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:

$$\emptyset, \quad \{x, y\}, \quad \bigcup x, \quad \mathcal{P}x$$

[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

[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:

$$\emptyset, \quad \{x, y\}, \quad \bigcup x, \quad \mathcal{P}x$$

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

$\Longrightarrow$ 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 $\mathbf{ZF}_n$ 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 **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 $\mathbf{ZF}_n$ asserting exactly n universes are hence categorical

Question: Do models of every $\mathbf{ZF}_n$ exist in Coq(+X)?

[Zermelo, 1930][Kirst and Smolka, 2017]

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

$\Longrightarrow$ Models of all $\mathbf{ZF}_n$

[Aczel, 1978], [Werner, 1997], [Barras, 2010]

Set Structures

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

Set Structures

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

$$\frac{x \subseteq WF}{x \in WF}$$

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

ZF-STRUCTURES

A **ZF-structure** is a set structure $\mathcal{M}$ together with constants

$$
\begin{aligned}
\emptyset &: \mathcal{M} & \_\cap\_ &: (\mathcal{M} \to \mathsf{Prop}) \to \mathcal{M} \to \mathcal{M} \\
\{\_,\_\} &: \mathcal{M} \to \mathcal{M} \to \mathcal{M} & & \\
\bigcup &: \mathcal{M} \to \mathcal{M} & \_@\_ &: (\mathcal{M} \to \mathcal{M}) \to \mathcal{M} \to \mathcal{M} \\
\mathcal{P} &: \mathcal{M} \to \mathcal{M} & \delta &: (\mathcal{M} \to \mathsf{Prop}) \to \mathcal{M}
\end{aligned}
$$

for empty set, pairing, union, power set, separation, replacement, and description.

Extensional Axiomatisation **ZF**

Extensionality:	$x \equiv y \to x = y$	
Foundation:	$x \in WF$	
Infinity:	$\exists \omega.\, \forall x.\, x \in \omega \leftrightarrow \exists n : \mathbb{N}.\, x = \mathcal{P}^n\, \emptyset$	
Emptiness:	$x \notin \emptyset$	
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:	$y \in P \cap x \leftrightarrow y \in x \land y \in P$	$\forall P : \mathcal{M} \to \mathsf{Prop}$
Replacement:	$z \in F@x \leftrightarrow \exists y \in x.\, z = F\, y$	$\forall F : \mathcal{M} \to \mathcal{M}$
Description:	$(\exists! x.\, x \in P) \to \delta P \in P$	$\forall P : \mathcal{M} \to \mathsf{Prop}$

Intensional Axiomatisation $\mathbf{ZF}_{\equiv}$

Morphism:	$x \equiv x' \to x \in y \to x' \in y$	
Foundation:	$x \in WF$	
Infinity:	$\exists \omega. \forall x. x \in \omega \leftrightarrow \exists n : \mathbb{N}. x \equiv \mathcal{P}^n \emptyset$	
Emptiness:	$x \notin \emptyset$	
Pairing:	$z \in \{x, y\} \leftrightarrow z \equiv x \lor z \equiv y$	
Union:	$z \in \bigcup x \leftrightarrow \exists y \in x. z \in y$	
Power:	$y \in \mathcal{P}x \leftrightarrow y \subseteq x$	
Separation:	$y \in P \cap x \leftrightarrow y \in x \land y \in P$	$\forall P : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop}$
Replacement:	$z \in F@x \leftrightarrow \exists y \in x. z \equiv F\, y$	$\forall F : \mathcal{M} \xrightarrow{\equiv} \mathcal{M}$
Description:	$(\exists x. P \approx [x]) \to \delta P \in P$	$\forall P : \mathcal{M} \xrightarrow{\equiv} \mathsf{Prop}$
	$P \approx P' \to \delta P = \delta P'$	$\forall P, P'$

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 $P : \mathcal{M} \to \mathsf{Prop}$ and functions $F : \mathcal{M} \to \mathcal{M}$ the following properties hold:

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

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 $P : \mathcal{M} \to \mathsf{Prop}$ and functions $F : \mathcal{M} \to \mathcal{M}$ the following properties hold:

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

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

- $\mathbf{ZF}_{\geq n}$ asserts at least n universes
- $\mathbf{ZF}_{n}$ asserts exactly n universes
- $\mathbf{ZF}_{\geq \omega}$ asserts infinitely many universes

Relational Replacement

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

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

$$z \in R@x \leftrightarrow \exists y.\, y \in x \wedge R\, y\, z$$

Relational Replacement

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

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

$$z \in R@x \leftrightarrow \exists y.\, y \in x \land R\,y\,z$$

Many other set operations can be reconstructed:

$$\{x, y\} = (\lambda ab.\, (a = \emptyset \land b = x) \lor (a = \mathcal{P}\emptyset \land b = y))@\mathcal{P}(\mathcal{P}\emptyset)$$

$$P \cap x = (\lambda ab.\, a \in P \land a = b)@x$$

$$F@x = (\lambda ab.\, b = F\,a)@x$$

$$\delta P = \bigcup((\lambda ab.\, b \in P)@\mathcal{P}\emptyset) \text{ if there is a unique } x \in P$$

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 $\mathcal{T}$: 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

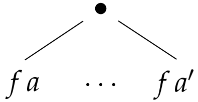
Define the inductive type $\mathcal{T}_i : \mathsf{Type}_i$ of **well-founded trees** with a term constructor $\tau : \forall (A : \mathsf{Type}_j)\,(f : A \to \mathcal{T}_i).\, \mathcal{T}_i$ for $j < i$.

[Aczel, 1978]

Aczel's Intensional Model

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

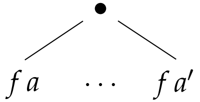
$\tau\, A\, f =$



ACZEL'S INTENSIONAL MODEL

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

$\tau\, A\, f =$



Tree equivalence is the binary inductive predicate defined by

$$\frac{\forall a : A.\, \exists b : B.\, f\,a \equiv_{\mathcal{T}} g\,b \qquad \forall b : B.\, \exists a : A.\, f\,a \equiv_{\mathcal{T}} g\,b}{\tau\, A\, f \equiv_{\mathcal{T}} \tau\, B\, g}$$

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:

$$\emptyset := \tau \perp \mathrm{elim}_{\perp}$$

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

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

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

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

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

$$\begin{aligned}
\emptyset &:= \tau \perp \mathrm{elim}_\perp \\
\{s, t\} &:= \tau\, \mathbb{B}\, (\lambda b.\, \text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau\, A f) &:= \tau\, (\Sigma\, a.\, p_1(f\, a))\, (\lambda(a, b).\, p_2(f\, a)\, b) \\
\mathcal{P}(\tau\, A f) &:= \tau\, (A \to \mathsf{Prop})\, (\lambda P.\, \tau\, (\Sigma\, a.\, a \in P)\, (f \circ \pi_1))
\end{aligned}$$

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

$$\begin{aligned}
\emptyset &:= \tau\,\bot\,\mathrm{elim}_\bot \\
\{s,t\} &:= \tau\,\mathbb{B}\,(\lambda b.\,\text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau\,A f) &:= \tau\,(\Sigma\,a.\,p_1(f\,a))\,(\lambda(a,b).\,p_2(f\,a)\,b) \\
\mathcal{P}(\tau\,A f) &:= \tau\,(A \to \mathsf{Prop})\,(\lambda P.\,\tau\,(\Sigma\,a.\,a \in P)\,(f \circ \pi_1)) \\
P \cap (\tau\,A f) &:= \tau\,(\Sigma\,a.\,(f\,a) \in P)\,(f \circ \pi_1)
\end{aligned}$$

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

$$\begin{aligned}
\emptyset &:= \tau \perp \mathrm{elim}_\perp \\
\{s,t\} &:= \tau\, \mathbb{B}\, (\lambda b.\, \text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau\, A f) &:= \tau\, (\Sigma\, a.\, p_1(f\, a))\, (\lambda(a,b).\, p_2(f\, a)\, b) \\
\mathcal{P}(\tau\, A f) &:= \tau\, (A \to \mathsf{Prop})\, (\lambda P.\, \tau\, (\Sigma\, a.\, a \in P)\, (f \circ \pi_1)) \\
P \cap (\tau\, A f) &:= \tau\, (\Sigma\, a.\, (f\, a) \in P)\, (f \circ \pi_1) \\
F@(\tau\, A f) &:= \tau\, A\, (\lambda a.\, F\, (f\, a))
\end{aligned}$$

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

$$\begin{aligned}
\emptyset &:= \tau \perp \mathrm{elim}_\perp \\
\{s, t\} &:= \tau\, \mathbb{B}\, (\lambda b.\, \text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau\, A f) &:= \tau\, (\Sigma\, a.\, p_1(f\, a))\, (\lambda(a, b).\, p_2(f\, a)\, b) \\
\mathcal{P}(\tau\, A f) &:= \tau\, (A \to \mathsf{Prop})\, (\lambda P.\, \tau\, (\Sigma\, a.\, a \in P)\, (f \circ \pi_1)) \\
P \cap (\tau\, A f) &:= \tau\, (\Sigma\, a.\, (f\, a) \in P)\, (f \circ \pi_1) \\
F@(\tau\, A f) &:= \tau\, A\, (\lambda a.\, F\, (f\, a)) \\
\omega &:= \tau\, \mathbb{N}\, (\lambda n.\, \mathcal{P}^n\, \emptyset)
\end{aligned}$$

[Aczel, 1978]

Aczel's Intensional Model (ctd.)

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

$$\begin{aligned}
\emptyset &:= \tau\,\bot\,\mathrm{elim}_\bot \\
\{s,t\} &:= \tau\,\mathbb{B}\,(\lambda b.\,\text{if } b \text{ then } s \text{ else } t) \\
\bigcup(\tau\,A\,f) &:= \tau\,(\Sigma\,a.\,p_1(f\,a))\,(\lambda(a,b).\,p_2(f\,a)\,b) \\
\mathcal{P}(\tau\,A\,f) &:= \tau\,(A \to \mathsf{Prop})\,(\lambda P.\,\tau\,(\Sigma\,a.\,a \in P)\,(f \circ \pi_1)) \\
P \cap (\tau\,A\,f) &:= \tau\,(\Sigma\,a.\,(f\,a) \in P)\,(f \circ \pi_1) \\
F@(\tau\,A\,f) &:= \tau\,A\,(\lambda a.\,F\,(f\,a)) \\
\omega &:= \tau\,\mathbb{N}\,(\lambda n.\,\mathcal{P}^n\,\emptyset)
\end{aligned}$$

Theorem

$\mathcal{T}$ satisfies $\mathbf{ZF}_\equiv$ without Description.

[Aczel, 1978]

AN EXTENSIONAL MODEL

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

An Extensional Model

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

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

$$\gamma s \equiv s \qquad s \equiv t \leftrightarrow \gamma s = \gamma t \qquad \gamma(\gamma s) = \gamma s$$

An Extensional Model

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

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

$$\gamma s \equiv s \qquad s \equiv t \leftrightarrow \gamma s = \gamma t \qquad \gamma(\gamma s) = \gamma s$$

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

An Extensional Model

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

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

$$\gamma s \equiv s \qquad s \equiv t \leftrightarrow \gamma s = \gamma t \qquad \gamma(\gamma s) = \gamma s$$

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

Theorem
$\mathcal{T}$ satisfies $\mathbf{ZF}_{\equiv}$ and $\mathcal{S}$ satisfies $\mathbf{ZF}$.

Large Models: $\mathbf{ZF}_{\geq n}$

Intensional models $\mathcal{M} : \mathsf{Type}_j$ 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 $\mathcal{S}_i \models \mathbf{ZF}_{\geq n+1}$.

Large Models: $\mathbf{ZF}_{\geq n}$

Intensional models $\mathcal{M} : \mathsf{Type}_j$ 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 $\mathcal{S}_i \models \mathbf{ZF}_{\geq n+1}$.

Theorem (informal)

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

Large Models: $\mathbf{ZF}_{\geq n}$

Intensional models $\mathcal{M} : \mathsf{Type}_j$ 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 $\mathcal{S}_i \models \mathbf{ZF}_{\geq n+1}$.

Theorem (informal)

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

Fact

$(\forall n : \mathbb{N}.\, \exists \mathcal{M} : \mathsf{Type}_i.\, \mathcal{M} \models \mathbf{ZF}_{\geq n})$?

LARGE MODELS: $\mathbf{ZF}_{\geq n}$

Intensional models $\mathcal{M} : \mathsf{Type}_j$ 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 $\mathcal{S}_i \models \mathbf{ZF}_{\geq n+1}$.

Theorem (informal)

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

Fact

$(\forall n : \mathbb{N}.\, \exists \mathcal{M} : \mathsf{Type}_i.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}) \to \mathcal{S}_{i+1} \models \mathbf{ZF}_{\geq \omega}$

Large Models: $\mathbf{ZF}_{\geq n}$

Intensional models $\mathcal{M} : \mathsf{Type}_j$ 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 $\mathcal{S}_i \models \mathbf{ZF}_{\geq n+1}$.

Theorem (informal)

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

Fact

$(\forall n : \mathbb{N}.\, \exists \mathcal{M} : \mathsf{Type}_i.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}) \to \mathcal{S}_{i+1} \models \mathbf{ZF}_{\geq \omega}$ ⚡

LARGE MODELS: $\mathbf{ZF}_n$

Sharpen last result using further ingredients:

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

[Kirst and Smolka, 2017]

LARGE MODELS: $\mathbf{ZF}_n$

Sharpen last result using further ingredients:

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

Theorem (informal)

$\mathbf{ZF}_n$ *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 **ZF** and $\mathbf{ZF}_{\geq 1}$ (∗)
- Independence of Foundation over the rest of **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

Aczel, P. (1978).
The Type Theoretic Interpretation of Constructive Set Theory.
Studies in Logic and the Foundations of Mathematics **96**, 55–66.

Barras, B. (2010).
Sets in Coq, Coq in Sets.
Journal of Formalized Reasoning **3**, 29–48.

Kirst, D. and Smolka, G. (2017).
Categoricity Results for Second-Order ZF in Dependent Type Theory.
In ITP 2017, Brasília, Brazil, September 26-29, 2017, (Ayala-Rincón, M. and Muñoz, C. A., eds), vol. 10499, of LNCS pp. 304–318, Springer.

Werner, B. (1997).
Sets in Types, Types in Sets.
In Theoretical Aspects of Computer Software pp. 530–546, Springer, Heidelberg.

Zermelo, E. (1930).
Über Grenzzahlen und Mengenbereiche: Neue Untersuchungen über die Grundlagen der Mengenlehre.
Fundamenta Mathematicæ **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

File	Spec	Proof
Prelims.v	236	92
Embeddings.v	92	227
Aczel.v	140	229
Quotient Constructions	244	377
Large.v	45	85
Basics.v	174	295
Uncountable.v	26	32
Stage.v	99	256
Infinity.v	132	348
Zermelo.v	177	304
Categoricity.v	15	30
Truncation.v	103	216
Permutation.v	108	168
Total	1591	2659

Overview of Results

Formal Statement	Axioms
$\mathcal{T}_i \models \mathbf{ZF}'_{\equiv}$	none
$\mathcal{S}'_i \models \mathbf{Z}$	CE, PI_1
$\mathcal{S}_i \models \mathbf{ZF}'$	CR, PI_2
$\mathcal{T}_i \models \mathbf{ZF}_{\equiv}$ and $\mathcal{S}_i \models \mathbf{ZF}$	TD, PI_2
$\forall n : \mathbb{N}.\, \exists \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_{\geq n}$	TD, PI_2
$\mathcal{M} \models \mathbf{ZF} \to (\forall x.\, x \in \Omega \leftrightarrow x \in HF)$	XM
$\mathcal{M} \models \mathbf{ZF} \to \mathcal{M} \models \mathbf{ZF}_{\geq 1}$	XM
$\mathcal{M} \models \mathbf{ZF}_{\geq 1} \to \mathcal{M} \models \mathbf{ZF}$	none
$(\exists \mathcal{M}. \mathcal{M} \models \mathbf{ZF}_{\geq n}) \to (\exists \mathcal{M}. \mathcal{M} \models \mathbf{ZF}_n)$	XM
$\forall n : \mathbb{N}.\, \exists! \mathcal{M}.\, \mathcal{M} \models \mathbf{ZF}_n$	TD, XM
$\mathcal{M} \models \mathbf{ZF}^* \to \mathcal{M}_{WF} \models \mathbf{ZF}$	XM
$\mathcal{M} \models \mathbf{ZF} \to \mathcal{M}_{(0\,1)} \models \mathbf{ZF}^* + \neg\mathsf{Found}$	XM

Hereditarily Finite Sets

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

$$\frac{}{\emptyset \in FI} \qquad \frac{y \in FI}{x.y \in FI} \qquad\qquad \frac{x \in FI \quad \forall y \in x.\, y \in HF}{x \in HF}$$

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

- $x \in \Omega$ iff $x \in HF$
- Ω is least universe
- $\mathcal{M} \models \mathbf{ZF}$ iff $\mathcal{M} \models \mathbf{ZF}_{\geq 1}$

Independence of Foundation

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

If $\mathcal{M}$ is a model of **ZF**, then every permutation $F : \mathcal{M} \to \mathcal{M}$ induces a model $\mathcal{M}_F$ of **ZF** without Foundation:

$$
\begin{aligned}
\emptyset_\pi &:= \pi^{-1}\,\emptyset & P \cap_\pi x &:= \pi^{-1}(P \cap (\pi\, x)) \\
\{x, y\}_\pi &:= \pi^{-1}(\{x, y\}) & F@_\pi x &:= \pi^{-1}(F@(\pi\, x)) \\
\textstyle\bigcup_\pi x &:= \pi^{-1}(\textstyle\bigcup(\pi@(\pi\, x))) & \delta_\pi P &:= \delta P \\
\mathcal{P}_\pi x &:= \pi^{-1}(\pi^{-1}@(\mathcal{P}(\pi\, x))) & x \in_\pi y &:= x \in (\pi\, y)
\end{aligned}
$$

Any transposition $F := (x\ \{x\})$ yields a model $\mathcal{M}_F$ with $x \in_F x$.