiv}$ and $S_i \models ZF$</td>
<td>TD, PI$_2$</td>
</tr>
<tr>
<td>$\forall n : \mathbb{N}. \exists M. \models ZF_{\geq n}$</td>
<td>TD, PI$_2$</td>
</tr>
<tr>
<td>$\models ZF \rightarrow (\forall x. x \in \Omega \leftrightarrow x \in HF)$</td>
<td>XM</td>
</tr>
<tr>
<td>$\models ZF \rightarrow \models ZF_{\geq 1}$</td>
<td>XM</td>
</tr>
<tr>
<td>$\models ZF_{\geq 1} \rightarrow \models ZF$</td>
<td>none</td>
</tr>
<tr>
<td>$(\exists M. \models ZF_{\geq n}) \rightarrow (\exists M. \models ZF_n)$</td>
<td>XM</td>
</tr>
<tr>
<td>$\forall n : \mathbb{N}. \exists! M. \models ZF_n$</td>
<td>XM</td>
</tr>
<tr>
<td>$\models ZF^* \rightarrow \models WF \models ZF$</td>
<td>XM</td>
</tr>
<tr>
<td>$\models ZF \rightarrow \models (01) \models ZF^* + \neg Found$</td>
<td>XM</td>
</tr>
</tbody>
</table>
Hereditarily Finite Sets

The classes $FI$ of finite sets and $HF$ of hereditarily finite sets are

\[
\begin{align*}
\emptyset & \in FI \\
y \in FI & \Rightarrow x.y \in FI \\
x \in FI & \Rightarrow \forall y \in x. y \in HF \\
x \in HF & \Rightarrow x \in FI
\end{align*}
\]

Set $\Omega := \bigcup \omega$, then:

- $x \in \Omega$ iff $x \in HF$
- $\Omega$ is least universe
- $\mathcal{M} \models ZF$ iff $\mathcal{M} \models ZF_{\geq 1}$
INDEPENDENCE OF FOUNDATION

If $M$ is a model of $ZF$ without Foundation, then $M_{WF} := (\Sigma x. x \in WF)$ induces a model of $ZF$.

If $M$ is a model of $ZF$, then every permutation $F : M \rightarrow M$ induces a model $M_F$ of $ZF$ without Foundation:

\[
\begin{align*}
\emptyset_\pi & := \pi^{-1}\emptyset \\
\{x, y\}_\pi & := \pi^{-1}\{x, y\} \\
\bigcup_\pi x & := \pi^{-1}\bigcup(\pi x) \\
\mathcal{P}_\pi x & := \pi^{-1}(\pi^{-1}@\mathcal{P}(\pi x)) \\
\bigcap_\pi x & := \pi^{-1}(\bigcap(\pi x)) \\
F@_\pi x & := \pi^{-1}(F@(\pi x)) \\
\delta_\pi P & := \delta P
\end{align*}
\]

Any transposition $F := (x \{x\})$ yields a model $M_F$ with $x \in F x$. 