Formal Construction of a Set Theory in Coq

Masters Defence

supervision: Prof. Smolka & Dr. Brown

Jonas Kaiser

UdS, Graduate School of Computer Science,
Programming Systems Lab

January 11, 2013

Outline

Basic Setup

- Intuitionistic type theory, namely CiC implemented in Coq

[1] can be avoided

Basic Setup

- Intuitionistic type theory, namely CiC implemented in Coq
- Add *law of the excluded middle*: Coq.Logic.Classical_Prop

$$\forall p : \textbf{Prop},\ p \vee \neg p$$

[1] can be avoided

Basic Setup

- Intuitionistic type theory, namely CiC implemented in Coq
- Add *law of the excluded middle*: Coq.Logic.Classical_Prop

$$\forall p : \textbf{Prop},\ p \lor \neg p$$

- Add *Hilbert's ε-operator*: Coq.Logic.Epsilon

$$\forall A : \textbf{Type},\ \forall P : A \to \textbf{Prop},$$
$$\text{inhabited}\ A \to \{x : A \mid (\exists y : A,\ P\ y) \to P\ x\}$$

[1] can be avoided

Basic Setup

- Intuitionistic type theory, namely CiC implemented in Coq
- Add *law of the excluded middle*: Coq.Logic.Classical_Prop

$$\forall p : \textbf{Prop},\ p \lor \neg p$$

- Add *Hilbert's ε-operator*: Coq.Logic.Epsilon

$$\begin{aligned}&\forall A : \textbf{Type},\ \forall P : A \to \textbf{Prop},\\ &\text{inhabited } A \to \{x : A \mid (\exists y : A,\ P\ y) \to P\ x\}\end{aligned}$$

- Inductive *types* used: nat[1], sum types, sigmas
- Inductive *propositions* used: =, inhabited , ⊥, ∨, ∧, ∃

[1] can be avoided

Characterisation of the Meta Theory

We have a *classical* type theory where the following types are inhabited:

Characterisation of the Meta Theory

We have a *classical* type theory where the following types are inhabited:

- $\forall P : \textbf{Prop},\ P + \neg P$

Characterisation of the Meta Theory

We have a *classical* type theory where the following types are inhabited:

- $\forall P : \textsf{\textbf{Prop}},\ P + \neg P$
- $\forall T : \textsf{\textbf{Type}},\ T + (T \to \bot)$

Axiomatisation of Tarski-Grothendieck

- We pose a type set : **Type**,

Axiomatisation of Tarski-Grothendieck

- We pose a type $\mathsf{set} : \textbf{Type}$,
- with the binary containment (or membership) relation

$$\in : \mathsf{set} \to \mathsf{set} \to \textbf{Prop}.$$

Axiomatisation of Tarski-Grothendieck

- We pose a type $\mathsf{set} : \textbf{Type}$,
- with the binary containment (or membership) relation

$$\in : \mathsf{set} \to \mathsf{set} \to \textbf{Prop}.$$

- We define

$$A \subseteq B := \forall x \in A,\ x \in B,$$
$$\mathrm{inh}_{\mathsf{set}}\, X := \exists x : \mathsf{set},\ x \in X.$$

Axiomatisation of Tarski-Grothendieck

- We pose a type $\mathsf{set} : \textbf{Type}$,
- with the binary containment (or membership) relation

$$\in : \mathsf{set} \to \mathsf{set} \to \textbf{Prop}.$$

- We define

$$A \subseteq B := \forall x \in A,\ x \in B,$$
$$\mathrm{inh}_{\mathsf{set}}\, X := \exists x : \mathsf{set},\ x \in X.$$

- Sets are extensional with respect to Coq's (=):

$$A \subseteq B \to B \subseteq A \to A = B.$$

Axiomatisation of Tarski-Grothendieck

- We pose a type $\mathsf{set} : \textbf{Type}$,
- with the binary containment (or membership) relation

$$\in : \mathsf{set} \to \mathsf{set} \to \textbf{Prop}.$$

- We define

$$A \subseteq B := \forall x \in A,\ x \in B,$$
$$\mathrm{inh}_{\mathsf{set}}\, X := \exists x : \mathsf{set},\ x \in X.$$

- Sets are extensional with respect to Coq's (=):

$$A \subseteq B \to B \subseteq A \to A = B.$$

- We pose an induction principle on membership (regularity):

$$\forall P : \mathsf{set} \to \textbf{Prop},\ (\forall X,\ (\forall x \in X,\ P\ x) \to P\ X) \to \forall X,\ P\ X.$$

The Zermelo-Fraenkel Axioms

Axioms from Zermelo[2]:

$$\forall x : \mathsf{set},\ x \notin \emptyset$$

$$\forall x : \mathsf{set},\ x \in \{y, z\} \leftrightarrow x = y \vee x = z$$

$$\forall x : \mathsf{set},\ x \in \bigcup X \leftrightarrow \exists Y \in X,\ x \in Y$$

$$\forall Y : \mathsf{set},\ Y \in \mathscr{P}(X) \leftrightarrow Y \subseteq X$$

[2]Ernst Zermelo. "Untersuchungen über die Grundlagen der Mengenlehre. I". In: *Mathematische Annalen* 65 (2 1908), pp. 261–281. ISSN: 0025-5831.

[3]Abraham A. Fraenkel. "Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre". In: *Mathematische Annalen* 86 (3 1922), pp. 230–237. ISSN: 0025-5831.

The Zermelo-Fraenkel Axioms

Axioms from Zermelo[2]:

$$\forall x : \mathsf{set},\ x \notin \emptyset$$
$$\forall x : \mathsf{set},\ x \in \{y, z\} \leftrightarrow x = y \lor x = z$$
$$\forall x : \mathsf{set},\ x \in \bigcup X \leftrightarrow \exists Y \in X,\ x \in Y$$
$$\forall Y : \mathsf{set},\ Y \in \mathscr{P}(X) \leftrightarrow Y \subseteq X$$

Fraenkel's Axiom of Replacement[3]:

$$\forall y : \mathsf{set},\ y \in \{F\ x \mid x \in X\} \leftrightarrow \exists x \in X,\ y = F\ x$$

---

[2]Ernst Zermelo. "Untersuchungen über die Grundlagen der Mengenlehre. I". In: *Mathematische Annalen* 65 (2 1908), pp. 261–281. ISSN: 0025-5831.

[3]Abraham A. Fraenkel. "Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre". In: *Mathematische Annalen* 86 (3 1922), pp. 230–237. ISSN: 0025-5831.

Example: Replacement

The Axiom of Replacement, not skolemised:

$$\forall X : \mathsf{set}, \forall F : \mathsf{set} \to \mathsf{set}, \; \exists Z : \mathsf{set}, \\ \forall y : \mathsf{set}, \; y \in Z \leftrightarrow \exists x \in X, \; y = F\ x$$

Example: Replacement

The Axiom of Replacement, not skolemised:

$$\forall X : \mathsf{set}, \forall F : \mathsf{set} \to \mathsf{set}, \exists Z : \mathsf{set}, \\ \forall y : \mathsf{set}, y \in Z \leftrightarrow \exists x \in X, y = F\, x$$

The Axiom of Replacement in the Coq development:

```
Parameter Repl : (set → set) → set → set.
Axiom ReplI : forall X : set, forall F : set → set,
  forall x : set, x ∈ X → (F x) ∈ (Repl F X).
Axiom ReplE : forall X : set, forall F : set → set,
  forall y : set, y ∈ (Repl F X) → exists x : set, x ∈ X ∧ y = F x.
```

Grothendieck Universes

- The set U is *transitive* if $(x \in X \to X \in U \to x \in U)$ holds.

[4] Alexander Grothendieck and Jean-Louis Verdier. “Exposé I: Prefaisceaux”. In: *Théorie des Topos et Cohomologie Etale des Schémas*. Ed. by Michael Artin. Vol. 269. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 1972.

Grothendieck Universes

- The set U is *transitive* if $(x \in X \to X \in U \to x \in U)$ holds.
- A *Grothendieck universe*[4] is a transitive set closed under the formation of
  - unordered pairs,
  - unions,
  - power-sets,
  - sets with replacement.

[4] Alexander Grothendieck and Jean-Louis Verdier. "Exposé I: Prefaisceaux". In: *Théorie des Topos et Cohomologie Etale des Schémas*. Ed. by Michael Artin. Vol. 269. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 1972.

Grothendieck Universes

- The set U is *transitive* if $(x \in X \rightarrow X \in U \rightarrow x \in U)$ holds.
- A *Grothendieck universe*[4] is a transitive set closed under the formation of
  - unordered pairs,
  - unions,
  - power-sets,
  - sets with replacement.
- We pose that for every set X there is a least Grothendieck universe containing X, denoted by GU_X.

```
Parameter GU : set → set.
Axiom GUIN : forall N : set, N ∈ (GU N).
```

[4] Alexander Grothendieck and Jean-Louis Verdier. "Exposé I: Prefaisceaux". In: *Théorie des Topos et Cohomologie Etale des Schémas*. Ed. by Michael Artin. Vol. 269. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 1972.

Grothendieck Universes

- The set U is *transitive* if $(x \in X \to X \in U \to x \in U)$ holds.
- A *Grothendieck universe*[4] is a transitive set closed under the formation of
  - unordered pairs,
  - unions,
  - power-sets,
  - sets with replacement.
- We pose that for every set X there is a least Grothendieck universe containing X, denoted by GU_X.

```
Parameter GU : set → set.
Axiom GUIn : forall N : set, N ∈ (GU N).
```

- Infinite stack of models of (ZF) set theory inside (TG) set theory.

[4] Alexander Grothendieck and Jean-Louis Verdier. "Exposé I: Prefaisceaux". In: *Théorie des Topos et Cohomologie Etale des Schémas*. Ed. by Michael Artin. Vol. 269. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 1972.

Grothendieck Universes, ctd.

- Our axiom is equivalent to Tarski's *Axiom A*[5].

[5] Alfred Tarski. "Über unerreichbare Kardinalzahlen". In: *Fundamenta Mathematicae* 30.1 (1938), pp. 68–89.

Grothendieck Universes, ctd.

- Our axiom is equivalent to Tarski's *Axiom A*[5].
- Conceptually we have assumed the existence of infinitely many inaccessible cardinals (independent of ZFC).

[5] Alfred Tarski. "Über unerreichbare Kardinalzahlen". In: *Fundamenta Mathematicae* 30.1 (1938), pp. 68–89.

Grothendieck Universes, ctd.

- Our axiom is equivalent to Tarski's *Axiom A*[5].
- Conceptually we have assumed the existence of infinitely many inaccessible cardinals (independent of ZFC).
- Remark: $\mathsf{GU}_\emptyset$ is the *infinite* set of *hereditarily finite* sets.

[5] Alfred Tarski. "Über unerreichbare Kardinalzahlen". In: *Fundamenta Mathematicae* 30.1 (1938), pp. 68–89.

Grothendieck Universes, ctd.

- Our axiom is equivalent to Tarski's *Axiom A*[5].
- Conceptually we have assumed the existence of infinitely many inaccessible cardinals (independent of ZFC).
- Remark: $\mathsf{GU}_\emptyset$ is the *infinite* set of *hereditarily finite* sets.
- Hence we do not require an *Axiom of Infinity*.

[5] Alfred Tarski. "Über unerreichbare Kardinalzahlen". In: *Fundamenta Mathematicae* 30.1 (1938), pp. 68–89.

A Remark on Choice

"Ist T eine Menge, deren sämtliche Elemente von 0 verschiedene Mengen und untereinander elementarfremd sind, so enthält ihre Vereinigung $\mathfrak{S}T$ mindestens eine Untermenge S_1, welche mit jedem Element von T ein und nur ein Element gemein hat." – Zermelo, 1908

A Remark on Choice

> *"Ist T eine Menge, deren sämtliche Elemente von 0 verschiedene Mengen und untereinander elementarfremd sind, so enthält ihre Vereinigung $\mathfrak{S}T$ mindestens eine Untermenge S_1, welche mit jedem Element von T ein und nur ein Element gemein hat." – Zermelo, 1908*

We can construct the set S_1

- ε_{set} : (set $\to$ **Prop**) $\to$ set $:= \varepsilon$ (inhabits $\emptyset$).
- $D(X)$: set $\to$ set $:= \varepsilon_{\text{set}}(\lambda x : \text{set}.\, x \in X)$.
- We observe $\text{inh}_{\text{set}}\, X \to D(X) \in X$.
- Then $S_1 := \{D(X) \,|\, X \in T\}$ satisfies

$$S_1 \subseteq \bigcup T$$
$$\forall X \in T,\ \exists x,\ \forall y,\ y \in X \land y \in S_1 \leftrightarrow y = x$$

Simple Constructions

- Singleton sets: $\{x\} := \{x, x\}$.

$$\forall y : \mathsf{set},\ y \in \{x\} \leftrightarrow y = x.$$

- Binary Union: $A \cup B := \bigcup\{A, B\}$.

$$\forall x : \mathsf{set},\ x \in A \cup B \leftrightarrow x \in A \vee x \in B.$$

- Union over Family of Indexed Sets: $\bigcup_{x \in X} F_x := \bigcup\{F\ x \mid x \in X\}$.

$$\forall y : \mathsf{set},\ y \in \bigcup_{x \in X} F_x \leftrightarrow \exists x \in X,\ y \in F_x.$$

- First three ordinals:

$$\mathbf{0} := \emptyset \qquad \mathbf{1} := \{\emptyset\} \qquad \mathbf{2} := \{\emptyset, \{\emptyset\}\}$$

Separation

Set comprehension, first attempt

- Consider $Q_P := \lambda Z : \mathsf{set}.\ \forall x : \mathsf{set},\ x \in Z \leftrightarrow P\ x$.
- The set $\varepsilon_{\text{set}}\ Q_P$ is the unrestricted comprehension $\{x \mid P\ x\}$, provided we can prove $Q_P(\varepsilon_{\text{set}}\ Q_P)$ for all P.
- Luckily we cannot, else the Russell set could be constructed.

Separation

Set comprehension, first attempt

- Consider $Q_P := \lambda Z : \mathsf{set}.\ \forall x : \mathsf{set},\ x \in Z \leftrightarrow P\ x$.
- The set $\varepsilon_{\text{set}}\ Q_P$ is the unrestricted comprehension $\{x \mid P\ x\}$, provided we can prove $Q_P(\varepsilon_{\text{set}}\ Q_P)$ for all P.
- Luckily we cannot, else the Russell set could be constructed.

Set comprehension, second attempt

- Now take $Q'_{P,X} := \lambda Z : \mathsf{set}.\ \forall x : \mathsf{set},\ x \in Z \leftrightarrow x \in X \wedge P\ x$.
- Given the axioms of *replacement* and the *empty set* we can now proof $Q'_{P,X}(\varepsilon_{\text{set}}\ Q'_{P,X})$ for all P and X.
- We write the set $\varepsilon_{\text{set}}\ Q'_{P,X}$ as $\{x \in X \mid P\ x\}$ and call it the separation over X.

Intersection and Ordered Pairs

Intersection: $\bigcap M := \{x \in \bigcup M \mid \forall A \in M,\ x \in A\}$

$$\mathrm{inh}_{\mathrm{set}}\, M \longrightarrow (\forall x,\ x \in \bigcap M \leftrightarrow \forall A \in M,\ x \in A)$$

$$\bigcap \emptyset = \emptyset$$

Intersection and Ordered Pairs

Intersection: $\bigcap M := \{x \in \bigcup M \mid \forall A \in M,\ x \in A\}$

$$\mathrm{inh}_{\mathrm{set}}\, M \longrightarrow (\forall x,\ x \in \bigcap M \leftrightarrow \forall A \in M,\ x \in A)$$

$$\bigcap \emptyset = \emptyset$$

Ordered Pairs: $\langle x, y\rangle := \{\{x\}, \{x, y\}\}$

$$\pi_1 p := \bigcup \bigcap p \qquad \pi_1\langle x, y\rangle = x$$

$$\pi_2 p := \bigcup \{x \in \bigcup p \mid x \in \bigcap p \to \bigcup p = \bigcap p\} \qquad \pi_2\langle x, y\rangle = y$$

The characteristic property follows from the projections:

$$\langle a, b\rangle = \langle c, d\rangle \leftrightarrow a = c \wedge b = d$$

Typed Functions and Function Spaces

Three new set formers,

$$\begin{aligned} \mathsf{ap} &: \mathsf{set} \to \mathsf{set} \to \mathsf{set}, \\ \mathsf{lam} &: \mathsf{set} \to (\mathsf{set} \to \mathsf{set}) \to \mathsf{set}, \\ \mathsf{Pi} &: \mathsf{set} \to (\mathsf{set} \to \mathsf{set}) \to \mathsf{set}, \end{aligned}$$

Typed Functions and Function Spaces

Three new set formers,

$$\begin{aligned}\mathsf{ap} &: \mathsf{set} \to \mathsf{set} \to \mathsf{set},\\ \mathsf{lam} &: \mathsf{set} \to (\mathsf{set} \to \mathsf{set}) \to \mathsf{set},\\ \mathsf{Pi} &: \mathsf{set} \to (\mathsf{set} \to \mathsf{set}) \to \mathsf{set},\end{aligned}$$

which should satisfy:

$$\begin{aligned}&\mathsf{ap}\ (\mathsf{lam}\ X\ e)\ x = e_x,\\ &\mathsf{lam}\ X\ e \in \mathsf{Pi}\ X\ Y,\\ &f \in \mathsf{Pi}\ X\ Y \to \mathsf{ap}\ f\ x \in Y_x,\\ &\forall A\ B \in \mathbf{2},\ A \dot{\longrightarrow} B \in \mathbf{2}.\end{aligned}$$

Typed Functions and Function Spaces

Three new set formers,

$$\mathsf{ap} : \mathsf{set} \to \mathsf{set} \to \mathsf{set},$$
$$\mathsf{lam} : \mathsf{set} \to (\mathsf{set} \to \mathsf{set}) \to \mathsf{set},$$
$$\mathsf{Pi} : \mathsf{set} \to (\mathsf{set} \to \mathsf{set}) \to \mathsf{set},$$

which should satisfy:

$$\mathsf{ap}\ (\mathsf{lam}\ X\ e)\ x = e_x,$$
$$\mathsf{lam}\ X\ e \in \mathsf{Pi}\ X\ Y,$$
$$f \in \mathsf{Pi}\ X\ Y \to \mathsf{ap}\ f\ x \in Y_x,$$
$$\forall A\ B \in \mathbf{2},\ A \dot{\longrightarrow} B \in \mathbf{2}.$$

Observation: Standard Graph Encoding fails on last property.

$$\mathbf{1} \dot{\longrightarrow} \mathbf{1} = \{\{\langle \mathbf{0}, \mathbf{0} \rangle\}\} \notin \mathbf{2}$$

Aczel Function Encoding

- We pose the following definitions due to Aczel[6]:

$$\begin{aligned} \mathsf{ap}\, f\ x &:= \{\pi_2\ p \mid p \in \{p \in f \mid \pi_1\ p = x \wedge \mathsf{is\_pair}\ p\}\} \\ \mathsf{lam}\ X\ F &:= \bigcup_{x \in X} \{\langle x, y\rangle \mid y \in F\ x\} \\ \mathsf{Pi}\ X\ Y &:= \{f \in \mathscr{P}(X \times \bigcup(\bigcup_{x \in X} Y_x)) \mid \forall x \in X,\ \mathsf{ap}\, f\ x \in Y_x\} \end{aligned}$$

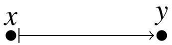
- This satisfies all four properties, in particular:

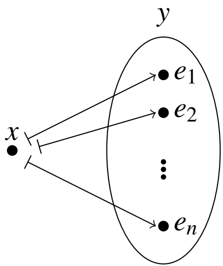
$$\mathbf{1} \dot{\longrightarrow} \mathbf{1} = \{\mathbf{0}\} = \mathbf{1} \in \mathbf{2}$$

[6] Peter Aczel. "On relating type theories and set theories". In: *TYPES*. 1998, pp. 1–18.

Comparison of encodings

Encoding of the function $(x \mapsto y)$





- Standard Graph encoding
- $\{\langle x, y\rangle\}$

- Aczel encoding
- $\{\langle x, e_1\rangle \ldots \langle x, e_n\rangle\}$

Finite Ordinals

Ordinal constructors and set of finite ordinals:

$$
\begin{aligned}
\mathsf{ord_O} &:= \emptyset \\
\mathsf{ord_S}\ N &:= N \cup \{N\} \\
\mathsf{FinOrd} &:= \{N \in \mathsf{GU}_\emptyset \mid \exists n : \mathbb{N},\ \mathsf{iter}\ n\ \mathsf{ord_S}\ \mathsf{ord_O} = N\}
\end{aligned}
$$

Finite Ordinals

Ordinal constructors and set of finite ordinals:

$$\begin{array}{lcl} \mathsf{ord}_{\mathsf{O}} & := & \emptyset \\ \mathsf{ord}_{\mathsf{S}}\, N & := & N \cup \{N\} \\ \mathsf{FinOrd} & := & \{N \in \mathsf{GU}_{\emptyset} \mid \exists n : \mathbb{N},\ \mathsf{iter}\ n\ \mathsf{ord}_{\mathsf{S}}\ \mathsf{ord}_{\mathsf{O}} = N\} \end{array}$$

(Almost) Isomorphism with $\mathbb{N}$

```
Definition FinOrd_embed (n: nat) : set := iter n ordS ordO.
Definition FinOrd_proj (N: set) : nat :=
  match dit {n: nat | iter n ordS ordO = N} with
    | inl (exist n _) ⇒ n
    | inr _ ⇒ 0
  end.
```

Conclusion and Future Work

- We are building set-theoretic models for type theories.
- Closely following the work of Barras[7].
- TG-model for ECC complete.
- Model for CiC in progress.

[7] Bruno Barras. “Sets in Coq, Coq in sets”. In: *Formalized reasoning* 3.1 (2010).

Conclusion and Future Work

- We are building set-theoretic models for type theories.
- Closely following the work of Barras[7].
- TG-model for ECC complete.
- Model for CiC in progress.

Long-term goal:

Construction of a classical type theory, guided by the set-theoretic semantics of our existing TG-models.

[7] Bruno Barras. "Sets in Coq, Coq in sets". In: *Formalized reasoning* 3.1 (2010).

Thank you

http://www.ps.uni-saarland.de/~jkaiser/master.php

Bibliography

[1] Peter Aczel. “On relating type theories and set theories”. In: *TYPES*. 1998, pp. 1–18.

[2] Bruno Barras. “Sets in Coq, Coq in sets”. In: *Formalized reasoning* 3.1 (2010).

[3] Abraham A. Fraenkel. “Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre”. In: *Mathematische Annalen* 86 (3 1922), pp. 230–237. ISSN: 0025-5831.

[4] Alexander Grothendieck and Jean-Louis Verdier. “Exposé I: Prefaisceaux”. In: *Théorie des Topos et Cohomologie Etale des Schémas*. Ed. by Michael Artin. Vol. 269. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 1972.

[5] Alfred Tarski. “Über unerreichbare Kardinalzahlen”. In: *Fundamenta Mathematicae* 30.1 (1938), pp. 68–89.

[6] Ernst Zermelo. “Untersuchungen über die Grundlagen der Mengenlehre. I”. In: *Mathematische Annalen* 65 (2 1908), pp. 261–281. ISSN: 0025-5831.